interact with said first storage unit and with said processor of said apparatus via said keyboard and display units, whereby said computer or cellular phone is configured to utilize and interact with said memory module, said processor and said sensor module of said apparatus.

4. The apparatus according to claim 1, further comprising:

a magnetic strip element that is only activatable after positive authentication of said user's personal biological biometric identification parameters and positive normal non critical measured output of all of the at least one of said life sign detectors of said user measured life sign parameters; and

wherein said magnetic strip is configured to be concealed within the apparatus and on activation configured to extend out of the apparatus for swiping and reading by any of group of devices including a credit card reader, ATM and point of sale magnetic strip reading device; and/or

further comprising an integrated digital data encoder/decoder and a RF transceiver module in communication with the processor, said integrated digital data encoder/decoder and a ~~RF~~ wireless transceiver being configured to communicate with any of a group of external devices including RF operated credit card readers, ATM machines, and remotely operated electronic locks gates and doors opener using RFID based techniques and/or

~~9.~~ The apparatus ~~according to claim 4~~, further comprising a supplementary base-station device in communication with said ~~RF~~ wireless transceiver, said base-station device configured to electrically charge the apparatus and simultaneously automatically execute a backup of the internal secured and non-secured stored data of the apparatus.

5. The apparatus according to claim 1, further comprising a power charging and data backup device in communication with the processor of said apparatus, said device comprising;

i. a charging plug for connecting to the mains supply, an AC-DC converter, a power supply unit and a rechargeable backup battery; and

Formatte

Formatte

ii. a micro processor and a mass memory unit; and

iii. an electronic buzzer activator, a button connected to said buzzer activator and an RF transmitter connected to said electronic buzzer activator , wherein on activating said buzzer button, said RF transmitter is configured to transmit a coded signal to the apparatus to enable the user to determine the location of the apparatus; and

wherein the first storage unit_of said apparatus is in communication with the mass memory unit of said device, thereby to compare and synchronize the version of data stored in the first storage unit_of said apparatus with the version of data stored in mass memory unit of said device; and/or

the apparatus further comprising an integrated GPS module in communication with the processor to precisely locate the geographical position of the apparatus; and/or

the apparatus further comprising at least one of a group of units including a cellular communication modem and a flat display and touch screen in communication with the processor.

6. A method for managing personal and secured data and documentation files of a plurality of unique users, each one of said plurality of unique users having a personal identification unit uniquely associated with said one user for storing each user's personal data and documentation files, each of said personal identification units comprising:

a plurality of biometric sensors integrated within the personal identification unit;

at least one life signs detector, integrated within the personal identification unit, said life signs detector being configured to measure and record at least one of said user's life sign parameters;

a processor in communication with said plurality of biometric sensors;

an authentication unit in communication with the processor;

an encryption unit in communication with said processor;

a first storage unit in communication with said processor and said encryption unit; and

communication and data connection means in communication with said processor;

the method comprising the steps of:

a. the plurality of biometric sensors reading a plurality of personal biological identification parameters of the user holding the personal identification unit~~,; and~~

b. at least one life signs detector, integrated within the apparatus, measuring and recording at least one of said user's life sign parameters;

c said authentication unit comparing each of the personal biological identification parameters of said user or any weighted combination thereof with a pre-recorded set of personal biological identification parameters or any weighted combination thereof stored in said authentication unit; and

d. if said authentication unit positively identifies said user, allowing said user access to said user's personal data and documentation files stored in said first storage unit and allowing said user to communicate with other communication means through said personal identification unit.

7. The method of claim 6 further comprising the steps of: said biometric sensors continuously reading a plurality of personal biological biometric identification parameters of said user holding the apparatus; and

in the event that a significant change occurs in any of the plurality of personal biological biometric identification parameters, or in the normal output reading of said least one of said life signs detectors,, denying access to the stored personal data files and completely shutting down the operation of said apparatus; and/or

wherein at least one of said plurality ~~of biometric sensors is a~~ of life signs ~~detector~~ detectors~~, configured to measure and record at least one of a group of life sign indicators including~~ includes a body pulse rate measurement

indicator, a body O2 saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator, the method further comprising the steps of:

initiating an emergency call to any of a group of registered emergency centers, whenever any of the life sign indicators detects a critical level; and

wherein said emergency call transmits any of a group of data files information associated with the user, including identification of the user, personal medical data file of the user, the measured set of life sign parameters of the user and location of the user; and/or

wherein the method further comprises the step of:

communicating, via any one of a group of communication means, with any of a group of service providers including banks, credit card companies, clinics, hospitals and medical insurance companies, municipal and utility entities and websites frequently accessed by said user thereby allowing said user to access and manage said user's personal data and documentation files stored by said group of service providers.

8. The method of claim 6, wherein said apparatus further comprises an emergency button in communication with said processor and said communication and data connection means, the method further comprising the steps of:

when said emergency button is activated, an emergency medical data file is displayed to the emergency button apparatus activating person and/or a call is initiated between said apparatus and any of a group of registered emergency centers; and

said emergency call transmitting any of a group of data files information associated with the user, including identification data of the user, the personal medical data file of the user, and location of the user; and/or

wherein the apparatus further comprises a magnetic strip element, the method further comprising the step of:

after positive authentication of said user's personal biological identification parameters, activating said magnetic strip thereby allowing said magnetic strip to be read by any of group of devices including a credit card reader, an ATM, a point of sale, a magnetic strip or near field communication reading device (NFC); and/or

wherein the apparatus further comprises a power charging and data backup device, said device comprising a charging and power ~~sub-~~unit, an electronic sub unit and a mass memory solid-state memory unit, the method further comprising the steps of:

comparing the memory content of said apparatus first storage unit to the memory content of said mass memory solid-state memory unit; and

if the first storage unit of the apparatus lacks data, updating the first storage unit with the last version of the data stored within the solid-state memory unit; and

if said solid-state memory unit of said device lacks data, updating the solid-state memory unit of said device with the last version of the data stored within said apparatus's solid-state memory unit.

9. The method of claim 6, wherein each of said plurality of unique users is in communication with a system manager, said system manager managing a remote centralized data communication storage and management system of said plurality of unique users, the method further comprising the steps of:

a. said system manager registering each unique user and storing the personal ID data file of each unique user in a memory sub-system connected to said centralized system; and

b. said registration further includes the step wherein said system manager generates for each system user N pairs of two different randomly selected characters strings, each of said strings is a combination of n alphanumeric characters in length; and

c. said system manager storing said N pairs in said system memory sub-system and sending said n characters strings pairs to be stored in said unique user personal identification unit memory module; and

d. said personal identification unit generating a secret access code of L alphanumeric characters to be further stored in said system memory within a special partition containing the list of said secret access codes for said plurality of unique users without assigning any identification or link between the associated users to his registered secret access code.

10. The method of claim 9, wherein after registration and upon normal initiation of communication between said system manager and each unique user, said system manager further communicating with said unique user and first comparing said unique user's ID data file and said personal identification unit unique embedded characterizing serial number stored in the unique user's personal identification unit with the corresponding user's ID and personal identification data stored in said memory sub-system; and

if the two sets of identification data match;

i. said system manager sending a first string of said stored N strings of coded alphanumeric data, to said user's personal identification unit; and

ii said user personal identification unit responding with the second matching string from the same stored pair of coded alphanumeric data uniquely associated with said user personal identification unit: and

iii said system manager comparing the received second string of coded alphanumeric data with a second string of coded alphanumeric data pre-stored in the memory sub-system; and

iv. said system manager comparing for consecutive M out of N times the received additional different strings of coded alphanumeric data pre-stored in the memory of said personal identification unit associated with said unique user with the additional strings of coded alphanumeric data pre-stored in the memory of sub-system; and

v. if all M strings of coded alphanumeric data match, then said system manager declares authenticating of said unique user and permitting said unique user access to said system.

11. The method of claim 9, further comprising the steps of:

after the step of authenticating, said system manager connecting the personal identification unit of said unique user with any of a group of emergency centers or service providers registered with said system manager at the request of said user personal identification unit; and

in the case of a medical emergency call initiated by said personal identification unit, transferring the user's updated medical data to the emergency center.

12. A system for managing personal and secured data and documentation files of a plurality of unique users, the system comprising:

a. a system manager for managing and updating personal data of said system plurality of unique users and for full-duplex communication with each of said plurality of unique users and a plurality of service providers; and

b. a storage system connected to said system manager to store updated personal data of each of said plurality of unique users; and

c. a plurality of personal identification units, each of said personal identification units being associated with a unique user, each unique user being registered with said system manager, each of said personal identification units comprising a storage unit configured to store the personal ID data file of each unique user and a plurality of biometric sensors for reading a plurality of personal biometric biological identification parameters of the user holding the apparatus, said plurality of biometric sensors being integrated within the personal identification units and at least one life signs detector, integrated within said personal identification units, said life signs detector being configured to measure and record at least one of said user's life sign parameters; and

d. a plurality of computer hosts and cellular phones in communication with said system manager, enabling the direct connection by said system manager with said plurality of unique users through their corresponding personal identification unit; and

**e.** a plurality of registered emergency centers and a plurality of registered service providers in communication with said system manager, said plurality of service providers including banks, credit card companies, insurance companies, clinics, hospitals and medical insurance companies, government, municipal and utility entities and selected websites frequently accessed by said plurality of users;

wherein said system manager's access to and communication with the personal data and documentation files stored in said personal identification units associated with each said unique user and to the personal data and documentation files stored by said group of service providers is only enabled after positive authentication of each of said unique user's personal biometric biological identification parameters by said authentication unit and measuring the normal measured output of each one of said user's life sign parameters;

wherein at least one of said plurality of biometric sensors is a life signs detector, said life signs detector being configured to measure and record at least one of said user's life sign parameters; and

wherein said at least one of said user's life sign parameters is measured by any of a group of life sign indicators including a body pulse rate measurement indicator, a body $O_2$ saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator.

13. The system according to claim 12, wherein each of said plurality of personal identification units comprises:

i. a sensor module comprising a plurality of biometric sensors for reading a plurality of personal biometric biological identification parameters

of the user holding the of personal identification units, said of personal identification units being uniquely identified with said user; and

ii. a processor in communication with said sensor module for processing said personal biological identification parameters and for processing and managing the personal and secured data and documentation files associated with said user; and

iii. an authentication unit in communication with the processor configured to receive and authenticate the identity of said user by comparing said user's personal biological identification parameters read or any weighted combination thereof, by the sensor module and processed by the processor, with a pre-recorded set of personal biological identification parameters or any weighted combination thereof stored in said authentication unit; and

iv. an encryption module in communication with said processor for the encryption plus compression and/or decompression plus decryption of said user's data files; and

v. a storage unit in communication with said processor and said encryption module for the storage of said user's data and documentation files; and

vi. communication and data connection means in communication with said processor for connecting said plurality of personal identification units with said system manager and plurality of service providers; through the use of any device from a group of connection and communication devices including a data interface connector attached to a host computer, a Mini USB, a compatible industrial data interface connector attached to a cellular phone, a near field wireless communication interface, a Bluetooth communication interface, a magnetic reader interface, and a smart card reader based on a contact-less communication interface using induction or RF communication

14. The system according to claim 13, wherein said system manager is configured:

to communicate with said personal identification units to compare the user's ID data file stored in the unique user's personal identification units with the corresponding identification data stored in said storage unit, and

if the two sets of identification data match, then said system manager is configured to initiate a further level of security identification prior to full communication and data updating capability being enabled between said system manager and said user personal identification unit; and

wherein said further level of security identification comprises said system manager sending a first string of coded alphanumeric data uniquely associated with said user personal identification unit to said user personal identification unit, said personal identification unit responding with a second string of coded alphanumeric data uniquely associated with said user personal identification unit, and said system manager verifying the received second string of coded alphanumeric data with a second string of coded alphanumeric data pre-stored in the memory sub-system; and

said system manager comparing for full matching for N consecutive times received additional different strings of coded alphanumeric data pre-stored in the memory of said personal identification unit associated with said unique user with counter generated additional strings of coded alphanumeric data pre-stored in the memory of sub-system; and/or

wherein said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with the user holding his unique personal identification units and in the event that a change occurs in any of the plurality of personal biological biometric identification parameters, access to the stored personal data files is denied and the operation of said identification units is completely shut down; and/or

wherein each personal identification unit further comprises an emergency button in communication with said processor and said communication and data connection means module;

~~wherein at least one of said plurality of biometric sensors is a life signs detector, said life signs detector being configured to measure and record at least one of said user's life sign parameters; and~~

~~wherein said at least one of said user's life sign parameters is measured by any of a group of life sign indicators including a body pulse rate measurement indicator, a body $O_2$ saturation level indicator, a body heat measurement indicator, an electro dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator; and~~

wherein the personal identification unit is configured to trancieve any of a group of data files containing information associated with the user, including files such as the identification data of the user, personal medical data file of the user, the measured set of life sign parameters of the user, financial, insurance and banking data files associated with the user and an updated location of the user.; and

wherein the personal identification unit is configured to initiate an emergency call to any of said plurality of registered emergency centers, whenever said emergency button is activated or whenever any of the group of life sign indicators detects a critical level.

15. The system of claim ~~32~~12, wherein said system, further comprises:

a computerized call center configured to receive phone calls or emergency voice and data messages from any of said plurality of registered emergency centers and a plurality of registered service providers and to communicate with any of said plurality of cellular phone and host computers; and

wherein said call center is configured to communicate the user's location coordinates to an emergency rescue team and simultaneously said call center is configured to communicate with any of said plurality of registered emergency centers and service providers to receive said user's updated medical data and to transfer said data to and from the user's personal identification unit.

**WHAT IS CLAIMED IS:**

1. Apparatus for storing and managing personal and secured data and documentation files associated with a specific user, comprising:

a plurality of biometric sensors for reading a plurality of personal biological biometric identification parameters of the user holding the apparatus, said plurality of biometric sensors being integrated within the apparatus;

at least one life signs detector integrated within the apparatus, said life signs detector being configured to measure and record at least one of said user's life sign parameters;

a first storage unit for the storage of said user's data and documentation files;

an authentication unit comprising a second storage unit, with said second storage unit configured to store a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user, wherein said authentication unit is configured to compare the plurality of personal biological biometric identification parameters of the user holding the apparatus or any weighted combination thereof with the pre-recorded set of personal biological biometric identification parameters or any weighted combination thereof stored in said second storage unit;

a processor in communication with said plurality of biometric sensors, said first storage unit and said authentication unit;

wherein access to the personal data and documentation files stored in said first storage unit is only enabled after said authentication unit positively matches each of the plurality of personal biometric biological identification parameters of the user holding the apparatus or any weighted combination thereof, with the pre-recorded set of personal biological identification parameters stored in said second storage unit; and

wherein, whenever any of said at least one life signs detector detects a critical level of said user measured life sign parameters, the apparatus is

configured to prevent access to said user's personal data and documentation files stored in said first storage unit.

2. The apparatus according to claim 1, wherein said plurality of biometric sensors are configured to continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, or any weighted combination thereof, access to the stored personal data files is denied and the operation of the apparatus is completely shut down; and/or

wherein said at least one of said user's life sign parameters is measured by any of a group of life sign indicators including a body pulse rate measurement indicator, a body O2 saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator

3. The apparatus according to claim 1, further comprising:

communication and data connection means for communicating with an external device, said communication and data connection means being controlled by and in communication with said processor; and/or

wherein, whenever any of the group of life sign indicators detects a critical level, the apparatus is configured to:

initiate an emergency call to any of a group of registered emergency medical or security centers including a request for medical help or police/security intervention, and send to said registered emergency centers any of a group of data files containing information associated with the user, including the identification data file of the user, personal medical and measured physical stress data parameters file of the user, the measured set of life sign parameters of the user and location of the user, and/or

the apparatus further comprises an encryption unit in communication with said processor for the encryption plus compression and for the decompression plus decryption of said user's data files; and/or

an emergency button in communication with said processor and said communication and data connection means module;

wherein on said emergency button being activated, communication is initiated between said apparatus and any of a group of registered emergency centers, said emergency call transmitting any of a group of data files containing information associated with the unique user of said apparatus, including the identification data of said user, the personal medical data file of said user, and location of said user; and/or.

. wherein said apparatus is configured to communicate with any of a group of service providers, said group of service providers including banks, credit card companies, clinics, hospitals and medical insurance companies, municipal and utility entities and websites frequently accessed by said user; thereby allowing said user to access and manage personal data and documentation files, associated with said user; and/or

wherein said external device comprises any one of a group including a remote server, a local server, a host computer, voice or data communication means and a cellular phone; and/or

wherein said emergency call is initiated via any one of a group of communication means including a secured server, directly via the internet by said apparatus connection and communication means, via the internet through any host computer, via a voice and data communication device and via any cellular phone network; and/or

wherein said communication and data connection means comprises at least one of a group of connection and communication devices including a data interface connector attached to a host computer, a Mini USB, a compatible industrial data interface connector attached to a cellular phone, a near field wireless communication interface, a Bluetooth communication interface, a magnetic reader interface, and a smart card reader based on a

contact-less communication interface using induction or RF communication; and/or

further comprising an integrated software module that automatically detects the operating system of the computer or cellular phone connected to said apparatus through one of said group of communicating devices through which the apparatus is connected, said computer or cellular phone having keyboard and display units associated therewith, thereby allowing the user to interact with said first storage unit and with said processor of said apparatus via said keyboard and display units, whereby said computer or cellular phone is configured to utilize and interact with said memory module, said processor and said sensor module of said apparatus.

4. The apparatus according to claim 1, further comprising:

a magnetic strip element that is only activatable after positive authentication of said user's personal biological biometric identification parameters and positive normal non critical measured output of all of the at least one of said life sign detectors of said user measured life sign parameters; and

wherein said magnetic strip is configured to be concealed within the apparatus and on activation configured to extend out of the apparatus for swiping and reading by any of group of devices including a credit card reader, ATM and point of sale magnetic strip reading device; and/or

further comprising an integrated digital data encoder/decoder and a RF transceiver module in communication with the processor, said integrated digital data encoder/decoder and a wireless transceiver being configured to communicate with any of a group of external devices including RF operated credit card readers, ATM machines, and remotely operated electronic locks gates and doors opener using RFID based techniques; and/or

the apparatus further comprising a supplementary base-station device in communication with said wireless transceiver, said base-station device configured to electrically charge the apparatus and simultaneously

automatically execute a backup of the internal secured and non-secured stored data of the apparatus.

5. The apparatus according to claim 1, further comprising a power charging and data backup device in communication with the processor of said apparatus, said device comprising;

i. a charging plug for connecting to the mains supply, an AC-DC converter, a power supply unit and a rechargeable backup battery; and

ii. a micro processor and a mass memory unit; and

iii. an electronic buzzer activator, a button connected to said buzzer activator and an RF transmitter connected to said electronic buzzer activator , wherein on activating said buzzer button, said RF transmitter is configured to transmit a coded signal to the apparatus to enable the user to determine the location of the apparatus; and

wherein the first storage unit of said apparatus is in communication with the mass memory unit of said device, thereby to compare and synchronize the version of data stored in the first storage unit of said apparatus with the version of data stored in mass memory unit of said device; and/or

the apparatus further comprising an integrated GPS module in communication with the processor to precisely locate the geographical position of the apparatus; and/or

the apparatus further comprising at least one of a group of units including a cellular communication modem and a flat display and touch screen in communication with the processor.

6. A method for managing personal and secured data and documentation files of a plurality of unique users, each one of said plurality of unique users having a personal identification unit uniquely associated with said one user for storing each user's personal data and documentation files, each of said personal identification units comprising:

a plurality of biometric sensors integrated within the personal identification unit;

at least one life signs detector, integrated within the personal identification unit, said life signs detector being configured to measure and record at least one of said user's life sign parameters;

a processor in communication with said plurality of biometric sensors;

an authentication unit in communication with the processor;

an encryption unit in communication with said processor;

a first storage unit in communication with said processor and said encryption unit; and

communication and data connection means in communication with said processor;

the method comprising the steps of:

a. the plurality of biometric sensors reading a plurality of personal biological identification parameters of the user holding the personal identification unit;

b. at least one life signs detector, integrated within the apparatus, measuring and recording at least one of said user's life sign parameters;

c said authentication unit comparing each of the personal biological identification parameters of said user or any weighted combination thereof with a pre-recorded set of personal biological identification parameters or any weighted combination thereof stored in said authentication unit; and

d. if said authentication unit positively identifies said user, allowing said user access to said user's personal data and documentation files stored in said first storage unit and allowing said user to communicate with other communication means through said personal identification unit.

7. The method of claim 6 further comprising the steps of: said biometric sensors continuously reading a plurality of personal biological biometric identification parameters of said user holding the apparatus; and

in the event that a significant change occurs in any of the plurality of personal biological biometric identification parameters, or in the normal output reading of said least one of said life signs detectors,, denying access to the stored personal data files and completely shutting down the operation of said apparatus; and/or

wherein at least one of said plurality of life signs detectors includes a body pulse rate measurement indicator, a body O2 saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator, the method further comprising the steps of:

initiating an emergency call to any of a group of registered emergency centers, whenever any of the life sign indicators detects a critical level; and

wherein said emergency call transmits any of a group of data files information associated with the user, including identification of the user, personal medical data file of the user, the measured set of life sign parameters of the user and location of the user; and/or

wherein the method further comprises the step of:

communicating, via any one of a group of communication means, with any of a group of service providers including banks, credit card companies, clinics, hospitals and medical insurance companies, municipal and utility entities and websites frequently accessed by said user thereby allowing said user to access and manage said user's personal data and documentation files stored by said group of service providers.

8. The method of claim 6, wherein said apparatus further comprises an emergency button in communication with said processor and said communication and data connection means, the method further comprising the steps of:

when said emergency button is activated, an emergency medical data file is displayed to the emergency button apparatus activating person and/or a call is initiated between said apparatus and any of a group of registered emergency centers; and

said emergency call transmitting any of a group of data files information associated with the user, including identification data of the user, the personal medical data file of the user, and location of the user; and/or

wherein the apparatus further comprises a magnetic strip element, the method further comprising the step of:

after positive authentication of said user's personal biological identification parameters, activating said magnetic strip thereby allowing said magnetic strip to be read by any of group of devices including a credit card reader, an ATM, a point of sale, a magnetic strip or near field communication reading device (NFC); and/or

wherein the apparatus further comprises a power charging and data backup device, said device comprising a charging and power unit, an electronic sub unit and a mass memory solid-state memory unit, the method further comprising the steps of:

comparing the memory content of said apparatus first storage unit to the memory content of said mass memory solid-state memory unit; and

if the first storage unit of the apparatus lacks data, updating the first storage unit with the last version of the data stored within the solid-state memory unit; and

if said solid-state memory unit of said device lacks data, updating the solid-state memory unit of said device with the last version of the data stored within said apparatus's solid-state memory unit.

9. The method of claim 6, wherein each of said plurality of unique users is in communication with a system manager, said system manager managing a remote centralized data communication storage and management system of said plurality of unique users, the method further comprising the steps of:

a. said system manager registering each unique user and storing the personal ID data file of each unique user in a memory sub-system connected to said centralized system; and

b. said registration further includes the step wherein said system manager generates for each system user N pairs of two different randomly selected characters strings, each of said strings is a combination of n alphanumeric characters in length; and

c. said system manager storing said N pairs in said system memory sub-system and sending said n characters strings pairs to be stored in said unique user personal identification unit memory module; and

d. said personal identification unit generating a secret access code of L alphanumeric characters to be further stored in said system memory within a special partition containing the list of said secret access codes for said plurality of unique users without assigning any identification or link between the associated users to his registered secret access code.

10. The method of claim 9, wherein after registration and upon normal initiation of communication between said system manager and each unique user, said system manager further communicating with said unique user and first comparing said unique user's ID data file and said personal identification unit unique embedded characterizing serial number stored in the unique user's personal identification unit with the corresponding user's ID and personal identification data stored in said memory sub-system; and

if the two sets of identification data match;

i. said system manager sending a first string of said stored N strings of coded alphanumeric data, to said user's personal identification unit; and

ii said user personal identification unit responding with the second matching string from the same stored pair of coded alphanumeric data uniquely associated with said user personal identification unit: and

iii said system manager comparing the received second string of coded alphanumeric data with a second string of coded alphanumeric data pre-stored in the memory sub-system; and

iv. said system manager comparing for consecutive M out of N times the received additional different strings of coded alphanumeric data pre-stored in the memory of said personal identification unit associated with said unique user with the additional strings of coded alphanumeric data pre-stored in the memory of sub-system; and

v. if all M strings of coded alphanumeric data match, then said system manager declares authenticating of said unique user and permitting said unique user access to said system.

11. The method of claim 9, further comprising the steps of:

after the step of authenticating, said system manager connecting the personal identification unit of said unique user with any of a group of emergency centers or service providers registered with said system manager at the request of said user personal identification unit; and

in the case of a medical emergency call initiated by said personal identification unit, transferring the user's updated medical data to the emergency center.

12. A system for managing personal and secured data and documentation files of a plurality of unique users, the system comprising:

a. a system manager for managing and updating personal data of said system plurality of unique users and for full-duplex communication with each of said plurality of unique users and a plurality of service providers; and

b. a storage system connected to said system manager to store updated personal data of each of said plurality of unique users; and

c. a plurality of personal identification units, each of said personal identification units being associated with a unique user, each unique user being registered with said system manager, each of said personal identification units comprising a storage unit configured to store the

personal ID data file of each unique user and a plurality of biometric sensors for reading a plurality of personal biometric biological identification parameters of the user holding the apparatus, said plurality of biometric sensors being integrated within the personal identification units and at least one life signs detector, integrated within said personal identification units, said life signs detector being configured to measure and record at least one of said user's life sign parameters; and

d. a plurality of computer hosts and cellular phones in communication with said system manager, enabling the direct connection by said system manager with said plurality of unique users through their corresponding personal identification unit; and

**e.** a plurality of registered emergency centers and a plurality of registered service providers in communication with said system manager, said plurality of service providers including banks, credit card companies, insurance companies, clinics, hospitals and medical insurance companies, government, municipal and utility entities and selected websites frequently accessed by said plurality of users;

wherein said system manager's access to and communication with the personal data and documentation files stored in said personal identification units associated with each said unique user and to the personal data and documentation files stored by said group of service providers is only enabled after positive authentication of each of said unique user's personal biometric biological identification parameters by said authentication unit and measuring the normal measured output of each one of said user's life sign parameters;

wherein at least one of said plurality of biometric sensors is a life signs detector, said life signs detector being configured to measure and record at least one of said user's life sign parameters; and

wherein said at least one of said user's life sign parameters is measured by any of a group of life sign indicators including a body pulse rate measurement indicator, a body $O_2$ saturation level indicator, a body heat

measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator.

13. The system according to claim 12, wherein each of said plurality of personal identification units comprises:

i. a sensor module comprising a plurality of biometric sensors for reading a plurality of personal biometric biological identification parameters of the user holding the of personal identification units, said of personal identification units being uniquely identified with said user; and

ii. a processor in communication with said sensor module for processing said personal biological identification parameters and for processing and managing the personal and secured data and documentation files associated with said user; and

iii. an authentication unit in communication with the processor configured to receive and authenticate the identity of said user by comparing said user's personal biological identification parameters read or any weighted combination thereof, by the sensor module and processed by the processor, with a pre-recorded set of personal biological identification parameters or any weighted combination thereof stored in said authentication unit; and

iv. an encryption module in communication with said processor for the encryption plus compression and/or decompression plus decryption of said user's data files; and

v. a storage unit in communication with said processor and said encryption module for the storage of said user's data and documentation files; and

vi. communication and data connection means in communication with said processor for connecting said plurality of personal identification units with said system manager and plurality of service providers; through the use of any device from a group of connection and communication devices including a data interface connector attached to a host computer, a Mini USB, a compatible industrial data interface connector attached to a cellular

phone, a near field wireless communication interface, a Bluetooth communication interface, a magnetic reader interface, and a smart card reader based on a contact-less communication interface using induction or RF communication

14. The system according to claim 13, wherein said system manager is configured:

to communicate with said personal identification units to compare the user's ID data file stored in the unique user's personal identification units with the corresponding identification data stored in said storage unit, and

if the two sets of identification data match, then said system manager is configured to initiate a further level of security identification prior to full communication and data updating capability being enabled between said system manager and said user personal identification unit; and

wherein said further level of security identification comprises said system manager sending a first string of coded alphanumeric data uniquely associated with said user personal identification unit to said user personal identification unit, said personal identification unit responding with a second string of coded alphanumeric data uniquely associated with said user personal identification unit, and said system manager verifying the received second string of coded alphanumeric data with a second string of coded alphanumeric data pre-stored in the memory sub-system; and

said system manager comparing for full matching for N consecutive times received additional different strings of coded alphanumeric data pre-stored in the memory of said personal identification unit associated with said unique user with counter generated additional strings of coded alphanumeric data pre-stored in the memory of sub-system; and/or

wherein said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with the user holding his unique personal identification units and in the event that a change occurs in any of the plurality of personal biological biometric identification parameters, access to the stored personal data files is denied

and the operation of said identification units is completely shut down; and/or

wherein each personal identification unit further comprises an emergency button in communication with said processor and said communication and data connection means module;

wherein the personal identification unit is configured to transfer any of a group of data files containing information associated with the user, including files such as the identification data of the user, personal medical data file of the user, the measured set of life sign parameters of the user, financial, insurance and banking data files associated with the user and an updated location of the user; and

wherein the personal identification unit is configured to initiate an emergency call to any of said plurality of registered emergency centers, whenever said emergency button is activated or whenever any of the group of life sign indicators detects a critical level.

15. The system of claim 12, wherein said system, further comprises:

a computerized call center configured to receive phone calls or emergency voice and data messages from any of said plurality of registered emergency centers and a plurality of registered service providers and to communicate with any of said plurality of cellular phone and host computers; and

wherein said call center is configured to communicate the user's location coordinates to an emergency rescue team and simultaneously said call center is configured to communicate with any of said plurality of registered emergency centers and service providers to receive said user's updated medical data and to transfer said data to and from the user's personal identification unit.

Europäisches Patentamt
European Patent Office
Office européen des brevets

# Acknowledgement of receipt

We hereby acknowledge receipt of the following subsequently filed document(s):

| | |
|---|---|
| Submission number | 2107292 |
| Application number | EP11752936.2 |
| Date of receipt | 29 April 2013 |
| Receiving Office | European Patent Office, The Hague |
| Your reference | P105633EP00 |
| Applicant | All applicants as on file |
| Documents submitted | package-data.xml<br>epf1038.pdf (1 p.)<br>SUBCLMS-2.pdf\p105633ep00comparisontable.pdf (1 p.)<br>SUBCLMS-1.pdf\p105633ep00epolletter161.pdf (1 p.)<br>ep-sfd-request.xml<br>CLMS-1.pdf\p105633ep00claimscleancopy.pdf (14 p.)<br>CLMS-HWA-1.pdf\p105633ep00trackedclaims.pdf (15 p.) |
| Submitted by | CN=P. Coyle 25345,O=FRKelly,C=IE |
| Method of submission | Online |
| Date and time receipt generated | 29 April 2013, 16:28 (CEST) |
| Message Digest | 31:40:B3:AB:49:87:CC:47:2C:BF:E0:74:3D:22:43:A3:AA:62:26:40 |

**Correction by the EPO of errors in debit instructions filed by eOLF**
Errors in debit instructions filed by eOLF that are caused by the editing of Form 1038E entries or the continued use of outdated software (all forms) may be corrected automatically by the EPO, leaving the payment date unchanged (see decision T 152/82, OJ EPO 1984, 301 and point 6.3 ff ADA, Supplement to OJ EPO 10/2007).

/European Patent Office/

Application No.: 11752936.2

The search has started on 13.01.14 (see Notice from the European Patent Office dated 03/2013, OJ EPO 2013, 153).

**Receiving Section**

Europäisches Patentamt
European Patent Office
Office européen des brevets

# SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application Number
EP 11 75 2936

## DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document with indication, where appropriate, of relevant passages | Relevant to claim | CLASSIFICATION OF THE APPLICATION (IPC) |
|---|---|---|---|
| X<br>Y | US 2009/083847 A1 (FADELL ANTHONY [US] ET AL) 26 March 2009 (2009-03-26)<br>* page 1, paragraphs 5, 8 *<br>* page 2, paragraphs 24,28,29 *<br>* page 3, paragraphs 31,33 *<br>* page 5, paragraph 57 *<br>* figure 1 *<br>----- | 1,6<br>2,7 | INV.<br>G06F21/32<br>G06F21/62 |
| X | US 6 957 337 B1 (CHAINER TIMOTHY JOSEPH [US] ET AL) 18 October 2005 (2005-10-18)<br>* column 4, line 26 - column 6, paragraph 46 *<br>----- | 1,6 | |
| Y | US 5 229 764 A (MATCHETT NOEL D [US] ET AL) 20 July 1993 (1993-07-20)<br>* column 5, line 1 - line 15 *<br>----- | 2,7 | |

TECHNICAL FIELDS SEARCHED (IPC)

G06F

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

| Place of search | Date of completion of the search | Examiner |
|---|---|---|
| The Hague | 24 January 2014 | Arbutina, Ljiljana |

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

1

EPO FORM 1503 03.82 (P04C04)

## CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing claims for which payment was due.

☐ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for those claims for which no payment was due and for those claims for which claims fees have been paid, namely claim(s):

☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for those claims for which no payment was due.

## LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

☐ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

☐ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.

☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:

☐ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:

☒ The present supplementary European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims (Rule 164 (1) EPC).

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. claims: 1, 2, 6(completely); 7(partially)

   Preventing unauthorized use of a device

   ---

2. claims: 11(completely); 3, 7, 8(partially)

   Providing data to emergency services

   ---

3. claim: 3(partially)

   How to use keyboard and display of the host device

   ---

4. claims: 4, 8(all partially)

   Providing magnetic strip communication

   ---

5. claim: 4(partially)

   Use of RFID technology

   ---

6. claims: 4, 5, 8(all partially)

   Providing data backup/synchronization

   ---

7. claim: 5(partially)

   Enabling the user to locate a device

   ---

8. claims: 9, 10

   Device authentication

   ---

9. claims: 12-15

   Implementing centralized management of personal data

   ---

1.0. The application lacks unity within the meaning of Article EPC for the following reasons:
1.1. The prior art has been identified as D1: US2009083847, which discloses in accordance with all the features of claim 1 (the references in parentheses applying to this document, the square brackets indicting added subject-matter in the claim)

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

an apparatus for storing and managing personal and secured data and documentation files associated with a specific user, comprising:
a plurality of biometric sensors for reading a plurality of personal biological [biometric] identification parameters of the user holding the apparatus, [said plurality of biometric sensors being integrated within the apparatus] (par.[28]);
at least one life signs detector integrated within the apparatus, said life signs detector being configured to measure and record at least one of said user's life sign parameters (par.[57];
a first storage unit for the storage of said user's data and documentation files (lines 1-5 of par.[24]);
an authentication unit [comprising a second storage unit, with said second storage unit configured to store a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user], wherein said authentication unit is configured to compare the plurality of personal biological biometric identification parameters of the user holding the apparatus [or any weighted combination thereof] with the pre-recorded set of personal biological biometric identification parameters [or any weighted combination thereof] stored in said second storage unit (fig.1, Authentication System; lines 1-4 of par.[41]; lines 11-13 of par.[79];
a processor in communication with said plurality of biometric sensors, said first storage unit and said authentication unit (fig.1, Processor);
wherein access to the personal data and documentation files stored in said first storage unit is only enabled after said authentication unit positively matches each of the plurality of personal biological [biometric] identification parameters of the user holding the apparatus [or any weighted combination thereof] with the pre-recorded set of personal biological identification parameters [stored in said second storage unit] (pr.[28] and [95]); and
[wherein, whenever any of said at least one life signs detector detects a critical level of said user measured life sign parameters, the apparatus is configured to prevent access to said user's personal data and documentation files stored in said first storage unit] (although this subject-matter represents added subject-matter, it is noted that it is disclosed in par.[57] and [95]).
1.1.1. The cited paragraphs of D1 disclose also the corresponding features of method claim 6, with exception of encryption unit, which is present in claim 1. However, encryption being a well-known technique, it cannot be considered to be a subject of an invention. For the same reason, it cannot form a single general inventive concept for claims 7-11 which are dependent on claim 6.
1.1.2.Considering the system claim 12, D1 discloses, in the above cited paragraphs, all the features of the personal identification unit, and, because the electronic device in D1 is a telephone/Internet enabled, see par.[50] and [51], D1 implicitly discloses a system manager with a database related to a plurality of cellular phones and their owners. It is noted that, in D1, the personal identification unit is integrated with the phone.

1.2. From the comparison between the first invention (see claims 2 and 7)

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

and document D1, the following features can be seen as making a contribution over the prior art:
said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied and the operation of the apparatus is completely shut down.
The technical effect of this difference is that an unauthorized user is detected and prevented access. Therefore, the objective problem to be solved by the first invention can be summarized as how to prevent unauthorized use of a device.
It is noted here that the other part of claim 2 consists in enumerating various types of life sign detectors and as such is not considered to be a subject of an invention.

1.3. From the comparison between the second invention (see claims 3, 7, 8 and 11) and document D1, the following features can be seen as making a contribution over the prior art:
whenever life sign indicator detects a critical level, or an emergency button of the apparatus is being activated, communication is initiated between said apparatus and any of a group of registered emergency centers, transmitting any of a group of data files containing information associated with the unique user of said apparatus.
The technical effect of this difference is that emergency services get information related to the user. Therefore, the objective problem to be solved by the second invention can be summarized as how to provide user related data to emergency services.

1.4. From the comparison between the third invention (see claim 3) and document D1, the following features can be seen as making a contribution over the prior art:
the apparatus comprises an integrated software module that automatically detects the operating system of the computer or cellular phone connected to said apparatus through one of said group of communicating devices through which the apparatus is connected, said computer or cellular phone having keyboard and display units associated therewith, thereby allowing the user to interact with said memory module and with said processing module of said apparatus via said keyboard and display units, whereby said computer or cellular phone is configured to utilize and interact with said memory module, said processing module and said sensor module of said apparatus.
The technical effect of this difference is that the keyboard and display of the host can be used, thereby simplifying the apparatus itself.
Therefore, the objective problem to be solved by the third invention can be summarized as how to enable using of the keyboard and display of another device.
It is noted here that the other parts of claim 3 consist use of data encryption and in enumerating various types of service providers and interfaces, and as such are not considered to be a subject of an invention.

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1.5. From the comparison between the fourth invention (see claims 4 and 8) and document D1, the following features can be seen as making a contribution over the prior art:
a magnetic strip element that is only activatable after positive authentication of said user's personal biological identification parameters; and wherein said magnetic strip is configured to be concealed within the apparatus and on activation configured to extend out of the apparatus for swiping and reading by any of group of devices including a credit card reader, ATM and point of sale magnetic strip reading device.
The technical effect of this difference is that apparatus can be connected to devices with a magnetic strip reader. Therefore, the objective problem to be solved by the fourth invention can be summarized as how to implement a magnetic strip interface.

1.6. From the comparison between the fifth invention (see claim 4) and document D1, the following features can be seen as making a contribution over the prior art:
an integrated digital data encoder/decoder and a RF transceiver module in communication with the processing module, said integrated digital data encoder/decoder and a RF transceiver module being configured to communicate with any of a group of external devices including RF operated credit card readers, ATM machines and electronic locks or gate/door opener remotely operated using RFID based techniques.
The technical effect of this difference is that the apparatus ca be recognized by the RFID technology compatible devices. Therefore, the objective problem to be solved by the fifth invention can be summarized as how to implement RFID technology.

1.7. From the comparison between the sixth invention (see claims 4, 5 and 8) and document D1, the following features can be seen as making a contribution over the prior art:
a power charging and data backup device in communication with the processing module of said apparatus, said device comprising: a charging and power sub module comprising a charging plug for connecting to the mains supply, an AC-DC converter, a power supply unit and a rechargeable backup battery, an electronic sub module comprising a micro processor, and a mass memory unit, wherein the memory module of said apparatus is in communication with the mass memory unit of said device, thereby to compare and synchronize the version of data stored in the memory module of said apparatus with the version of data stored in mass memory unit of said device.
The technical effect of this difference is that the apparatus gets charged and data updated. Therefore, the objective problem to be solved by the sixth invention can be summarized as how to charge the apparatus and update the data.

1.8. From the comparison between the seventh invention (see claim 5) and document D1, the following features can be seen as making a contribution over the prior art:
an activation sub-module comprising an electronic buzzer activator, a button connected to said buzzer activator and an RF transmitter connected

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

to said electronic buzzer activator , wherein on activating said buzzer button, said RF transmitter is configured to transmit a coded signal to the apparatus to enable the user to determine the location of the apparatus; and an integrated GPS module in communication with the processing module to precisely locate the geographical position of the apparatus.
The technical effect of this difference is that the device can be localized. Therefore, the objective problem to be solved by the seventh invention can be summarized as how to enable a user to locate a device.

1.9. Considering features of claim 9, D1 further discloses
each of plurality of unique users is in communication with a system manager, said system manager managing a remote centralized data communication storage and management system of said plurality of unique users, where said system manager is registering each unique user and storing the personal ID data file of each unique user in a memory sub-system connected to said centralized system (this is implicitly the infrastructure for telephones and Internet-enabled devices, see D1, par.[50] and 51].)
The remaining features of claim 9, namely generating and storing pairs of character strings and a secret access code, do not provide any technical effect, since the use of these strings is not clear from claim 9. They can be seen as making a contribution over the prior art in combination with features of claim 10, namely
comparing said unique user's ID data file and said personal identification unit unique embedded characterizing serial number stored in the unique user's personal identification unit with the corresponding user's ID and personal identification data stored in said memory sub-system; and if the two sets of identification data match;
i system manager sending a first string of said stored N strings of coded alphanumeric data, to said user's personal identification unit; and
ii said user personal identification unit responding with the second matching string from the same stored pair of coded alphanumeric data uniquely associated with said user personal identification unit: and
iii said system manager comparing the received second string of coded alphanumeric data with a second string of coded alphanumeric data pre-stored in the memory sub-system; and
iv. said system manager comparing for consecutive M out of N times the received additional different strings of coded alphanumeric data pre-stored in the memory of said personal identification unit associated with said unique user with the additional strings of coded alphanumeric data pre-stored in the memory of sub-system; and
v. if all M strings of coded alphanumeric data match, then said system manager declares authenticating of said unique user and permitting said unique user access to said system.
The technical effect of this difference is that the device is authenticated (it is noted here that the strings are stored in the device; therefore, a user is authenticated by authenticating the device). Therefore, the objective problem to be solved by the eighth invention can be summarized as how to authenticate a device.

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1.10. From the comparison between the ninth invention (see claim 12 and paragraph 1.1.2. here above) and document D1, the following features can be seen as making a contribution over the prior art:
said system manager's access to and communication with the personal data and documentation files stored in said personal identification units associated with each said unique user and to the personal data and documentation files stored by said group of service providers is only enabled after positive authentication of said unique user's personal biological identification parameters by said authentication unit.
The technical effect of this difference is the centralized management of personal data of the user. Therefore, the objective problem to be solved by the ninth invention can be summarized as how to provide centralized data management.
It is noted here that the other parts of claim 12 consist in enumerating various types of life sign detectors and service providers, and as such are not considered to be a subject of an invention.
1.11. The above analysis shows that the special technical features disclosed by the identified four inventions are not the same. Furthermore, a comparison of the objective problems shows that these objective problems are different and have no corresponding technical effect. Consequently, the technical relationship between the subject-matter of claims belonging to the four identified inventions, required by Rule 30, is lacking, and the requirement for the unity of invention referred to in Article 82 EPC is not fulfilled.

## ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 11 75 2936

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

24-01-2014

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2009083847 A1 | 26-03-2009 | AU 2008305338 A1 | 02-04-2009 |
| | | CN 101809581 A | 18-08-2010 |
| | | EP 2203865 A2 | 07-07-2010 |
| | | EP 2528010 A1 | 28-11-2012 |
| | | JP 2010541046 A | 24-12-2010 |
| | | JP 2013232197 A | 14-11-2013 |
| | | KR 20100074218 A | 01-07-2010 |
| | | KR 20110114732 A | 19-10-2011 |
| | | TW 200919255 A | 01-05-2009 |
| | | TW 201235880 A | 01-09-2012 |
| | | US 2009083847 A1 | 26-03-2009 |
| | | US 2009083850 A1 | 26-03-2009 |
| | | WO 2009042392 A2 | 02-04-2009 |
| US 6957337 B1 | 18-10-2005 | NONE | |
| US 5229764 A | 20-07-1993 | NONE | |

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

The examination is being carried out on the **following application documents**

**Description, Pages**

1-60 as published

**Claims, Numbers**

1-15 filed with entry into the regional phase before the EPO

**Drawings, Sheets**

1/9-9/9 as published

Reference is made to the following documents; the numbering will be adhered to in the rest of the procedure.

D1 US 2009/083847 A1 (FADELL ANTHONY [US] ET AL) 26 March 2009 (2009-03-26)

D2 US 5 229 764 A (MATCHETT NOEL D [US] ET AL) 20 July 1993 (1993-07-20)

**Added Subject-Matter**

1. The amendments filed with entry into the regional phase introduce subject - matter which extends beyond the content of the application as filed, contrary to Article 123(2) EPC, for the following reasons:

Claim 1:

1.1. Original claim 1 was drafted as

"Apparatus managing personal and secured data..."

whereas new claim 1 recites

"Apparatus for ... managing personal and secured data..."

This allows the reading "Apparatus *suitable* for ..." thus broadening the scope of the claim in such a way that it extends beyond the content of the application as originally filed.

1.2. In the introductory part of claim 1, it is not clear to what refers the term "associated with a specific user" (Art. 84 EPC); it can be interpreted as referring to the apparatus, or data and files.

According to the originally filed claim, last two lines of feature (a), it is the apparatus that is associated with the user. Thus, new wording of the claim allows broader interpretation, where the apparatus *is not* associated with the user.

1.3. The first feature introduces terms (underlined):

1) "biologic biometric", and

2) "biometric sensors being integrated within the apparatus".

The applicant does provide support for these amendments. Moreover, they appear to be redundant, infringing also Art. 84 EPC:

for 1) it is not clear what would be the difference between biometric and biologic, and

for 2) it is not clear what is the additional features of sensors being integrated within the apparatus versus apparatus comprising sensors.

1.4. The feature

"a first storage unit for storage of said user's data and documentation files"

appears to replace the originally drafted feature

"a memory module in communication with said processing module and said encryption module for the storage of said user's data and documentation files",

having different scope. The applicant did not provide any support for this amendment.

1.5. The feature relating to the authentication unit has been amended in two ways:

1) addition of "a second storage unit, configured to store ... biometric identification parameters", and

2) "weighted combination".

The applicant did not provide, and the examiner could not identify, any support for these amendments. Considering amendment 2) the description discloses, on page 28, lines 23-25, "combining the measured results of the multi sensors tests output to a final go/no-go", but there is no weighted combination disclosed. Considering amendment 1), the description does disclose, in last paragraph on page 28, a (memory) module 150 in relation to (authentication) module 140, but module 130 does not contain biometric identification parameters. The description further discloses, lines 24-26 on page 30, that "Module 140 will store the registered user's original, initial registration step, bio sensors measured output for reference", but it does not disclose *where* it will store this information.

Therefore, the amendments identified here above are not present in the application as filed.

1.6. The feature referring to enabling access introduces terms "each of the plurality", "biometric", "weighted combination", and "said second storage unit". The applicant did not provide, and the examiner could not identify, any support for these amendments.

1.7. The applicant indicated originally filed claims 1 and 3 as basis for new claim 1. However, the last feature of present claim 1, namely, "whenever any of said life signs detectors detects a critical level... the apparatus is configured to prevent access..." is not present neither in claim 1 nor in claim 3 in the originally filed set of claims.

Claim 2:

1.8. "Weighted combination" is a new feature. The applicant did not provide, and the examiner could not identify, any support for this amendment.

1.9. In the original set of claims, claim 2 was dependent on claim 1, and claim 4 was dependent on claim 3 which was dependent on claim 1. Therefore, new claim 2 introduces combinations of features that was not present in the application as originally filed: one is the combination of features of new claim 2 with the new feature of claim 1 (life sign detector), and the other combination is the "and" part of the wording "and/or".

Claim 3:

1.10. The applicant cited originally filed claims 5-11 and 17 as basis for new claim 3.

In the original set of claims, claims 5, 6,7, 8, and 11 were dependent on claim 1, in separate trees. Therefore, new claim 3 introduces combinations of features that was not present in the application as originally filed: one is the combination of features of new claim 3 with the new feature of claim 1 (life sign detector), and the other combination is the "and" part of the wording "and/or".

1.11. The examiner could not find the support for "medical or security centers", "request for medical help or police/security intervention", and "measured physical data parameters file of the user" in claims 5-11 and 17.

Claim 4:

1.12. The applicant cited originally filed claims 13, 15 and 16 as basis for new claim 4.

In the original set of claims, claims 13 and 15 were dependent on claim 1, in separate trees. Therefore, new claim 4 introduces combinations of features that was not present in the application as originally filed: one is the combination of features of new claim 4 with the new feature of claim 1 (life sign detector), and the other combination is the "and" part of the wording "and/or".

1.13. The examiner could not find support for addition of "biological biometric identification", "positive normal non critical measured output... life sign parameters", and for change from RF to wireless, in claims 13, 15 and 16.

Claim 5:

1.14. The applicant cited originally filed claims 18, 19 and 20 as basis for new claim 5.

In the original set of claims, claims 18, 19 and 20 were dependent on claim 1, in separate trees. Therefore, new claim 5 introduces combinations of features that was not present in the application as originally filed: one is the combination of features of new claim 5 with the new feature of claim 1 (life sign detector), and the other combination is the "and" part of the wording "and/or".

Claim 6:

1.15. "Weighted combination" is a new feature. The applicant did not provide, and the examiner could not identify, any support for this amendment.

Claim 7:

1.16. The applicant cited originally filed claims 22 and 23 as basis for new claim 7. The examiner further notes that claim 25 appears to be basis for the last feature.

In the original set of claims, claims 22, 23 and 25 were dependent on claim 21, in separate trees. Therefore, new claim 7 introduces combinations of features that was not present in the application as originally filed: one is the combination of features of new claim 7 with the new feature of claim 6 (life sign detector), and the other combination is the "and" part of the wording "and/or".

1.17. The examiner could not find support for addition of "biological biometric identification", and "normal output reading of said at least one of said life sign detectors" in claims 22,23 and 25.

Claim 8:

1.18. The applicant cited originally filed claims 24, 26 and 27 as basis for new claim 8.

In the original set of claims, claims 24, 26 and 27 were dependent on claim 21, in separate trees. Therefore, new claim 8 introduces combinations of features that was not present in the application as originally filed: one is the combination of features of new claim 8 with the new feature of claim 6 (life sign detector), and the other combination is the "and" part of the wording "and/or".

1.19. The examiner could not find support for addition of "emergency medical data is displayed to the emergency button apparatus activating person" in claims 24,26 and 27.

Claim 9:

1.20. In the original set of claims, claim 28 was dependent on claim 21, and the new feature of claim 6 (life sign detector) was in claim 23, which was also dependent on claim 21. Therefore, new claim 9 introduces combinations of features that was not present in the application as originally filed

Claim 12:

1.21. Originally filed claim 32 appears to be basis for the new claim 12. However, the originally filed claim 32 does not disclose "full duplex communication" and "plurality of service provides", as recites feature a) of present claim 12, nor does it disclose life sign detector, as recited in features c) and e) of present claim 12.

Claim 13:

1.22. Originally filed claim 33 is the basis for the new claim 12. However, the originally filed claim 32 does not disclose biometric biological identification, weighted combination, nor does it disclose the last feature of claim 13, namely, "through the use of any device from a group of connection and communication devices including ...".

Claim 14:

1.23. The applicant cited originally filed claims 34-36 as basis for new claim 14.

In the original set of claims, claims 34-36 were dependent on claim 33, in separate trees. Therefore, new claim 14 introduces combinations of features that was not present in the application as originally filed.

1.24. Claim 14 introduces terms "biological biometric identification", "trancieve", and "financial, insurance, and banking data files", not present in claims 34-36.

**Non - Unity**

2.0. The application lacks unity within the meaning of Article 82 EPC for the following reasons:

2.1. The prior art has been identified as D1, which discloses in accordance with all the features of claim 1 (the references in parentheses applying to this document, the square brackets indicting added subject-matter in the claim)

an apparatus for storing and managing personal and secured data and documentation files associated with a specific user, comprising:

a plurality of biometric sensors for reading a plurality of personal biological [biometric] identification parameters of the user holding the apparatus, [said plurality of biometric sensors being integrated within the apparatus] (par.[28]);

at least one life signs detector integrated within the apparatus, said life signs detector being configured to measure and record at least one of said user's life sign parameters (par.[57];

a first storage unit for the storage of said user's data and documentation files (lines 1-5 of par.[24]);

an authentication unit [comprising a second storage unit, with said second storage unit configured to store a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user], wherein said authentication unit is configured to compare the plurality of personal biological biometric identification parameters of the user holding the apparatus [or any weighted combination thereof] with the pre-recorded set of personal biological biometric identification parameters [or any weighted combination thereof] stored in said second storage unit (fig.1, Authentication System; lines 1-4 of par.[41]; lines 11-13 of par.[79]);

a processor in communication with said plurality of biometric sensors, said first storage unit and said authentication unit (fig.1, Processor);

wherein access to the personal data and documentation files stored in said first storage unit is only enabled after said authentication unit positively matches each of the plurality of personal biological [biometric] identification parameters of the user holding the apparatus [or any weighted combination thereof] with the pre-recorded set of personal biological identification parameters [stored in said second storage unit] (pr. [28] and [95]); and

[wherein, whenever any of said at least one life signs detector detects a critical level of said user measured life sign parameters, the apparatus is configured to prevent access to said user's personal data and documentation files stored in said first storage unit] (although this subject-matter represents added subject-matter, it is noted that it is disclosed in par.[57] and [95]).

2.1.1. The cited paragraphs of D1 disclose also the corresponding features of method claim 6, with exception of encryption unit, which is present in claim 1. However, encryption being a well-known technique, it cannot be considered to be a subject of an invention. For the same reason, it cannot form a single general inventive concept for claims 7-11 which are dependent on claim 6.

2.1.2.Considering the system claim 12, D1 discloses, in the above cited paragraphs, all the features of the personal identification unit, and, because the electronic device in D1 is a telephone/Internet enabled, see par.[50] and [51], D1 implicitly discloses a

system manager with a database related to a plurality of cellular phones and their owners. It is noted that, in D1, the personal identification unit is integrated with the phone.

2.2. From the comparison between the first invention (see claims 2 and 7) and document D1, the following features can be seen as making a contribution over the prior art:

said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied and the operation of the apparatus is completely shut down.

The technical effect of this difference is that an unauthorized user is detected and prevented access. Therefore, the objective problem to be solved by the first invention can be summarized as how to prevent unauthorized use of a device.

It is noted here that the other part of claim 2 consists in enumerating various types of life sign detectors and as such is not considered to be a subject of an invention.

2.3. From the comparison between the second invention (see claims 3, 7, 8 and 11) and document D1, the following features can be seen as making a contribution over the prior art:

whenever life sign indicator detects a critical level, or an emergency button of the apparatus is being activated, communication is initiated between said apparatus and any of a group of registered emergency centers, transmitting any of a group of data files containing information associated with the unique user of said apparatus.

The technical effect of this difference is that emergency services get information related to the user. Therefore, the objective problem to be solved by the second invention can be summarized as how to provide user related data to emergency services.

2.4. From the comparison between the third invention (see claim 3) and document D1, the following features can be seen as making a contribution over the prior art:

the apparatus comprises an integrated software module that automatically detects the operating system of the computer or cellular phone connected to said apparatus through one of said group of communicating devices through which the apparatus is connected, said computer or cellular phone having keyboard and display units

associated therewith, thereby allowing the user to interact with said memory module and with said processing module of said apparatus via said keyboard and display units, whereby said computer or cellular phone is configured to utilize and interact with said memory module, said processing module and said sensor module of said apparatus.

The technical effect of this difference is that the keyboard and display of the host can be used, thereby simplifying the apparatus itself. Therefore, the objective problem to be solved by the third invention can be summarized as how to enable using of the keyboard and display of another device.

It is noted here that the other parts of claim 3 consist use of data encryption and in enumerating various types of service providers and interfaces, and as such are not considered to be a subject of an invention.

2.5. From the comparison between the fourth invention (see claims 4 and 8) and document D1, the following features can be seen as making a contribution over the prior art:

a magnetic strip element that is only activatable after positive authentication of said user's personal biological identification parameters; and wherein said magnetic strip is configured to be concealed within the apparatus and on activation configured to extend out of the apparatus for swiping and reading by any of group of devices including a credit card reader, ATM and point of sale magnetic strip reading device.

The technical effect of this difference is that apparatus can be connected to devices with a magnetic strip reader. Therefore, the objective problem to be solved by the fourth invention can be summarized as how to implement a magnetic strip interface.

2.6. From the comparison between the fifth invention (see claim 4) and document D1, the following features can be seen as making a contribution over the prior art:

an integrated digital data encoder/decoder and a RF transceiver module in communication with the processing module, said integrated digital data encoder/ decoder and a RF transceiver module being configured to communicate with any of a group of external devices including RF operated credit card readers, ATM machines and electronic locks or gate/door opener remotely operated using RFID based techniques.

The technical effect of this difference is that the apparatus ca be recognized by the RFID technology compatible devices. Therefore, the objective problem to be solved by the fifth invention can be summarized as how to implement RFID technology.

2.7. From the comparison between the sixth invention (see claims 4, 5 and 8) and document D1, the following features can be seen as making a contribution over the prior art:

a power charging and data backup device in communication with the processing module of said apparatus, said device comprising: a charging and power sub module comprising a charging plug for connecting to the mains supply, an AC-DC converter, a power supply unit and a rechargeable backup battery, an electronic sub module comprising a micro processor, and a mass memory unit, wherein the memory module of said apparatus is in communication with the mass memory unit of said device, thereby to compare and synchronize the version of data stored in the memory module of said apparatus with the version of data stored in mass memory unit of said device.

The technical effect of this difference is that the apparatus gets charged and data updated. Therefore, the objective problem to be solved by the sixth invention can be summarized as how to charge the apparatus and update the data.

2.8. From the comparison between the seventh invention (see claim 5) and document D1, the following features can be seen as making a contribution over the prior art:

an activation sub-module comprising an electronic buzzer activator, a button connected to said buzzer activator and an RF transmitter connected to said electronic buzzer activator , wherein on activating said buzzer button, said RF transmitter is configured to transmit a coded signal to the apparatus to enable the user to determine the location of the apparatus; and an integrated GPS module in communication with the processing module to precisely locate the geographical position of the apparatus.

The technical effect of this difference is that the device can be localized. Therefore, the objective problem to be solved by the seventh invention can be summarized as how to enable a user to locate a device.

2.9. Considering features of claim 9, D1 further discloses

each of plurality of unique users is in communication with a system manager, said system manager managing a remote centralized data communication storage and management system of said plurality of unique users, where said system manager is registering each unique user and storing the personal ID data file of each unique user in a memory sub-system connected to said centralized system (this is implicitly the infrastructure for telephones and Internet-enabled devices, see D1, par.[50] and 51].)

The remaining features of claim 9, namely generating and storing pairs of character strings and a secret access code, do not provide any technical effect, since the use of these strings is not clear from claim 9. They can be seen as making a contribution over the prior art in combination with features of claim 10, namely

comparing said unique user's ID data file and said personal identification unit unique embedded characterizing serial number stored in the unique user's personal identification unit with the corresponding user's ID and personal identification data stored in said memory sub-system; and if the two sets of identification data match;

i system manager sending a first string of said stored N strings of coded alphanumeric data, to said user's personal identification unit; and

ii said user personal identification unit responding with the second matching string from the same stored pair of coded alphanumeric data uniquely associated with said user personal identification unit: and

iii said system manager comparing the received second string of coded alphanumeric data with a second string of coded alphanumeric data pre-stored in the memory sub-system; and

iv. said system manager comparing for consecutive M out of N times the received additional different strings of coded alphanumeric data pre-stored in the memory of said personal identification unit associated with said unique user with the additional strings of coded alphanumeric data pre-stored in the memory of sub-system; and

v. if all M strings of coded alphanumeric data match, then said system manager declares authenticating of said unique user and permitting said unique user access to said system.

The technical effect of this difference is that the device is authenticated (it is noted here that the strings are stored in the device; therefore, a user is authenticated by authenticating the device). Therefore, the objective problem to be solved by the eighth invention can be summarized as how to authenticate a device.

2.10. From the comparison between the ninth invention (see claim 12 and paragraph 2.1.2. here above) and document D1, the following features can be seen as making a contribution over the prior art:

said system manager's access to and communication with the personal data and documentation files stored in said personal identification units associated with each said unique user and to the personal data and documentation files stored by said group of service providers is only enabled after positive authentication of said unique user's personal biological identification parameters by said authentication unit.

The technical effect of this difference is the centralized management of personal data of the user. Therefore, the objective problem to be solved by the ninth invention can be summarized as how to provide centralized data management.

It is noted here that the other parts of claim 12 consist in enumerating various types of life sign detectors and service providers, and as such are not considered to be a subject of an invention.

2.11. The above analysis shows that the special technical features disclosed by the identified four inventions are not the same. Furthermore, a comparison of the objective problems shows that these objective problems are different and have no corresponding technical effect. Consequently, the technical relationship between the subject-matter of claims belonging to the four identified inventions, required by Rule 30, is lacking, and the requirement for the unity of invention referred to in Article 82 EPC is not fulfilled.

3.0. As the applicant has not had a search report drawn up on other inventions (Rule 64 EPC), the application will be prosecuted on the basis of the invention in respect of which a search has already been carried out, in other words the invention first mentioned in the claims. The applicant should therefore limit the application to the invention searched and excise those parts of the application relating to the other inventions.

The subject-matter to be excised may be made the subject of one or more divisional applications according to Rule 36 EPC.

**Patentability**

4.0. The present application does not meet the requirements of Article 52(1) EPC because the subject-matter of claim 1 is not new within the meaning of Article 54(1) and (2) EPC, and the subject-matter of claim 6 not inventive in the sense of Artice 56 EPC, see par.2.1 and 2.1.1. here above.

4.1. Considering the first invention, see par.2.2 here above, the problem of preventing unauthorized use of a device was solved in D2, see col.5, lines 14-15, by using the same features as claims 2 and 7, namely,

the plurality of biometric sensors continuously reading a plurality of personal biological identification parameters associated with said user holding the apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied and the operation of the apparatus is completely shut down

see D1, col.4, line 61 - col.5, line 6. Therefore, these features cannot be considered as having inventive contribution over the prior art.

**Clarity**

5.0. The last two features of claim 1 are drafted in a form of a method step, thereby rendering the category, and as a consequence, the scope of said claim unclear, contrary to requirements of Article 84 EPC.

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
Postbus 5818
2280 HV RIJSWIJK
NETHERLANDS
Tel. +31 (0)70 340-2040
Fax +31 (0)70 340-3016

**For any questions about this communication:**
Tel.:+31 (0)70 340 45 00

Coyle, Philip Aidan
F. R. Kelly & Co.
27 Clyde Road
Ballsbridge
Dublin 4
IRLANDE

Date
05.02.14

| Reference | Application No./Patent No. |
|---|---|
| p105633ep00 | 11752936.2 - 1957 / 2545485 PCT/IB2011051002 |

Applicant/Proprietor
OS - New Horizon Personal Computing Solutions Ltd.

## Communication

The extended European search report is enclosed.

The extended European search report includes, pursuant to Rule 62 EPC, the supplementary European search report (Art. 153(7) EPC) and the European search opinion.

Copies of documents cited in the European search report are attached.

☑ 0 additional set(s) of copies of such documents is (are) enclosed as well.

**Refund of the search fee**
If applicable under Article 9 Rules relating to fees, a separate communication from the Receiving Section on the refund of the search fee will be sent later.

Should you wish to further prosecute this application in the examination phase, your attention is drawn to the provisions of Rule 70a EPC. An invitation to respond to the extended European search report will be issued shortly (R. 70(2) EPC).

Europäisches Patentamt • European Patent Office • Office européen des brevets

EPO Form 1507S 06.12

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
Postbus 5818
2280 HV RIJSWIJK
NETHERLANDS
Tel. +31 (0)70 340-2040
Fax +31 (0)70 340-3016

**For any questions about this communication:**
Tel.:+31 (0)70 340 45 00

Coyle, Philip Aidan
F. R. Kelly & Co.
27 Clyde Road
Ballsbridge
Dublin 4
IRLANDE

Date: 21.02.14

| Reference | Application No./Patent No. |
|---|---|
| p105633ep00 | 11752936.2 - 1957 / 2545485 PCT/IB2011051002 |

Applicant/Proprietor
OS - New Horizon Personal Computing Solutions Ltd.

**Communication pursuant to Rules 70(2) and 70a(2) EPC**

A supplementary European search report has been drawn up concerning the above-identified European patent application (publication number: 2545485).

Since the request for examination has been filed (R. 70(1), 159(1)(f), Art. 94(1) EPC) prior to the transmission of the supplementary European search report, you are hereby invited to indicate within

**six months**

of notification of this communication whether you wish to proceed further with the European patent application.

If you do not indicate in due time that you wish to proceed further with the European patent application, it **will be deemed to be withdrawn** (R. 70(3) EPC).

You are invited, within the above-mentioned six-month period, to comment on the objections raised in the opinion accompanying the European search report and/or to file any amendments to the description, claims and drawings correcting any deficiencies noted in the opinion (R. 70a(2), R. 137(2) EPC; Guidelines for Examination in the EPO, B-XI, 8).

If filing amendments, you must identify them and indicate the basis for them in the application as filed. Failure to meet either requirement may lead to a communication from the Examining Division requesting that you correct this deficiency (R. 137(4) EPC).

Should the reply to the invitation pursuant to Rule 70a(2) EPC be filed in an admissible non-EPO language, a translation is to be submitted within one month of its filing (R. 6(2) EPC).

Should you not comply with this invitation within the time limit, the application **will be deemed to be withdrawn** in accordance with Rule 70a(3) EPC.

**Receiving Section**

Europäisches Patentamt • European Patent Office • Office européen des brevets

**Registered letter**
EPO Form 1224 11.12 (RTB/ESOP01=N) DMEX

Europäisches Patentamt
European Patent Office
Office européen des brevets

# Letter accompanying subsequently filed items


Representative:

**Mr Paul Keane**
**FRKELLY**
**27 Clyde Road**
**D4 Dublin**
**Ireland**

**Phone: +353 1 231 4862**
**Fax: +353 1 614 4756**
**E-mail: p.keane@frkelly.com**

80298 Munich
Germany
Tel. +49(0)89 2399-0 | Fax -4465

P.O. Box 5818
NL-2280 HV Rijswijk
Netherlands
Tel. +31(0)70 340-2040 | Fax -3016

10958 Berlin
Germany
Tel. +49(0)30 25901-0 | Fax -840


The document(s) listed below is (are) subsequently filed documents pertaining to the following application:

| | |
|---|---|
| Application number | 11752936.2 |
| Applicant's or representative's reference | P105633EP00 |

| | Description of document | Original file name | Assigned file name |
|---|---|---|---|
| 1 | Amended claims (clean copy) | P105633EP00 Claims Clean Aug28.pdf | CLMS-1.pdf |
| 2 | Amended claims with annotations | P105633EP00 Claims Markup Aug28.pdf | CLMS-HWA-1.pdf |
| 3 | Reply to search opinion/written opinion/IPER | P105633EP00 Response Finalised Aug28.pdf | WOREPLY-1.pdf |

**Signatures**

Place:

Date: **28 August 2014**

Signed by: **Paul Keane 36258**

Capacity: **(Representative)**

FRKELLY
EUROPEAN PATENT AND TRADE MARK ATTORNEYS

European Patent Office
D-80298 Munich
Germany

**Your Ref :** 11752936.2
**Our Ref :** P105633EP00

28 August 2014

Dear Sirs

**European Patent Application No. 11752936.2**
**"A Secured Personal Data Handling and Management System"**
**OS - NEW HORIZON PERSONAL COMPUTING SOLUTIONS LTD.**

In response to the Communication pursuant to Rule 70a(2) EPC, we hereby confirm the Applicant's desire to proceed further with the above Application.

**Response to Written Opinion**

**Patent Prosecution Highway (PPH)**
A request for participation in the Patent Prosecution Highway (PPH) programme based on US Patent No. 8,401,875 was filed on April 3 2014. The revised claims filed herewith correspond to the granted claims of US Patent No. 8,401,875.

**Amended Claims**
We enclose a replacement set of claims for replacing the claim set currently on file. An annotated claim set is also provided showing the claim revisions. Claims 1, 2, 6 and 13 have been amended to remove the phrase "or any weighted combination thereof".

Claims 4, 5 and 11 have been deleted. Applicant reserves right to file divisional applications.

Additionally, claims 1-3, 7-8, 12-15 have been amended in response to the "Added Subject Matter" objections. Amendments have been made according to the Examiner's guidelines.

Thus, the amended set of claims meet the requirements of Article 123(2) EPC and Article 84 EPC.

It is respectfully submitted that a person skilled in the art will readily understand that in the context of the description as a whole that the removed feature is:

1. not explained as essential in the disclosure,
2. is not, as such, indispensable for the function of the invention in the light of the technical problem it serves to solve, and
3. its removal requires no real modification of other features to compensate for the change.

This phrase was not included in the original application. Thus the removal of the feature from the revised claim 1 meets the three points test set out in T331/87, and should be allowable.

FRKelly 27 Clyde Road, Dublin 4, Ireland. Tel: +353-1 231 4848 Fax: +353-1 614 4756 dublin@frkelly.com www.frkelly.com

OFFICES: DUBLIN & BELFAST

**Unity of Invention**

Applicants respectfully disagree that the application does not comply with Unity of Invention requirements (Rule 44 EPC, Art 82 EPC)).

It is respectfully submitted that the Examiner did not consider all the features of the claims when assessing unity of invention. In particular, the Examiner indicated that a number of features in claim 1 was directed to added subject matter. The applicant strongly contests this assessment. The attached 'REFERENCE TABLE to ADDED MATTER' lists references in the description and figures for several phrases, which the Examiner indicated referred to added matter. As shown in the reference table, other terms/ phrases listed are referred to in the specification and/or figures.

Thus, applicants respectfully submits that the amended claims do not contain any added matter.

**REFERENCE TABLE [ ADDED MATTER? Rejection]**

| | Description, Page refs | Figs. | Fig. Ref No |
|---|---|---|---|
| Biometric | 26, line 19- 28, line 20 | 2 | 124; 126 |
| | 40, lines 7- 23 | 4 | 403 |
| | 45, lines 15-23 | 5 | 503 |
| Plurality of biometric sensors being integrated within the apparatus | 30, lines 23-24;<br>34, lines 18-20;<br>36, lines 16-17;<br>39, lines 13-14 | | |
| second storage unit (configured to store a ...personal biological biometric identification parameters) | 28, line 22;<br>30, lines23-28;<br>36, line 28;<br>45, line 26 | 2 | 140 |
| Life signs detector detects a critical level... prevents access | 40, lines 7- 23 to page 41 line 3 | 4 | 403 |

It is respectfully submitted that T194/84 referenced on page 347 of the Case Law of the Boards of Appeal 6th Edition makes it clear that "*The test for additional subject matter corresponded to the test for novelty only in so far as both required assessment of whether or not information was directly and unambiguously derivable from that previously present in the originally filed application or in a prior art document respectively. An amendment was not allowable if the resulting change in content of the application, in other words the subject-matter generated by the amendment, was novel when compared with the content of the original application or, looked at another way, if the said change in content would be novelty-destroying for a hypothetical future claim when the original content would not be.*" It is clear from the above table that the subject matter identified by the examiner as being "Added matter" is in fact directly and unambiguously derivable form the Application as originally filed and for this reason at least the previous amendments are allowable under 123(2) EPC.

It is respectfully submitted that D1 fails to disclose each and every one of the following features of claim 1.

> *Apparatus for managing personal and secured data and documentation files, stored in the apparatus ,comprising:*
> *a plurality of biometric sensors for reading a plurality of personal biometric identification parameters of the user holding the apparatus, said plurality of biometric sensors being stored within the apparatus;*

*at least one life signs detector integrated within the apparatus, said life signs detector being configured to measure and record at least one of said user's life sign parameters;*

*a first memory module in communication with said processing module and said encryption module for the storage of said user's data and documentation files;*

*an authentication unit configured to compare the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-recorded set of personal biometric identification parameters;*

*a processor in communication with said plurality of biometric sensors, said first memory module and said authentication unit;*

*wherein access to the personal data and documentation files stored in said first memory module is only enabled after said authentication unit positively matches each of the plurality of personal biometric identification parameters of the user holding the apparatus, with the pre-recorded set of personal biometric identification parameters; and*

*wherein, whenever any of said at least one life signs detector detects a critical level of said user measured life sign parameters, the apparatus is configured to prevent access to said user's personal data and documentation files stored in said first memory module.*

The claim numbering used in the following comments corresponds to the claim numbering used by the Examiner in the Search Opinon.

Apparatus claims 1-5 relate to a single invention which is described in the preamble to claim 1 "*Apparatus for managing personal and secured data and documentation files stored in the apparatus*". The technical effects of the claims is that an user is detected and authenticated (or not) through '*a plurality of personal (biological) biometric identification parameters' and 'at least one life signs detector*'.

Access to personal data and documentation files stored in the apparatus is only enabled after "*the authentication unit positively matches each of the plurality of personal biometric (biological) identification parameters of the user holding the apparatus*"

In addition, *as a corollary to allowing access,* whenever any of "*life signs detector detects a critical level of the user measured life sign parameters, the apparatus is configured to prevent access to the user's personal data and documentation files*". *(Claim 1).*

By continuously "*reading the plurality of personal biological identification parameters associated with the user holding the apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied*". (*Claim 2*).

Thus, the problem being solved is how to detect and authenticate an user of a device, to prevent unauthorized use and to detect a critical level or emergency situation.

Claim 3 extends the invention of claims 1 and 2, by configuring the apparatus to make an emergency call when the 'critical level' (of claim 1) is detected. The effect of this feature is that the "*authenticated user*" is able to communicate with emergency services in a "critical" situation. The communication may include sending the user's medical data to the service. Claim 3 does not refer to the problem of "how to provide user related data to emergency services".

Similarly, claims 6-11 relate to a method utilizing the apparatus of claim 1 to "managing personal and secured data and documentation files of a plurality of unique users". Claim 6 detects and authenticates (or not) an user of the apparatus through '*a plurality of personal*

*biological biometric identification parameters' and 'at least one life signs detector'*- similar to the effect of claim 1 above.

Claim 7 (partially) has a similar effect as claim 2 (above).

Part of claim 7 and part of claim 8 have a similar effect as claim 3, in that emergency services are contactable when a 'critical level' is indicated.

Claims 9 and 10 refer to the *authentication* of the device (apparatus claims 1-5). The problem being solved is the same problem as claims 1,2 and 6,7.

Thus, Inventions 1, 2 and 8 intrinsically refer to the same problem, that is of "*how to detect and authenticate an user of a device, to prevent unauthorized use and to detect a critical level or emergency situation of the user.*"

Claims 12-15 is a system claim which refers to a system for "*managing the personal and secured data and documentation files asscciated with a plurality of unique users, each utilizing the apparatus of claim 1*".

Claim 12 refer to the same problem as claims 1 and 6 that is of "*how to detect and authenticate an user of a device, to prevent unauthorized use and to detect a critical level or emergency situation albeit for a plurality of users.*"

Thus, Invention 12 is identical to Inventions 1, 2 and 8.

Thus, applicants respectfully submit that claims 1, 2, 3, 6, 7, 8, 9, 10 and 12-15 refer to a single invention and meet the requirements of Unity of invention (Rule 44 EPC, Art 82 EPC)).

**Inventive Step**

The Applicant notes that it is mandatory under the EPC that the Examiner demonstrates why one skilled in the art **would, not just could,** arrive at the claimed invention starting with the closest prior art bearing in mind the objective technical problem to be solved.

According to the Guidelines for Examination (Could-Would approach) "*the question to be answered is whether there is any teaching in the prior art as a whole that **would (not simply could**, but would) have prompted the skilled person, faced with the objective technical problem, to modify or adapt the closest prior art while taking account of that teaching, thereby arriving at something falling within the terms of the claims, and thus achieving what the invention achieves In other words, the point is not whether the skilled person could have arrived at the invention by adapting or modifying the closest prior art, but whether he **would have done** so because the prior art **incited him to do so in the hope of solving the objective technical problem or in expectation of some improvement or advantage** (see T2/83, OJ6/1984, 265).*" The Division must explain why he would do this, not just could.

It is respectfully submitted that there is not a scintilla of motivation in the prior art that would prompt a person skilled in the art to redesign the prior art to include all the features as recited in claim 1. Examiners should be wary of ex post facto analysis.

The Applicant respectfully reminds the Examining Division that they are obliged under the EPC to grant the application unless there is a valid basis to refuse. The onus is on the Examining Division to establish beyond doubt that the objection is valid and to substantiate all objections. In doing so, the Division must refrain from using hindsight, assumption or innuendo which is not permissible under the EPC.

As is evident from the above argument the Examiner has not provided sufficient anticipation of the claimed features or reasoning why the person of skill in the art would be motivated upon reading the prior art to modify it to arrive at the claimed features. In view of the claim

amendments and arguments presented herein, Applicant submits that the claims are both novel and inventive in view of the cited prior art.

**General**

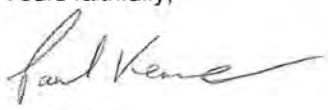
Any amendments made by way of the present letter, and the observations contained herein, are made solely for the purposes of the prosecution of this European patent application and without prejudice to the applicant in other jurisdictions.

It should be noted that insofar as any subject-matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments mentioned above and/or incorporated in the new pages submitted with this letter, the Applicant wishes to reserve the right to restore such subject matter and/or file a divisional application in respect thereof.

In the event that it is intended to refuse this application, or before any adverse decision is taken, the applicant hereby requests, in order of preference, a telephone interview, a personal interview, or oral proceedings under Article 116 EPC.

Favourable reconsideration of this application is requested. It is believed that the present submission properly overcomes all remaining objections and that the application is in order for grant. However, if there are any remaining objections which may be usefully dealt with by telephone, the Examiner is invited to call me on **+353 1 231 4862**.

Yours faithfully,



Paul Keane
Representative

p.keane@frkelly.com
+353-1-2314862

**WHAT IS CLAIMED IS-with Revision Marks:**

1. Apparatus for ~~storing and~~ managing personal and secured data and documentation files ~~associated with a specific user~~ stored in the apparatus, comprising:

a plurality of biometric sensors for reading a plurality of personal ~~biological~~ biometric identification parameters of the user holding the apparatus, said plurality of biometric sensors being ~~integrated~~stored within the apparatus;

at least one life signs detector ~~integrated~~stored within the apparatus, said life signs detector being configured to measure and record at least one of said user's life sign parameters;

a first ~~storage unit~~ memory module in communication with said processing module and said encryption module for the storage of said user's data and documentation files;

an authentication unit ~~comprising a second storage unit, with said second storage unit configured to store a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user, wherein said authentication unit is~~ configured to compare the plurality of personal biological biometric identification parameters of the user holding the apparatus ~~or any weighted combination thereof~~ with the pre-recorded set of personal ~~biological~~ biometric identification parameters ~~or any weighted combination thereof stored in said second storage unit~~;

a processor in communication with said plurality of biometric sensors, said first ~~storage unit~~memory module and said authentication unit;

wherein access to the personal data and documentation files stored in said first ~~storage unit~~ memory module is only enabled after said authentication unit positively matches each of the plurality of personal biometric ~~biological~~ identification parameters of the user holding the apparatus ~~or any weighted combination thereof~~, with the pre-recorded set of

Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Strikethrough

personal ~~biological~~ identification parameters ~~stored in said second storage unit~~; and

wherein, whenever any of said at least one life signs detector detects a critical level of said user measured life sign parameters, the apparatus is configured to prevent access to said user's personal data and documentation files stored in said first memory module~~storage unit~~.

2. The apparatus according to claim 1, wherein said plurality of biometric sensors are configured to continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, ~~or any weighted combination thereof~~, access to the stored personal data files is denied and the operation of the apparatus is completely shut down; ~~and/~~or

wherein said at least one of said user's life sign parameters is measured by any of a group of life sign indicators including a body pulse rate measurement indicator, a body O2 saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator

3. The apparatus according to claim 1, further comprising:

communication and data connection means for communicating with an external device, said communication and data connection means being controlled by and in communication with said processor; ~~and/~~or

wherein, whenever any of the group of life sign indicators detects a critical level, the apparatus is configured to:

initiate an emergency call to any of a group of registered emergency medical or security centers ~~including a request for medical help or police/security intervention~~, and send to said registered emergency centers any of a group of data files containing information associated with the user, including the identification data file of the user, personal medical ~~and measured physical stress data parameters~~ file of the user,

Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Indent: Left: 0 cm, First line: 0 cm
Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Strikethrough
Formatted: Strikethrough

the measured set of life sign parameters of the user and location of the user, ~~and/~~or

the apparatus further comprises an encryption unit in communication with said processor for the encryption plus compression and for the decompression plus decryption of said user's data files; ~~and/~~or

an emergency button in communication with said processor and said communication and data connection means module;

wherein on said emergency button being activated, communication is initiated between said apparatus and any of a group of registered emergency centers, said emergency call transmitting any of a group of data files containing information associated with the unique user of said apparatus, including the identification data of said user, the personal medical data file of said user, and location of said user; ~~and/~~or.

wherein said apparatus is configured to communicate with any of a group of service providers, said group of service providers including banks, credit card companies, clinics, hospitals and medical insurance companies, municipal and utility entities and websites frequently accessed by said user; thereby allowing said user to access and manage personal data and documentation files, associated with said user; ~~and/~~or

wherein said external device comprises any one of a group including a remote server, a local server, a host computer, voice or data communication means and a cellular phone; ~~and/~~or

wherein said emergency call is initiated via any one of a group of communication means including a secured server, directly via the internet by said apparatus connection and communication means, via the internet through any host computer, via a voice and data communication device and via any cellular phone network; ~~and/~~or

wherein said communication and data connection means comprises at least one of a group of connection and communication devices including a data interface connector attached to a host computer, a Mini USB, a compatible industrial data interface connector attached to a cellular phone, a

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Strikethrough

near field wireless communication interface, a Bluetooth communication interface, a magnetic reader interface, and a smart card reader based on a contact-less communication interface using induction or RF communication; ~~and/~~or

further comprising an ~~integrated~~stored software module that automatically detects the operating system of the computer or cellular phone connected to said apparatus through one of said group of communicating devices through which the apparatus is connected, said computer or cellular phone having keyboard and display units associated therewith, thereby allowing the user to interact with said first ~~storage unit~~ memory module and with said processor of said apparatus via said keyboard and display units, whereby said computer or cellular phone is configured to utilize and interact with said memory module, said processor and said sensor module of said apparatus.

~~4. The apparatus according to claim 1, further comprising:~~

~~a magnetic strip element that is only activatable after positive authentication of said user's personal biological biometric identification parameters and positive normal non-critical measured output of all of the at least one of said life sign detectors of said user measured life sign parameters; and~~

~~wherein said magnetic strip is configured to be concealed within the apparatus and on activation configured to extend out of the apparatus for swiping and reading by any of group of devices including a credit card reader, ATM and point of sale magnetic strip reading device; and/or~~

~~further comprising an integrated digital data encoder/decoder and a RF transceiver module in communication with the processor, said integrated digital data encoder/decoder and a wireless transceiver being configured to communicate with any of a group of external devices including RF operated credit card readers, ATM machines, and remotely operated electronic locks gates and doors opener using RFID based techniques; and/or~~

Formatted: Claims

Formatted: Strikethrough

~~the apparatus further comprising a supplementary base station device in communication with said wireless transceiver, said base station device configured to electrically charge the apparatus and simultaneously automatically execute a backup of the internal secured and non secured stored data of the apparatus.~~

~~5. The apparatus according to claim 1, further comprising a power charging and data backup device in communication with the processor of said apparatus, said device comprising;~~

~~i. a charging plug for connecting to the mains supply, an AC DC converter, a power supply unit and a rechargeable backup battery; and~~

~~ii. a micro processor and a mass memory unit; and~~

~~iii. an electronic buzzer activator, a button connected to said buzzer activator and an RF transmitter connected to said electronic buzzer activator, wherein on activating said buzzer button, said RF transmitter is configured to transmit a coded signal to the apparatus to enable the user to determine the location of the apparatus; and~~

~~wherein the first storage unit of said apparatus is in communication with the mass memory unit of said device, thereby to compare and synchronize the version of data stored in the first storage unit of said apparatus with the version of data stored in mass memory unit of said device; and/or~~

~~the apparatus further comprising an integrated GPS module in communication with the processor to precisely locate the geographical position of the apparatus; and/or~~

~~the apparatus further comprising at least one of a group of units including a cellular communication modem and a flat display and touch screen in communication with the processor.~~

~~6~~4. A method for managing personal and secured data and documentation files of a plurality of unique users, each one of said plurality of unique users having a personal identification unit uniquely associated with said one user

Formatted: Claims, Indent: Left: 0 cm

Formatted: Claims

for storing each user's personal data and documentation files, each of said personal identification units comprising:

a plurality of biometric sensors ~~integrated~~stored within the personal identification unit;

at least one life signs detector, ~~integrated~~stored within the personal identification unit, said life signs detector being configured to measure and record at least one of said user's life sign parameters;

a processor in communication with said plurality of biometric sensors;

an authentication unit in communication with the processor;

an encryption unit in communication with said processor;

a first ~~storage unit~~ memory module in communication with said processor and said encryption unit; and

communication and data connection means in communication with said processor;

the method comprising the steps of:

a. the plurality of biometric sensors reading a plurality of personal ~~biological~~ identification parameters of the user holding the personal identification unit;

Formatted: Strikethrough

b. at least one life signs detector, ~~integrated~~stored within the apparatus, measuring and recording at least one of said user's life sign parameters;

c said authentication unit comparing each of the personal biological identification parameters of said user ~~or any weighted combination thereof~~ with a pre-recorded set of personal biological identification parameters ~~or any weighted combination thereof~~ stored in said authentication unit; and

d. if said authentication unit positively identifies said user, allowing said user access to said user's personal data and documentation files stored in said first ~~\storage unit~~ memory module and allowing said user to communicate with other communication means through said personal identification unit.

~~75~~. The method of claim ~~64~~ further comprising the steps of: said biometric sensors continuously reading a plurality of personal biological ~~biometric~~ identification parameters of said user holding the apparatus; and

in the event that a significant change occurs in any of the plurality of personal biological ~~biometric~~ identification parameters~~, or in the normal output reading~~ of said least one of said life signs detectors,, denying access to the stored personal data files and completely shutting down the operation of said apparatus; ~~and/~~or

wherein at least one of said plurality of life signs detectors includes a body pulse rate measurement indicator, a body O2 saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator, the method further comprising the steps of:

initiating an emergency call to any of a group of registered emergency centers, whenever any of the life sign indicators detects a critical level; and

wherein said emergency call transmits any of a group of data files information associated with the user, including identification of the user, personal medical data file of the user, the measured set of life sign parameters of the user and location of the user; ~~and/~~or

wherein the method further comprises the step of:

communicating, via any one of a group of communication means, with any of a group of service providers including banks, credit card companies, clinics, hospitals and medical insurance companies, municipal and utility entities and websites frequently accessed by said user thereby allowing said user to access and manage said user's personal data and documentation files stored by said group of service providers.

~~86~~. The method of claim ~~6~~ 4, wherein said apparatus further comprises an emergency button in communication with said processor and said communication and data connection means, the method further comprising the steps of:

Formatted: Strikethrough

when said emergency button is activated, ~~an emergency medical data file is displayed to the emergency button apparatus activating person and/or~~ a call is initiated between said apparatus and any of a group of registered emergency centers; and

said emergency call transmitting any of a group of data files information associated with the user, including identification data of the user, the personal medical data file of the user, and location of the user; ~~and/~~or

wherein the apparatus further comprises a magnetic strip element, the method further comprising the step of:

after positive authentication of said user's personal ~~biological~~ identification parameters, activating said magnetic strip thereby allowing said magnetic strip to be read by any of group of devices including a credit card reader, an ATM, a point of sale, a magnetic strip or near field communication reading device (NFC); ~~and/~~or

wherein the apparatus further comprises a power charging and data backup device, said device comprising a charging and power unit, an electronic sub unit and a mass memory solid-state memory unit, the method further comprising the steps of:

comparing the memory content of said apparatus first ~~storage unit~~ memory module to the memory content of said mass memory solid-state memory unit; and

if the first ~~storage unit~~ memory module of the apparatus lacks data, updating the first ~~storage unit~~ memory module with the last version of the data stored within the solid-state memory unit; and

if said solid-state memory unit of said device lacks data, updating the solid-state memory unit of said device with the last version of the data stored within said apparatus's solid-state memory unit.

~~9~~7. The method of claim ~~6~~ 4, wherein each of said plurality of unique users is in communication with a system manager, said system manager managing a

Formatted: Strikethrough

remote centralized data communication storage and management system of said plurality of unique users, the method further comprising the steps of:

a. said system manager registering each unique user and storing the personal ID data file of each unique user in a memory sub-system connected to said centralized system; and

b. said registration further includes the step wherein said system manager generates for each system user N pairs of two different randomly selected characters strings, each of said strings is a combination of n alphanumeric characters in length; and

c. said system manager storing said N pairs in said system memory sub-system and sending said n characters strings pairs to be stored in said unique user personal identification unit memory module; and

d. said personal identification unit generating a secret access code of L alphanumeric characters to be further stored in said system memory within a special partition containing the list of said secret access codes for said plurality of unique users without assigning any identification or link between the associated users to his registered secret access code.

~~108~~. The method of claim ~~97~~, wherein after registration and upon normal initiation of communication between said system manager and each unique user, said system manager further communicating with said unique user and first comparing said unique user's ID data file and said personal identification unit unique embedded characterizing serial number stored in the unique user's personal identification unit with the corresponding user's ID and personal identification data stored in said memory sub-system; and

if the two sets of identification data match;

i. said system manager sending a first string of said stored N strings of coded alphanumeric data, to said user's personal identification unit; and

ii said user personal identification unit responding with the second matching string from the same stored pair of coded alphanumeric data uniquely associated with said user personal identification unit: and

iii said system manager comparing the received second string of coded alphanumeric data with a second string of coded alphanumeric data pre-stored in the memory sub-system; and

iv. said system manager comparing for consecutive M out of N times the received additional different strings of coded alphanumeric data pre-stored in the memory of said personal identification unit associated with said unique user with the additional strings of coded alphanumeric data pre-stored in the memory of sub-system; and

v. if all M strings of coded alphanumeric data match, then said system manager declares authenticating of said unique user and permitting said unique user access to said system.

~~11. The method of claim 9, further comprising the steps of:~~

~~after the step of authenticating, said system manager connecting the personal identification unit of said unique user with any of a group of emergency centers or service providers registered with said system manager at the request of said user personal identification unit; and~~

~~in the case of a medical emergency call initiated by said personal identification unit, transferring the user's updated medical data to the emergency center.~~

~~12~~9. A system for managing personal and secured data and documentation files of a plurality of unique users, the system comprising:

a. a system manager for managing and updating personal data of said system plurality of unique users ~~and for full duplex communication~~ with each of said plurality of unique users ~~and a plurality of service providers~~; and

b. a storage system connected to said system manager to store updated personal data of each of said plurality of unique users; and

c. a plurality of personal identification units, each of said personal identification units being associated with a unique user, each unique user being registered with said system manager, each of said personal identification units comprising a storage unit configured to store the

Field Code Changed

Formatted: Claims

personal ID data file of each unique user and a plurality of biometric sensors for reading a plurality of personal biometric ~~biological~~ identification parameters of the user holding the apparatus, said plurality of biometric sensors being ~~integrated~~stored within the personal identification units ~~and at least one life signs detector, integrated~~stored within said personal identification units, said life signs detector being configured to measure and record at least one of said user's life sign parameters; and

d. a plurality of computer hosts and cellular phones in communication with said system manager, enabling the direct connection by said system manager with said plurality of unique users through their corresponding personal identification unit; and

e. a plurality of registered emergency centers and a plurality of registered service providers in communication with said system manager, said plurality of service providers including banks, credit card companies, insurance companies, clinics, hospitals and medical insurance companies, government, municipal and utility entities and selected websites frequently accessed by said plurality of users;

wherein said system manager's access to and communication with the personal data and documentation files stored in said personal identification units associated with each said unique user and to the personal data and documentation files stored by said group of service providers is only enabled after positive authentication of each of said unique user's personal biometric ~~biological~~ identification parameters by said authentication unit and measuring the normal measured output of each one of said user's life sign parameters;

~~wherein at least one of said plurality of biometric sensors is a life signs detector, said life signs detector being configured to measure and record at least one of said user's life sign parameters;~~ and

wherein said at least one of said user's life sign parameters is measured by any of a group of life sign indicators including a body pulse rate measurement indicator, a body $O_2$ saturation level indicator, a body heat

Formatted: Strikethrough

Formatted: Strikethrough

measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator.

~~13~~10. The system according to claim ~~12~~ 9, wherein each of said plurality of personal identification units comprises:

i. a sensor module comprising a plurality of biometric sensors for reading a plurality of personal biometric ~~biological~~ identification parameters of the user holding the of personal identification units, said of personal identification units being uniquely identified with said user; and

ii. a processor in communication with said sensor module for processing said personal ~~biological~~ identification parameters and for processing and managing the personal and secured data and documentation files associated with said user; and

iii. an authentication unit in communication with the processor configured to receive and authenticate the identity of said user by comparing said user's personal ~~biological~~ identification parameters read ~~or any weighted combination thereof~~, by the sensor module and processed by the processor, with a pre-recorded set of personal ~~biological~~ identification parameters ~~or any weighted combination thereof~~ stored in said authentication unit; and

iv. an encryption module in communication with said processor for the encryption plus compression ~~and/~~or decompression plus decryption of said user's data files; and

v. a storage unit in communication with said processor and said encryption module for the storage of said user's data and documentation files; and

vi. communication and data connection means in communication with said processor for connecting said plurality of personal identification units with said system manager and plurality of service providers.~~; through the use of any device from a group of connection and communication devices including a data interface connector attached to a host computer, a Mini USB, a compatible industrial data interface connector attached to a cellular~~

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Strikethrough

~~phone, a near field wireless communication interface, a Bluetooth communication interface, a magnetic reader interface, and a smart card reader based on a contact less communication interface using induction or RF communication~~

~~14~~11. The system according to claim ~~13~~10, wherein said system manager is configured:

to communicate with said personal identification units to compare the user's ID data file stored in the unique user's personal identification units with the corresponding identification data stored in said storage unit, and

if the two sets of identification data match, then said system manager is configured to initiate a further level of security identification prior to full communication and data updating capability being enabled between said system manager and said user personal identification unit; and

wherein said further level of security identification comprises said system manager sending a first string of coded alphanumeric data uniquely associated with said user personal identification unit to said user personal identification unit, said personal identification unit responding with a second string of coded alphanumeric data uniquely associated with said user personal identification unit, and said system manager verifying the received second string of coded alphanumeric data with a second string of coded alphanumeric data pre-stored in the memory sub-system; and

said system manager comparing for full matching for N consecutive times received additional different strings of coded alphanumeric data pre-stored in the memory of said personal identification unit associated with said unique user with counter generated additional strings of coded alphanumeric data pre-stored in the memory of sub-system; ~~and/~~or

wherein said plurality of biometric sensors continuously read a plurality of personal ~~biological~~ biometric identification parameters associated with the user holding his unique personal identification units and in the event that a change occurs in any of the plurality of personal ~~biological~~ biometric identification parameters, access to the stored personal data files is denied

Formatted: Strikethrough

Formatted: Strikethrough

and the operation of said identification units is completely shut down; ~~and/~~or

wherein each personal identification unit further comprises an emergency button in communication with said processor and said communication and data connection means module;

wherein the personal identification unit is configured to transfer any of a group of data files containing information associated with the user, including files such as the identification data of the user, personal medical data file of the user, the measured set of life sign parameters of the user, ~~financial, insurance and banking data files~~ associated with the user and an updated location of the user; and

wherein the personal identification unit is configured to initiate an emergency call to any of said plurality of registered emergency centers, whenever said emergency button is activated or whenever any of the group of life sign indicators detects a critical level.

~~15~~12. The system of claim ~~12~~9, wherein said system, further comprises:

a computerized call center configured to receive phone calls or emergency voice and data messages from any of said plurality of registered emergency centers and a plurality of registered service providers and to communicate with any of said plurality of cellular phone and host computers; and

wherein said call center is configured to communicate the user's location coordinates to an emergency rescue team and simultaneously said call center is configured to communicate with any of said plurality of registered emergency centers and service providers to receive said user's updated medical data and to transfer said data to and from the user's personal identification unit.

## WHAT IS CLAIMED IS

1. Apparatus for managing personal and secured data and documentation files stored in the apparatus, comprising:

a plurality of biometric sensors for reading a plurality of personal biometric identification parameters of the user holding the apparatus, said plurality of biometric sensors being stored within the apparatus;

at least one life signs detector stored within the apparatus, said life signs detector being configured to measure and record at least one of said user's life sign parameters;

a first memory module in communication with said processing module and said encryption module for the storage of said user's data and documentation files;

an authentication unit configured to compare the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-recorded set of personal biometric identification parameters;

a processor in communication with said plurality of biometric sensors, said first memory module and said authentication unit;

wherein access to the personal data and documentation files stored in said first memory module is only enabled after said authentication unit positively matches each of the plurality of personal biometric identification parameters of the user holding the apparatus, with the pre-recorded set of personal identification parameters; and

wherein, whenever any of said at least one life signs detector detects a critical level of said user measured life sign parameters, the apparatus is configured to prevent access to said user's personal data and documentation files stored in said first memory module.

2. The apparatus according to claim 1, wherein said plurality of biometric sensors are configured to continuously read a plurality of personal identification parameters associated with said user holding the apparatus

and in the event that a change occurs in any of the plurality of personal identification parameters, access to the stored personal data files is denied and the operation of the apparatus is completely shut down; or

wherein said at least one of said user's life sign parameters is measured by any of a group of life sign indicators including a body pulse rate measurement indicator, a body O2 saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator

3. The apparatus according to claim 1, further comprising:

communication and data connection means for communicating with an external device, said communication and data connection means being controlled by and in communication with said processor; or

wherein, whenever any of the group of life sign indicators detects a critical level, the apparatus is configured to:

initiate an emergency call to any of a group of registered emergency medical or security centers and send to said registered emergency centers any of a group of data files containing information associated with the user, including the identification data file of the user, personal medical file of the user, the measured set of life sign parameters of the user and location of the user, or

the apparatus further comprises an encryption unit in communication with said processor for the encryption plus compression and for the decompression plus decryption of said user's data files; or

an emergency button in communication with said processor and said communication and data connection means module;

wherein on said emergency button being activated, communication is initiated between said apparatus and any of a group of registered emergency centers, said emergency call transmitting any of a group of data files containing information associated with the unique user of said apparatus, including the identification data of said user, the personal medical data file of said user, and location of said user; or.

wherein said apparatus is configured to communicate with any of a group of service providers, said group of service providers including banks, credit card companies, clinics, hospitals and medical insurance companies, municipal and utility entities and websites frequently accessed by said user; thereby allowing said user to access and manage personal data and documentation files, associated with said user; or

wherein said external device comprises any one of a group including a remote server, a local server, a host computer, voice or data communication means and a cellular phone; or

wherein said emergency call is initiated via any one of a group of communication means including a secured server, directly via the internet by said apparatus connection and communication means, via the internet through any host computer, via a voice and data communication device and via any cellular phone network; or

wherein said communication and data connection means comprises at least one of a group of connection and communication devices including a data interface connector attached to a host computer, a Mini USB, a compatible industrial data interface connector attached to a cellular phone, a near field wireless communication interface, a Bluetooth communication interface, a magnetic reader interface, and a smart card reader based on a contact-less communication interface using induction or RF communication; or

further comprising an stored software module that automatically detects the operating system of the computer or cellular phone connected to said apparatus through one of said group of communicating devices through

which the apparatus is connected, said computer or cellular phone having keyboard and display units associated therewith, thereby allowing the user to interact with said first memory module and with said processor of said apparatus via said keyboard and display units, whereby said computer or cellular phone is configured to utilize and interact with said memory module, said processor and said sensor module of said apparatus.

4. A method for managing personal and secured data and documentation files of a plurality of unique users, each one of said plurality of unique users having a personal identification unit uniquely associated with said one user for storing each user's personal data and documentation files, each of said personal identification units comprising:

a plurality of biometric sensors stored within the personal identification unit;

at least one life signs detector, stored within the personal identification unit, said life signs detector being configured to measure and record at least one of said user's life sign parameters;

a processor in communication with said plurality of biometric sensors;

an authentication unit in communication with the processor;

an encryption unit in communication with said processor;

a first memory module in communication with said processor and said encryption unit; and

communication and data connection means in communication with said processor;

the method comprising the steps of:

a. the plurality of biometric sensors reading a plurality of personal identification parameters of the user holding the personal identification unit;

b. at least one life signs detector, stored within the apparatus, measuring and recording at least one of said user's life sign parameters;

c said authentication unit comparing each of the personal biological identification parameters of said user with a pre-recorded set of personal biological identification parameters stored in said authentication unit; and

d. if said authentication unit positively identifies said user, allowing said user access to said user's personal data and documentation files stored in said first memory module and allowing said user to communicate with other communication means through said personal identification unit.

5. The method of claim 4 further comprising the steps of: said biometric sensors continuously reading a plurality of personal biological identification parameters of said user holding the apparatus; and

in the event that a significant change occurs in any of the plurality of personal biological identification parameters of said least one of said life signs detectors, denying access to the stored personal data files and completely shutting down the operation of said apparatus; or

wherein at least one of said plurality of life signs detectors includes a body pulse rate measurement indicator, a body O2 saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator, the method further comprising the steps of:

initiating an emergency call to any of a group of registered emergency centers, whenever any of the life sign indicators detects a critical level; and

wherein said emergency call transmits any of a group of data files information associated with the user, including identification of the user, personal medical data file of the user, the measured set of life sign parameters of the user and location of the user; or

wherein the method further comprises the step of:

communicating, via any one of a group of communication means, with any of a group of service providers including banks, credit card companies, clinics, hospitals and medical insurance companies, municipal and utility entities and websites frequently accessed by said user thereby allowing said

user to access and manage said user's personal data and documentation files stored by said group of service providers.

6. The method of claim 4, wherein said apparatus further comprises an emergency button in communication with said processor and said communication and data connection means, the method further comprising the steps of:

when said emergency button is activated, a call is initiated between said apparatus and any of a group of registered emergency centers; and

said emergency call transmitting any of a group of data files information associated with the user, including identification data of the user, the personal medical data file of the user, and location of the user; or

wherein the apparatus further comprises a magnetic strip element, the method further comprising the step of:

after positive authentication of said user's personal identification parameters, activating said magnetic strip thereby allowing said magnetic strip to be read by any of group of devices including a credit card reader, an ATM, a point of sale, a magnetic strip or near field communication reading device (NFC); or

wherein the apparatus further comprises a power charging and data backup device, said device comprising a charging and power unit, an electronic sub unit and a mass memory solid-state memory unit, the method further comprising the steps of:

comparing the memory content of said apparatus first memory module to the memory content of said mass memory solid-state memory unit; and

if the first memory module of the apparatus lacks data, updating the first memory module with the last version of the data stored within the solid-state memory unit; and

if said solid-state memory unit of said device lacks data, updating the solid-state memory unit of said device with the last

version of the data stored within said apparatus's solid-state memory unit.

7. The method of claim 4, wherein each of said plurality of unique users is in communication with a system manager, said system manager managing a remote centralized data communication storage and management system of said plurality of unique users, the method further comprising the steps of:

a. said system manager registering each unique user and storing the personal ID data file of each unique user in a memory sub-system connected to said centralized system; and

b. said registration further includes the step wherein said system manager generates for each system user N pairs of two different randomly selected characters strings, each of said strings is a combination of n alphanumeric characters in length; and

c. said system manager storing said N pairs in said system memory sub-system and sending said n characters strings pairs to be stored in said unique user personal identification unit memory module; and

d. said personal identification unit generating a secret access code of L alphanumeric characters to be further stored in said system memory within a special partition containing the list of said secret access codes for said plurality of unique users without assigning any identification or link between the associated users to his registered secret access code.

8. The method of claim 7, wherein after registration and upon normal initiation of communication between said system manager and each unique user, said system manager further communicating with said unique user and first comparing said unique user's ID data file and said personal identification unit unique embedded characterizing serial number stored in the unique user's personal identification unit with the corresponding user's ID and personal identification data stored in said memory sub-system; and

if the two sets of identification data match;

i. said system manager sending a first string of said stored N strings of coded alphanumeric data, to said user's personal identification unit; and

ii said user personal identification unit responding with the second matching string from the same stored pair of coded alphanumeric data uniquely associated with said user personal identification unit: and

iii said system manager comparing the received second string of coded alphanumeric data with a second string of coded alphanumeric data pre-stored in the memory sub-system; and

iv. said system manager comparing for consecutive M out of N times the received additional different strings of coded alphanumeric data pre-stored in the memory of said personal identification unit associated with said unique user with the additional strings of coded alphanumeric data pre-stored in the memory of sub-system; and

v. if all M strings of coded alphanumeric data match, then said system manager declares authenticating of said unique user and permitting said unique user access to said system.

9. A system for managing personal and secured data and documentation files of a plurality of unique users, the system comprising:

a. a system manager for managing and updating personal data of said system plurality of unique users with each of said plurality of unique users; and

b. a storage system connected to said system manager to store updated personal data of each of said plurality of unique users; and

c. a plurality of personal identification units, each of said personal identification units being associated with a unique user, each unique user being registered with said system manager, each of said personal identification units comprising a storage unit configured to store the personal ID data file of each unique user and a plurality of biometric sensors for reading a plurality of personal biometric identification parameters of the user holding the apparatus, said plurality of biometric sensors being stored

within the personal identification units stored within said personal identification units, said life signs detector being configured to measure and record at least one of said user's life sign parameters; and

d. a plurality of computer hosts and cellular phones in communication with said system manager, enabling the direct connection by said system manager with said plurality of unique users through their corresponding personal identification unit; and

**e.** a plurality of registered emergency centers and a plurality of registered service providers in communication with said system manager, said plurality of service providers including banks, credit card companies, insurance companies, clinics, hospitals and medical insurance companies, government, municipal and utility entities and selected websites frequently accessed by said plurality of users;

wherein said system manager's access to and communication with the personal data and documentation files stored in said personal identification units associated with each said unique user and to the personal data and documentation files stored by said group of service providers is only enabled after positive authentication of each of said unique user's personal biometric identification parameters by said authentication unit and measuring the normal measured output of each one of said user's life sign parameters; and

wherein said at least one of said user's life sign parameters is measured by any of a group of life sign indicators including a body pulse rate measurement indicator, a body $O_2$ saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator.

10. The system according to claim 9, wherein each of said plurality of personal identification units comprises:

i. a sensor module comprising a plurality of biometric sensors for reading a plurality of personal biometric identification parameters of the user holding the of personal identification units, said of personal identification units being uniquely identified with said user; and

ii. a processor in communication with said sensor module for processing said personal identification parameters and for processing and managing the personal and secured data and documentation files associated with said user; and

iii. an authentication unit in communication with the processor configured to receive and authenticate the identity of said user by comparing said user's personal identification parameters read by the sensor module and processed by the processor, with a pre-recorded set of personal identification parameters stored in said authentication unit; and

iv. an encryption module in communication with said processor for the encryption plus compression or decompression plus decryption of said user's data files; and

v. a storage unit in communication with said processor and said encryption module for the storage of said user's data and documentation files; and

vi. communication and data connection means in communication with said processor for connecting said plurality of personal identification units with said system manager and plurality of service providers.

11. The system according to claim 10, wherein said system manager is configured:

to communicate with said personal identification units to compare the user's ID data file stored in the unique user's personal identification units with the corresponding identification data stored in said storage unit, and

if the two sets of identification data match, then said system manager is configured to initiate a further level of security identification prior to full communication and data updating capability being enabled between said system manager and said user personal identification unit; and

wherein said further level of security identification comprises said system manager sending a first string of coded alphanumeric data uniquely associated with said user personal identification unit to said user personal identification unit, said personal identification unit responding with a second

string of coded alphanumeric data uniquely associated with said user personal identification unit, and said system manager verifying the received second string of coded alphanumeric data with a second string of coded alphanumeric data pre-stored in the memory sub-system; and

said system manager comparing for full matching for N consecutive times received additional different strings of coded alphanumeric data pre-stored in the memory of said personal identification unit associated with said unique user with counter generated additional strings of coded alphanumeric data pre-stored in the memory of sub-system; or

wherein said plurality of biometric sensors continuously read a plurality of personal biometric identification parameters associated with the user holding his unique personal identification units and in the event that a change occurs in any of the plurality of personal ~~biological~~ biometric identification parameters, access to the stored personal data files is denied and the operation of said identification units is completely shut down; or

wherein each personal identification unit further comprises an emergency button in communication with said processor and said communication and data connection means module;

wherein the personal identification unit is configured to transfer any of a group of data files containing information associated with the user, including files such as the identification data of the user, personal medical data file of the user, the measured set of life sign parameters of the user, associated with the user and an updated location of the user; and

wherein the personal identification unit is configured to initiate an emergency call to any of said plurality of registered emergency centers, whenever said emergency button is activated or whenever any of the group of life sign indicators detects a critical level.

12. The system of claim 9, wherein said system, further comprises:

a computerized call center configured to receive phone calls or emergency voice and data messages from any of said plurality of registered emergency centers and a plurality of registered service providers and to communicate with any of said plurality of cellular phone and host computers; and

wherein said call center is configured to communicate the user's location coordinates to an emergency rescue team and simultaneously said call center is configured to communicate with any of said plurality of registered emergency centers and service providers to receive said user's updated medical data and to transfer said data to and from the user's personal identification unit.

Europäisches Patentamt
European Patent Office
Office européen des brevets

# Acknowledgement of receipt

We hereby acknowledge receipt of the following subsequently filed document(s):

| | |
|---|---|
| Submission number | 2968301 |
| Application number | EP11752936.2 |
| Date of receipt | 28 August 2014 |
| Receiving Office | European Patent Office, The Hague |
| Your reference | P105633EP00 |
| Applicant | All applicants as on file |
| Documents submitted | package-data.xml<br>epf1038.pdf (1 p.)<br>CLMS-HWA-1.pdf\P105633EP00 Claims Markup Aug28.pdf (14 p.)<br>ep-sfd-request.xml<br>CLMS-1.pdf\P105633EP00 Claims Clean Aug28.pdf (12 p.)<br>WOREPLY-1.pdf\P105633EP00 Response Finalised Aug28.pdf (5 p.) |
| Submitted by | CN=Paul Keane 36258 |
| Method of submission | Online |
| Date and time receipt generated | 28 August 2014, 13:15 (CEST) |
| Message Digest | C9:B7:41:E5:CC:EB:30:BD:CF:93:D7:9A:6D:A5:1B:8F:1D:02:60:91 |

**Correction by the EPO of errors in debit instructions filed by eOLF**
Errors in debit instructions filed by eOLF that are caused by the editing of Form 1038E entries or the continued use of outdated software (all forms) may be corrected automatically by the EPO, leaving the payment date unchanged (see decision T 152/82, OJ EPO 1984, 301 and point 6.3 ff ADA, Supplement to OJ EPO 10/2007).

/European Patent Office/

Application No.: 11752936.2

Substantive examination has started on 19.12.14 (see Notice from the European Patent Office dated 29.01.2013, OJ EPO 2013, 153).

**For the Examining Division**

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
Postbus 5818
2280 HV Rijswijk
NETHERLANDS
Tel: +31 70 340 2040
Fax: +31 70 340 3016

Coyle, Philip Aidan
F. R. Kelly & Co.
27 Clyde Road
Ballsbridge
Dublin 4
IRLANDE

**Formalities Officer**
Name: Avilés Parrales, O
Tel: +31 70 340 - 1066
or call
+31 (0)70 340 45 00

**Substantive Examiner**
Name: Arbutina, Ljiljana
Tel: +31 70 340 - 4522

| Application No. | Ref. | Date |
|---|---|---|
| 11 752 936.2 - 1957 | p105633ep00 | 05.01.2015 |
| Applicant: OS - New Horizon Personal Computing Solutions Ltd. | | |

**Communication pursuant to Article 94(3) EPC**

The examination of the above-identified application has revealed that it does not meet the requirements of the European Patent Convention for the reasons enclosed herewith. If the deficiencies indicated are not rectified the application may be refused pursuant to Article 97(2) EPC.

You are invited to file your observations and insofar as the deficiencies are such as to be rectifiable, to correct the indicated deficiencies within a period

**of 4 months**

from the notification of this communication, this period being computed in accordance with Rules 126(2) and 131(2) and (4) EPC. One set of amendments to the description, claims and drawings is to be filed within the said period on separate sheets (R. 50(1) EPC).

If filing amendments, you must identify them and indicate the basis for them in the application as filed. Failure to meet either requirement may lead to a communication from the Examining Division requesting that you correct this deficiency (R. 137(4) EPC).

**Failure to comply with this invitation in due time will result in the application being deemed to be withdrawn (Art. 94(4) EPC).**

**Registered letter**
EPO Form 2001 12.10CSX

Arbutina, Ljiljana
Primary Examiner
**For the Examining Division**

Enclosure(s): 4 page/s reasons (Form 2906)

The examination is being carried out on the **following application documents**

**Description, Pages**

1-60 as published

**Claims, Numbers**

1-12 filed in electronic form on 28-08-2014

**Drawings, Sheets**

1/9-9/9 as published

## Added Subject-Matter

1.0. The amendments filed on 28.08.2014 contain subject-matter which extends beyond the content of the application as filed, contrary to requirements of Art.123(2) EPC, as follows:

1.1. Claim 1, the feature "life signs detector detects a critical level ... prevent access..."

The applicant cited in his letter of reply the passage on page 40, lines 7-23 to page 31 line 3 as being the support for this amendment.

The examiner is of the opinion that this feature is not present in the cited passage, nor is it directly and unambiguously derivable from it. This newly generated subject-matter is novel when compared with the original application, and thus the objection raised under Art.123(2) EPC against this feature is not in contradiction with the case T194/84, cited by the applicant in his letter of reply.

Therefore, the objection raised in the previous communication regarding this feature is maintained.

1.2. Claim 3, the feature "the apparatus is configured to initiate an emergency call to any of a group of registered emergency medical or security centers"

The originally filed claim recites that the apparatus is configured to initiate an emergency call to any of a group of registered emergency centers.

The applicant did not provide any support for the amendment "medical or security centers", therefore the objection from the previous communication is maintained.

1.3. Claim 7 (previously claim 9)

The applicant did not provide any support for this new combination of features. The objection from the previous communication is maintained.

**Clarity**

2.0. Claim 1 has been amended by putting back the originally filed feature "a memory module in communication with said processing module and said encryption module...". However, claim 1 includes neither an encryption module, nor a processing module.

In the following reasoning, it will be considered that the intention of the applicant was to include the encryption module in the claimed subject-matter, and that the term "processing module" refers to the processor as recited in claim 1.

2.1. In claim 1 and 4, the term "integrated" was changed to the term "stored". The applicant did not provide reason for this change. The examiner is of the opinion that the term "integrated", used in the originally filed application documents, is more suitable in this case. The use of a new term introduces a doubt about the intended scope of protection.

**Unity of Invention**

3.0. The objection under Art.82 from the previous communication is maintained, the reasons therefore being given here below.

3.1. The applicant argued in his letter of reply that the examiner has not considered all the features of the claims when assessing unity of invention. He then identified four elements of added matter, and gave passages as support for these amendments. The examines addresses these four elements as follows:

1) "biometric": document D1 discloses use of biometric, as already indicated in the previous communication;

2) "plurality of biometric sensors being integrated within the apparatus": this feature is disclosed in D1, see fig.1, lines 1-6 of par.[0029], and par.]0039];

3) "second storage unit ... biometric identification parameters": this feature is disclosed in D1, see par.[0079];

4) "life sign detector ... prevents access...": as argued here above, the examiner is still of the opinion that this feature infringes Art.123(2) EPC. However, the *content* of the passage cited as being support for this feature will be discussed further below.

3.2. The applicant argues further that D1 fails to disclose each and every one of the features of claim 1, without identifying the features he is actually disputing.

The examiner carefully re-considered the arguments given in the previous communication, par.2.1, and, in combination with amendments of claim 1, identified that claim 1 differs from the document D1 in the following:

a) Apparatus of the claim 1 manages "personal and secured data and documentation files", whereas the apparatus of claim 1 manages "different data or files associated with different applications" (D1, par.[0041])

This difference consists in the interpretation of data contained in the file and as such does not change the subject-matter defined by the claim (T0511/06: "With regard to the "blocks of information" which are transferred from the external device 12 to the information device 10, the patentee argued that the downloaded data in E1 was encrypted and that the skilled person would realise that the "blocks of information" in claim 1 were raw (i.e. non-encrypted) data. In the Board's view, the wording of claim 1 does not justify the patentee's narrow interpretation as to the format of the data transferred. Nonetheless, the format (i.e. raw or encrypted) of the data makes no difference to the capability of the external device for transferring the information: in both cases, the downloaded data will be comprised of a string of ones and zeros, whether it is encrypted or not. The Board is therefore of the opinion that this argument is of no significance with regard to the subject-matter defined in claim 1.")

b) An encryption module

Use of encryption is a matter of general knowledge and cannot represent a single general inventive concept.

c) Whenever one of said at least one life signs detector detects a critical level of said user measured life sign parameters, the apparatus is configured to prevent access to said user's personal data and documentation files stored in said first memory module

This feature is considered to be added subject-matter, as already discussed here above. However, it appears from the applicants arguments given in his letter of reply, page 3, 2nd paragraph of the reasoning, that the applicant considers this to be the core of the unity of invention. The applicant did not clearly identify the general inventive concept, but he stated that "the technical effect of the claims is that an user is detected and authenticated (or not) through *a plurality of personal biometric identification parameters and at least one life signs detector*".

Although the feature as drafted infringes Art.123(2) EPC, the examiner acknowledges that this *concept* is present in the passage of the application as filed identified by the applicant as being page 40, lines 7-23 to page 41, line 3. However, the examiner notes that this concept is present in D1, see par.[0057]. Therefore, even if the claim would be amended to include this concept without infringing Art.123(2) EPC, this would not overcome the objection under Art.82 EPC.

**Patentability**

4.0. The subject-matter of independent claims 1 and 4 is not inventive in the sense of Art. 56 EPC, as shown here above in par.3.2. Considering the system claim 9, the personal identification unit corresponds to the apparatus of claim 1 which is not inventive, as shown here above, and, because the electronic device in D1 is a telephone/Internet enabled, see par.[50] and [51], D1 implicitly discloses a system manager with a database related to a plurality of cellular phones and their owners. Therefore, the subject-matter of claim 9 is also not inventive.

4.1. The objection under Art.56 for the first invention as presented in the previous communication is maintained.

FRKELLY
EUROPEAN PATENT AND TRADE MARK ATTORNEYS

Examiner: Arbutina, Ljiljana
European Patent Office
D-80298 Munich
Germany

**Your Ref :** 11752936.2
**Our Ref :** P105633EP00

14 May 2015

Dear Examiner,

**European Patent Application No. 11752936.2**
**"A Secured Personal Data Handling and Management System"**
**OS - NEW HORIZON PERSONAL COMPUTING SOLUTIONS LTD.**

---

With reference to the Examination Report of January 5 2015, the Applicant's response is set out below.

**Amended Claims**
We enclose a replacement set of claims which are to form the basis for further proceedings before the EPO. An annotated claim set is also provided which shows the revisions.

**Added Subject-Matter**
**1.1** The Examiner has indicated that the amendments filed on 28.08.2014 contain subject-matter which extends beyond the content of the application as filed, contrary to requirements of Art.123(2) EPC. In particular, the Examiner has objected to the phrase "*life signs detector detects a critical level ... prevent access ...*". While not acquiescing to the merits of the rejection, the offending feature has been deleted from claim 1 in an effort to advance prosecution.

It is submitted that the offending phrase has been deleted and Claim 1 has been revised to recite, inter alia:

> *wherein said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied and the operation of the apparatus is completely shut down*

*Support for this feature may be found at least in the original PCT claim 2. Accordingly, the added matter objection against claim 1 has been rendered moot.*

**1.2** Furthermore, the Examiner has objected to the term "medical or security" in claim 3. It is submitted that this term has been deleted thereby rendering the objection against claim 3 moot.

FRKelly 27 Clyde Road, Dublin 4, Ireland. Tel: +353-1 231 4848 Fax: +353-1 614 4756 dublin@frkelly.com www.frkelly.com

BRENDA O'REGAN
SHANE SMYTH
ALAN WALLACE

ALAN CASEY
DAVID FLYNN
CAROL GORMLEY
ANNA HALLY
TARA JENNINGS
PAUL KEANE
STEPHEN MURPHY
JOHN O'FLAHERTY
BRONWYN O'HAGAN
MICHAEL SCANNELL
SHAUNA TILLEY
STEPHEN WALLER

CONSULTANTS:
LINDSAY J CASEY
PETER F KELLY

OFFICES: DUBLIN & BELFAST

**1.3** The Examiner has indicated that the applicant did not provide any support for this new combination of features in claim 7.

It is submitted that claim 7 substantially corresponds to PCT claim 28 and that claim 4 substantially correpsonds to PCT claim 21. PCT claim 28 was dependent on PCT claim 21. It is submitted that the combination of the features in claim 7 are directly and unambiguously derivable for the description with reference to Figure 2.

**Clarity**

**2.0** The Examiner has objected to the omission of the feature "*encryption module*" from claim 1. While not acquiescing to the merits of the rejection, claim 1 has been revised to recite: *an encryption module in communication with the processing module.* Furthermore, the term 'processor" has been replaced with the term "processing module" in an effort to advance prosecution.

**2.1** In claims 1 and 4 the term 'stored' has been reinstated to 'integrated' thereby rendering the objection of paragraph 2.1 moot.

**Unity of Invention**

Applicants respectfully disagree that the application does not comply with Unity of Invention requirements (Rule 44 EPC, Art 82 EPC)).

It is respectfully submitted that D1 at least fails to disclose:

1) A portable handheld apparatus for managing personal and secured data and documentation files stored in the apparatus while the apparatus is communicating with an external device;

2) an encryption module in communication with said processing module;

3) communication and data connection means for communicating with an external device, said communication and data connection means being controlled by and in communication with said processing module;

*4) wherein said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied and the operation of the apparatus is completely shut down*

*In paragraph 2.1.1 of the search opinion, the Examiner stated the following:*

2.1.1. The cited paragraphs of D1 disclose also the corresponding features of method claim 6, with exception of encryption unit, which is present in claim 1. However, encryption being a well-known technique, it cannot be considered to be a subject of an invention. For the same reason, it cannot form a single general inventive concept for claims 7-11 which are dependent on claim 6.

It is respectfully submitted that a lack of unity can only arise if claim 1 lacks novelty in light of D1. In view of the Examiner's comments in paragraph 2.2.1 of the search opinion, it is clear that claim 1 is novel in light of D1 by virtue of at least the 'encryption module'. As a consequence, the unity objection has been rendered moot. The Examiner cannot selectively omit the technical feature of the 'encryption module' when assessing unity.

Accordingly, the unity of invention objection has been rendered moot.

**Patentability**
The Examiner has indicated that the subject matter of independent claims 1 and 4 is not inventive in the sense of Article 56. The Applicant respectfully disagrees with this assessment. However, in an effort to advance prosecution claims 1 and 4 have been revised in an effort to advance prosecution.

To better understand the user's benefits of using the claimed invention, it is required to understand that presently users are frequently losing their saved personal and important data files, due to mechanical or electrical failures of their electromagnetic driven hard-discs, or suffer from sensitive data files failure or damages related to malfunctions of their personal computers or smart cell phones.

Another source for lost sensitive data files is due to software malfunction problems while running on the users' personal computers or smart cell phones. All these problems can be eliminated by the present invention which provides a solution by separating the user's sensitive data storage and management functions from the cell phone. This functional separation is a very important aspect of the present application.

The Examiner has indicated that D1 is the closest prior art for assessing an inventive step. A person of ordinary skill in the art would readily understand that in D1 the sensitive information and cellular functionality are provided on a single device which is direct contrast to the present invention. Thus the teaching of D1 points away from the claimed invention. The closest prior art is that which in one single reference discloses the combination of features which constitutes the most promising starting point for a development leading to the invention. In selecting the closest prior art, the first consideration is that it should be directed to a similar purpose or effect as the invention. It is respectfully submitted that D1 is not directed to the similar purpose as the claimed invention as it fails to provide the sensitive information on a separate device to that with cellular functionality.

In an effort to clarify that the sensitive information is stored on a separate device to the external device, claim 1 has been revised to recite; inter alia:

> *A portable handheld apparatus for managing personal and secured data and documentation files stored in the apparatus while the apparatus is communicating with an external device [**support page 18 lines13-17**, ].*
>
> *communication and data connection means for communicating with an external device, said communication and data connection means being controlled by and in communication with said processing module*; [**step (f) of the original PCT claim** 1]

It is respectfully submitted that D1 fails to disclose, hint or suggest this inventive aspect of the present Application. It appears that the Examiner acknowledges that D1 fail to disclose "*wherein said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied and the operation of the apparatus is completely shut down*" because in paragraph 4.1 of the search opinion, the examiner relies of prior art document D2 to teach this feature. Paragraph 4.1 of the search opinion is provided below for the Examiner's convenience.

> 4.1. Considering the first invention, see par.2.2 here above, the problem of preventing unauthorized use of a device was solved in D2, see col.5, lines 14-15, by using the same features as claims 2 and 7, namely,
>
> the plurality of biometric sensors continuously reading a plurality of personal biological identification parameters associated with said user holding the apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied and the operation of the apparatus is completely shut down

For the appropriate test for Article 56, the Applicant notes that it is mandatory under the EPC that the Examiner demonstrates why one skilled in the art **would, not just could,** arrive at the claimed invention starting with the closest prior art bearing in mind the objective technical problem to be solved.

When constructing an inventive step objection it is necessary to show (G-VII, 5.3):

> *In other words, the point is not whether the skilled person could have arrived at the invention by adapting or modifying the closest prior art, but whether he **would have done** so because the prior art incited him to do so in the hope of solving the objective technical problem or in expectation of some improvement or advantage (see T 2/83, OJ 6/1984, 265).*

The Examiner is again reminded as to the Guidelines requirements for a valid inventive step objection and specifically G-VII, 8 where it states:

> *In all cases he should attempt to visualise the overall state of the art confronting the skilled person before the applicant's contribution, and he should seek to make a "real-life" assessment of this and other relevant factors. He should take into account all that is known concerning the background of the invention and give fair weight to relevant arguments or evidence submitted by the applicant. If, for example, an invention is shown to be of considerable technical value, and particularly if it provides a technical advantage which is new and surprising and which is not merely achieved as a bonus effect in a "one-way street" situation (see 11.10.2), and this technical advantage can convincingly be related to one or more of the features included in the claim defining the invention, the examiner should be hesitant in pursuing an objection that such a claim lacks inventive step.*

It is respectfully submitted that there is no hint or suggestion in D1 of the specific limitations in claim 1 above, and of the advantage that this provides.

It is respectfully submitted that there is not a scintilla of motivation in the prior art that would prompt a person skilled in the art to redesign the prior art to include all the features as recited in claim 1. Examiners should be wary of ex post-facto analysis.

The Applicant respectfully reminds the Examining Division that they are obliged under the EPC to grant the application unless there is a valid basis to refuse. The onus is on the Examining Division to establish beyond doubt that the objection is valid and to substantiate all objections. In doing so, the Division must refrain from using hindsight, assumption or innuendo which is not permissible under the EPC.

As is evident from the above argument the Examiner has not provided sufficient anticipation of the claimed features or reasoning why the person of skill in the art would be motivated upon reading the prior art to modify it to arrive at the claimed features.

This omission of D1 is not compensated or addressed by the teaching of D2 which similarly fail to direct the person of skill to the specifics of the claimed teaching. In the absence of D1 or the

secondary references providing any teaching or motivation to the person of skill in the art to provide a method such as that now claimed, it is respectfully submitted that independent claim 1 of the present application is inventive.

For at least the above reasons, it is respectfully submitted that D1 to D2 do not disclose, hint or suggest the subject matter of independent claim 1 of the present application and accordingly claim1 currently on file is both novel and inventive, thereby meeting the requirements of Article 52(1) EPC, Article 54(1) and (2) EPC and Article 56 EPC. It is respectfully submitted that the examiner handling the counterpart U.S. application, which issued as U.S. Patent No. 8,401,875 considered the subject matter of claim 1 to be inventive.

**General**

Any amendments made by way of the present letter, and the observations contained herein, are made solely for the purposes of the prosecution of this European patent application and without prejudice to the applicant in other jurisdictions.

It should be noted that insofar as any subject-matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments mentioned above and/or incorporated in the new pages submitted with this letter, the Applicant wishes to reserve the right to restore such subject matter and/or file a divisional application in respect thereof.

In the event that it is intended to refuse this application, or before any adverse decision is taken, the applicant hereby requests, in order of preference, a telephone interview, a personal interview, or oral proceedings under Article 116 EPC.

Favourable reconsideration of this application is requested. It is believed that the present submission properly overcomes all remaining objections and that the application is in order for grant. However, if there are any remaining objections which may be usefully dealt with by telephone, the Examiner is invited to call me on +**353 1 231 4862**.

Yours faithfully,



Paul Keane
Representative

p.keane@frkelly.com
+353-1-2314862

Europäisches Patentamt
European Patent Office
Office européen des brevets

# Letter accompanying subsequently filed items


Representative:

**Mr Paul Keane**
**FRKELLY**
**27 Clyde Road**
**D4 Dublin**
**Ireland**

**Phone: +353 1 231 4862**
**Fax: +353 1 614 4756**
**E-mail: p.keane@frkelly.com**

80298 Munich
Germany
Tel. +49(0)89 2399-0 | Fax -4465

P.O. Box 5818
NL-2280 HV Rijswijk
Netherlands
Tel. +31(0)70 340-2040 | Fax -3016

10958 Berlin
Germany
Tel. +49(0)30 25901-0 | Fax -840


The document(s) listed below is (are) subsequently filed documents pertaining to the following application:

| | |
|---|---|
| Application number | 11752936.2 |
| Applicant's or representative's reference | P105633EP00 |

| | Description of document | Original file name | Assigned file name |
|---|---|---|---|
| 1 | Amended claims (clean copy) | P105633EP00 Claims clean May 14.pdf | CLMS-1.pdf |
| 2 | Amended claims with annotations | P105633EP00 Claims markup May 14.pdf | CLMS-HWA-1.pdf |
| 3 | Reply to examination report | P105633EP00 Response May14.pdf | EXRE3-1.pdf |

**Signatures**

Place:

Date: **14 May 2015**

Signed by: **Paul Keane 36258**

Representative name: **Paul Keane**

Capacity: **(Representative)**

**Claims**

1. A portable handheld apparatus for managing personal and secured data and documentation files stored in the apparatus while the apparatus is communicating with an external device, the apparatus comprising:

a plurality of biometric sensors for reading a plurality of personal biometric identification parameters of the user holding the apparatus, said plurality of biometric sensors being integrated within the apparatus;

at least one life signs detector integrated within the apparatus, said life signs detector being configured to measure and record at least one of said user's life sign parameters;

a first memory module in communication with said processing module and said encryption module for the storage of said user's data and documentation files;

an authentication unit configured to compare the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-recorded set of personal biometric identification parameters;

a processing module in communication with said plurality of biometric sensors, said first memory module and said authentication unit;

an encryption module in communication with the processing module;

communication and data connection means for communicating with an external device, said communication and data connection means being controlled by and in communication with said processing module;

wherein access to the personal data and documentation files stored in said first memory module is only enabled after said authentication unit positively matches each of the plurality of personal biometric identification parameters of the user holding the apparatus, with the pre-recorded set of personal identification parameters; and

wherein said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied and the operation of the apparatus is completely shut down.

2. The apparatus according to claim 1, wherein said at least one of said user's life sign parameters is measured by any of a group of life sign indicators including a body pulse rate measurement indicator, a body O2 saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator.

3. The apparatus according to claim 1,

wherein, whenever any of the group of life sign indicators detects a critical level, the apparatus is configured to:

initiate an emergency call to any of a group of registered emergency centers and send to said registered emergency centers any of a group of data files containing information associated with the user, including the identification data file of the user, personal medical file of the user, the measured set of life sign parameters of the user and location of the user, or

an emergency button in communication with said processing module and said communication and data connection means module; wherein on said emergency button being activated, communication is initiated between said apparatus and any of a group of registered emergency centers, said emergency call transmitting any of a group of data files containing information associated with the unique user of said apparatus, including the identification data of said user, the personal medical data file of said user, and location of said user; or

wherein said apparatus is configured to communicate with any of a group of service providers, said group of service providers including banks,

credit card companies, clinics, hospitals and medical insurance companies, municipal and utility entities and websites frequently accessed by said user; thereby allowing said user to access and manage personal data and documentation files, associated with said user; or

wherein said external device comprises any one of a group including a remote server, a local server, a host computer, voice or data communication means and a cellular phone; or

wherein said emergency call is initiated via any one of a group of communication means including a secured server, directly via the internet by said apparatus connection and communication means, via the internet through any host computer, via a voice and data communication device and via any cellular phone network; or

wherein said communication and data connection means comprises at least one of a group of connection and communication devices including a data interface connector attached to a host computer, a Mini USB, a compatible industrial data interface connector attached to a cellular phone, a near field wireless communication interface, a Bluetooth communication interface, a magnetic reader interface, and a smart card reader based on a contact-less communication interface using induction or RF communication; or

further comprising an stored software module that automatically detects the operating system of the computer or cellular phone connected to said apparatus through one of said group of communicating devices through which the apparatus is connected, said computer or cellular phone having keyboard and display units associated therewith, thereby allowing the user to interact with said first memory module and with said processing module of said apparatus via said keyboard and display units, whereby said computer or cellular phone is configured to utilize and interact with said memory module, said processing module and said sensor module of said apparatus.

4. A method for managing personal and secured data and documentation files of a plurality of unique users, each one of said plurality of unique users

having a personal identification unit uniquely associated with said one user for storing each user's personal data and documentation files, each of said personal identification units comprising:

a plurality of biometric sensors stored within the personal identification unit;

at least one life signs detector, stored within the personal identification unit, said life signs detector being configured to measure and record at least one of said user's life sign parameters;

a processing module in communication with said plurality of biometric sensors;

an authentication unit in communication with the processing module;

an encryption unit in communication with said processing module;

a first memory module in communication with said processing module and said encryption unit; wherein said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus while the personal identification unit are communicating with an external device and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied and the operation of the apparatus is completely shut down; and

communication and data connection means in communication with said processing module; the method comprising the steps of:

a. the plurality of biometric sensors reading a plurality of personal identification parameters of the user holding the personal identification unit;

b. at least one life signs detector, integrated within the apparatus, measuring and recording at least one of said user's life sign parameters;

c said authentication unit comparing each of the personal biological identification parameters of said user with a pre-recorded set of personal biological identification parameters stored in said authentication unit; and

d. if said authentication unit positively identifies said user, allowing said user access to said user's personal data and documentation files stored in said first memory module and allowing said user to communicate with other communication means through said personal identification unit.

5. The method of claim 4

wherein at least one of said plurality of life signs detectors includes a body pulse rate measurement indicator, a body O2 saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator, the method further comprising the steps of:

initiating an emergency call to any of a group of registered emergency centers, whenever any of the life sign indicators detects a critical level; and

wherein said emergency call transmits any of a group of data files information associated with the user, including identification of the user, personal medical data file of the user, the measured set of life sign parameters of the user and location of the user; or

wherein the method further comprises the step of:

communicating, via any one of a group of communication means, with any of a group of service providers including banks, credit card companies, clinics, hospitals and medical insurance companies, municipal and utility entities and websites frequently accessed by said user thereby allowing said user to access and manage said user's personal data and documentation files stored by said group of service providers.

6. The method of claim 4, wherein said apparatus further comprises an emergency button in communication with said processing module and said communication and data connection means, the method further comprising the steps of:

when said emergency button is activated, a call is initiated between said apparatus and any of a group of registered emergency centers; and

said emergency call transmitting any of a group of data files information associated with the user, including identification data of the user, the personal medical data file of the user, and location of the user; or

wherein the apparatus further comprises a magnetic strip element, the method further comprising the step of:

after positive authentication of said user's personal identification parameters, activating said magnetic strip thereby allowing said magnetic strip to be read by any of group of devices including a credit card reader, an ATM, a point of sale, a magnetic strip or near field communication reading device (NFC); or

wherein the apparatus further comprises a power charging and data backup device, said device comprising a charging and power unit, an electronic sub unit and a mass memory solid-state memory unit, the method further comprising the steps of:

comparing the memory content of said apparatus first memory module to the memory content of said mass memory solid-state memory unit; and

if the first memory module of the apparatus lacks data, updating the first memory module with the last version of the data stored within the solid-state memory unit; and

if said solid-state memory unit of said device lacks data, updating the solid-state memory unit of said device with the last version of the data stored within said apparatus's solid-state memory unit.

7. The method of claim 4, wherein each of said plurality of unique users is in communication with a system manager, said system manager managing a remote centralized data communication storage and management system of said plurality of unique users, the method further comprising the steps of:

a. said system manager registering each unique user and storing the personal ID data file of each unique user in a memory sub-system connected to said centralized system; and

b. said registration further includes the step wherein said system manager generates for each system user N pairs of two different randomly selected characters strings, each of said strings is a combination of n alphanumeric characters in length; and

c. said system manager storing said N pairs in said system memory sub-system and sending said n characters strings pairs to be stored in said unique user personal identification unit memory module; and

d. said personal identification unit generating a secret access code of L alphanumeric characters to be further stored in said system memory within a special partition containing the list of said secret access codes for said plurality of unique users without assigning any identification or link between the associated users to his registered secret access code.

8. The method of claim 7, wherein after registration and upon normal initiation of communication between said system manager and each unique user, said system manager further communicating with said unique user and first comparing said unique user's ID data file and said personal identification unit unique embedded characterizing serial number stored in the unique user's personal identification unit with the corresponding user's ID and personal identification data stored in said memory sub-system; and

if the two sets of identification data match;

i. said system manager sending a first string of said stored N strings of coded alphanumeric data, to said user's personal identification unit; and

ii said user personal identification unit responding with the second matching string from the same stored pair of coded alphanumeric data uniquely associated with said user personal identification unit: and

iii said system manager comparing the received second string of coded alphanumeric data with a second string of coded alphanumeric data pre-stored in the memory sub-system; and

iv. said system manager comparing for consecutive M out of N times the received additional different strings of coded alphanumeric data pre-stored in the memory of said personal identification unit associated with said unique user with the additional strings of coded alphanumeric data pre-stored in the memory of sub-system; and

v. if all M strings of coded alphanumeric data match, then said system manager declares authenticating of said unique user and permitting said unique user access to said system.

9. A system for managing personal and secured data and documentation files of a plurality of unique users, the system comprising:

a. a system manager for managing and updating personal data of said system plurality of unique users with each of said plurality of unique users; and

b. a storage system connected to said system manager to store updated personal data of each of said plurality of unique users; and

c. a plurality of personal identification units, each of said personal identification units being associated with a unique user, each unique user being registered with said system manager, each of said personal identification units comprising a storage unit configured to store the personal ID data file of each unique user and a plurality of biometric sensors for reading a plurality of personal biometric identification parameters of the user holding the apparatus, said plurality of biometric sensors being stored within the personal identification units stored within said personal identification units, said life signs detector being configured to measure and record at least one of said user's life sign parameters; wherein said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus while the personal identification unit are communicating with an external

device and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied and the operation of the personal identification unit is completely shut down; and

d. a plurality of computer hosts and cellular phones in communication with said system manager, enabling the direct connection by said system manager with said plurality of unique users through their corresponding personal identification unit; and

e. a plurality of registered emergency centers and a plurality of registered service providers in communication with said system manager, said plurality of service providers including banks, credit card companies, insurance companies, clinics, hospitals and medical insurance companies, government, municipal and utility entities and selected websites frequently accessed by said plurality of users;

wherein said system manager's access to and communication with the personal data and documentation files stored in said personal identification units associated with each said unique user and to the personal data and documentation files stored by said group of service providers is only enabled after positive authentication of each of said unique user's personal biometric identification parameters by said authentication unit and measuring the normal measured output of each one of said user's life sign parameters; and

wherein said at least one of said user's life sign parameters is measured by any of a group of life sign indicators including a body pulse rate measurement indicator, a body $O_2$ saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator.

10. The system according to claim 9, wherein each of said plurality of personal identification units comprises:

i. a sensor module comprising a plurality of biometric sensors for reading a plurality of personal biometric identification parameters of the

user holding the of personal identification units, said of personal identification units being uniquely identified with said user; and

ii. a processing module in communication with said sensor module for processing said personal identification parameters and for processing and managing the personal and secured data and documentation files associated with said user; and

iii. an authentication unit in communication with the processing module configured to receive and authenticate the identity of said user by comparing said user's personal identification parameters read by the sensor module and processed by the processing module, with a pre-recorded set of personal identification parameters stored in said authentication unit; and

iv. an encryption module in communication with said processing module for the encryption plus compression or decompression plus decryption of said user's data files; and

v. a storage unit in communication with said processing module and said encryption module for the storage of said user's data and documentation files; and

vi. communication and data connection means in communication with said processing module for connecting said plurality of personal identification units with said system manager and plurality of service providers.

11. The system according to claim 10, wherein said system manager is configured:

to communicate with said personal identification units to compare the user's ID data file stored in the unique user's personal identification units with the corresponding identification data stored in said storage unit, and

if the two sets of identification data match, then said system manager is configured to initiate a further level of security identification prior to full communication and data updating capability being enabled between said system manager and said user personal identification unit; and

wherein said further level of security identification comprises said system manager sending a first string of coded alphanumeric data uniquely associated with said user personal identification unit to said user personal identification unit, said personal identification unit responding with a second string of coded alphanumeric data uniquely associated with said user personal identification unit, and said system manager verifying the received second string of coded alphanumeric data with a second string of coded alphanumeric data pre-stored in the memory sub-system; and

said system manager comparing for full matching for N consecutive times received additional different strings of coded alphanumeric data pre-stored in the memory of said personal identification unit associated with said unique user with counter generated additional strings of coded alphanumeric data pre-stored in the memory of sub-system; or

wherein each personal identification unit further comprises an emergency button in communication with said proccssing module and said communication and data connection means module;

wherein the personal identification unit is configured to transfer any of a group of data files containing information associated with the user, including files such as the identification data of the user, personal medical data file of the user, the measured set of life sign parameters of the user, associated with the user and an updated location of the user; and

wherein the personal identification unit is configured to initiate an emergency call to any of said plurality of registered emergency centers, whenever said emergency button is activated or whenever any of the group of life sign indicators detects a critical level.

12. The system of claim 9, wherein said system, further comprises:

a computerized call center configured to receive phone calls or emergency voice and data messages from any of said plurality of registered emergency centers and a plurality of registered service providers and to communicate with any of said plurality of cellular phone and host computers; and

wherein said call center is configured to communicate the user's location coordinates to an emergency rescue team and simultaneously said call center is configured to communicate with any of said plurality of registered emergency centers and service providers to receive said user's updated medical data and to transfer said data to and from the user's personal identification unit.

**Claims**

1. A portable handheld Aapparatus for managing personal and secured data and documentation files stored in the apparatus while the apparatus is communicating with an external device, the apparatus comprising:

a plurality of biometric sensors for reading a plurality of personal biometric identification parameters of the user holding the apparatus, said plurality of biometric sensors being ~~stored~~integrated within the apparatus;

at least one life signs detector ~~stored~~integrated within the apparatus, said life signs detector being configured to measure and record at least one of said user's life sign parameters;

a first memory module in communication with said processing module and said encryption module for the storage of said user's data and documentation files;

an authentication unit configured to compare the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-recorded set of personal biometric identification parameters;

a ~~processor~~processing module in communication with said plurality of biometric sensors, said first memory module and said authentication unit;

an encryption module in communication with the processing module;

communication and data connection means for communicating with an external device, said communication and data connection means being controlled by and in communication with said processing module;

wherein access to the personal data and documentation files stored in said first memory module is only enabled after said authentication unit positively matches each of the plurality of personal biometric identification

parameters of the user holding the apparatus, with the pre-recorded set of personal identification parameters; and

wherein said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied and the operation of the apparatus is completely shut down. ~~wherein, whenever any of said at least one life signs detector detects a critical level of said user measured life sign parameters, the apparatus is configured to prevent access to said user's personal data and documentation files stored in said first memory module.~~

2. The apparatus according to claim 1, ~~wherein said plurality of biometric sensors are configured to continuously read a plurality of personal identification parameters associated with said user holding the apparatus and in the event that a change occurs in any of the plurality of personal identification parameters, access to the stored personal data files is denied and the operation of the apparatus is completely shut down; or~~

wherein said at least one of said user's life sign parameters is measured by any of a group of life sign indicators including a body pulse rate measurement indicator, a body O2 saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator.

3. The apparatus according to claim 1, ~~further comprising:~~

~~communication and data connection means for communicating with an external device, said communication and data connection means being controlled by and in communication with said processor; or~~

wherein, whenever any of the group of life sign indicators detects a critical level, the apparatus is configured to:

initiate an emergency call to any of a group of registered emergency ~~medical or security~~ centers and send to said registered emergency

Formatted: Claims2

Formatted: Claims

centers any of a group of data files containing information associated with the user, including the identification data file of the user, personal medical file of the user, the measured set of life sign parameters of the user and location of the user, or

~~the apparatus further comprises an eneryption unit in communication with said processor for the eneryption plus compression and for the decompression plus deeryption of said user's data files; or~~

an emergency button in communication with said ~~processor~~processing module and said communication and data connection means module; wherein on said emergency button being activated, communication is initiated between said apparatus and any of a group of registered emergency centers, said emergency call transmitting any of a group of data files containing information associated with the unique user of said apparatus, including the identification data of said user, the personal medical data file of said user, and location of said user; or~~,~~

wherein said apparatus is configured to communicate with any of a group of service providers, said group of service providers including banks, credit card companies, clinics, hospitals and medical insurance companies, municipal and utility entities and websites frequently accessed by said user; thereby allowing said user to access and manage personal data and documentation files, associated with said user; or

wherein said external device comprises any one of a group including a remote server, a local server, a host computer, voice or data communication means and a cellular phone; or

wherein said emergency call is initiated via any one of a group of communication means including a secured server, directly via the internet by said apparatus connection and communication means, via the internet through any host computer, via a voice and data communication device and via any cellular phone network; or

wherein said communication and data connection means comprises at least one of a group of connection and communication devices including a

data interface connector attached to a host computer, a Mini USB, a compatible industrial data interface connector attached to a cellular phone, a near field wireless communication interface, a Bluetooth communication interface, a magnetic reader interface, and a smart card reader based on a contact-less communication interface using induction or RF communication; or

further comprising an stored software module that automatically detects the operating system of the computer or cellular phone connected to said apparatus through one of said group of communicating devices through which the apparatus is connected, said computer or cellular phone having keyboard and display units associated therewith, thereby allowing the user to interact with said first memory module and with said ~~processor~~processing module of said apparatus via said keyboard and display units, whereby said computer or cellular phone is configured to utilize and interact with said memory module, said ~~processor~~processing module and said sensor module of said apparatus.

4. A method for managing personal and secured data and documentation files of a plurality of unique users, each one of said plurality of unique users having a personal identification unit uniquely associated with said one user for storing each user's personal data and documentation files, each of said personal identification units comprising:

a plurality of biometric sensors stored within the personal identification unit;

at least one life signs detector, stored within the personal identification unit, said life signs detector being configured to measure and record at least one of said user's life sign parameters;

a ~~processor~~processing module in communication with said plurality of biometric sensors;

an authentication unit in communication with the ~~processor~~processing module;

an encryption unit in communication with said ~~processor~~processing module;

a first memory module in communication with said ~~processor~~processing module and said encryption unit; wherein said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus while the personal identification unit are communicating with an external device and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied and the operation of the apparatus is completely shut down; and

communication and data connection means in communication with said ~~processor~~processing module;the method comprising the steps of:

a. the plurality of biometric sensors reading a plurality of personal identification parameters of the user holding the personal identification unit;

b. at least one life signs detector, ~~stored~~integrated within the apparatus, measuring and recording at least one of said user's life sign parameters;

c said authentication unit comparing each of the personal biological identification parameters of said user with a pre-recorded set of personal biological identification parameters stored in said authentication unit; and

d. if said authentication unit positively identifies said user, allowing said user access to said user's personal data and documentation files stored in said first memory module and allowing said user to communicate with other communication means through said personal identification unit.

5. The method of claim 4 ~~further comprising the steps of: said biometric sensors continuously reading a plurality of personal biological identification parameters of said user holding the apparatus; and~~

~~in the event that a significant change occurs in any of the plurality of personal biological identification parameters of said least one of said life signs detectors, denying access to the stored personal data files and completely shutting down the operation of said apparatus; or~~

wherein at least one of said plurality of life signs detectors includes a body pulse rate measurement indicator, a body O2 saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator, the method further comprising the steps of:

initiating an emergency call to any of a group of registered emergency centers, whenever any of the life sign indicators detects a critical level; and

wherein said emergency call transmits any of a group of data files information associated with the user, including identification of the user, personal medical data file of the user, the measured set of life sign parameters of the user and location of the user; or

wherein the method further comprises the step of:

communicating, via any one of a group of communication means, with any of a group of service providers including banks, credit card companies, clinics, hospitals and medical insurance companies, municipal and utility entities and websites frequently accessed by said user thereby allowing said user to access and manage said user's personal data and documentation files stored by said group of service providers.

6. The method of claim 4, wherein said apparatus further comprises an emergency button in communication with said ~~processor~~processing module and said communication and data connection means, the method further comprising the steps of:

when said emergency button is activated, a call is initiated between said apparatus and any of a group of registered emergency centers; and

said emergency call transmitting any of a group of data files information associated with the user, including identification data of the user, the personal medical data file of the user, and location of the user; or

wherein the apparatus further comprises a magnetic strip element, the method further comprising the step of:

after positive authentication of said user's personal identification parameters, activating said magnetic strip thereby allowing said magnetic strip to be read by any of group of devices including a credit card reader, an ATM, a point of sale, a magnetic strip or near field communication reading device (NFC); or

wherein the apparatus further comprises a power charging and data backup device, said device comprising a charging and power unit, an electronic sub unit and a mass memory solid-state memory unit, the method further comprising the steps of:

comparing the memory content of said apparatus first memory module to the memory content of said mass memory solid-state memory unit; and

if the first memory module of the apparatus lacks data, updating the first memory module with the last version of the data stored within the solid-state memory unit; and

if said solid-state memory unit of said device lacks data, updating the solid-state memory unit of said device with the last version of the data stored within said apparatus's solid-state memory unit.

7. The method of claim 4, wherein each of said plurality of unique users is in communication with a system manager, said system manager managing a remote centralized data communication storage and management system of said plurality of unique users, the method further comprising the steps of:

a. said system manager registering each unique user and storing the personal ID data file of each unique user in a memory sub-system connected to said centralized system; and

b. said registration further includes the step wherein said system manager generates for each system user N pairs of two different randomly

selected characters strings, each of said strings is a combination of n alphanumeric characters in length; and

c. said system manager storing said N pairs in said system memory sub-system and sending said n characters strings pairs to be stored in said unique user personal identification unit memory module; and

d. said personal identification unit generating a secret access code of L alphanumeric characters to be further stored in said system memory within a special partition containing the list of said secret access codes for said plurality of unique users without assigning any identification or link between the associated users to his registered secret access code.

8. The method of claim 7, wherein after registration and upon normal initiation of communication between said system manager and each unique user, said system manager further communicating with said unique user and first comparing said unique user's ID data file and said personal identification unit unique embedded characterizing serial number stored in the unique user's personal identification unit with the corresponding user's ID and personal identification data stored in said memory sub-system; and

if the two sets of identification data match;

i. said system manager sending a first string of said stored N strings of coded alphanumeric data, to said user's personal identification unit; and

ii said user personal identification unit responding with the second matching string from the same stored pair of coded alphanumeric data uniquely associated with said user personal identification unit: and

iii said system manager comparing the received second string of coded alphanumeric data with a second string of coded alphanumeric data pre-stored in the memory sub-system; and

iv. said system manager comparing for consecutive M out of N times the received additional different strings of coded alphanumeric data pre-stored in the memory of said personal identification unit associated with

said unique user with the additional strings of coded alphanumeric data pre-stored in the memory of sub-system; and

v. if all M strings of coded alphanumeric data match, then said system manager declares authenticating of said unique user and permitting said unique user access to said system.

9. A system for managing personal and secured data and documentation files of a plurality of unique users, the system comprising:

a. a system manager for managing and updating personal data of said system plurality of unique users with each of said plurality of unique users; and

b. a storage system connected to said system manager to store updated personal data of each of said plurality of unique users; and

c. a plurality of personal identification units, each of said personal identification units being associated with a unique user, each unique user being registered with said system manager, each of said personal identification units comprising a storage unit configured to store the personal ID data file of each unique user and a plurality of biometric sensors for reading a plurality of personal biometric identification parameters of the user holding the apparatus, said plurality of biometric sensors being stored within the personal identification units stored within said personal identification units, said life signs detector being configured to measure and record at least one of said user's life sign parameters; wherein said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus while the personal identification unit are communicating with an external device and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied and the operation of the personal identification unit is completely shut down; and

d. a plurality of computer hosts and cellular phones in communication with said system manager, enabling the direct connection by said system

manager with said plurality of unique users through their corresponding personal identification unit; and

**e.** a plurality of registered emergency centers and a plurality of registered service providers in communication with said system manager, said plurality of service providers including banks, credit card companies, insurance companies, clinics, hospitals and medical insurance companies, government, municipal and utility entities and selected websites frequently accessed by said plurality of users;

wherein said system manager's access to and communication with the personal data and documentation files stored in said personal identification units associated with each said unique user and to the personal data and documentation files stored by said group of service providers is only enabled after positive authentication of each of said unique user's personal biometric identification parameters by said authentication unit and measuring the normal measured output of each one of said user's life sign parameters; and

wherein said at least one of said user's life sign parameters is measured by any of a group of life sign indicators including a body pulse rate measurement indicator, a body $O_2$ saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator.

10. The system according to claim 9, wherein each of said plurality of personal identification units comprises:

i. a sensor module comprising a plurality of biometric sensors for reading a plurality of personal biometric identification parameters of the user holding the of personal identification units, said of personal identification units being uniquely identified with said user; and

ii. a ~~processor~~processing module in communication with said sensor module for processing said personal identification parameters and for processing and managing the personal and secured data and documentation files associated with said user; and

iii. an authentication unit in communication with the ~~processor~~processing module configured to receive and authenticate the identity of said user by comparing said user's personal identification parameters read by the sensor module and processed by the ~~processor~~processing module, with a pre-recorded set of personal identification parameters stored in said authentication unit; and

iv. an encryption module in communication with said ~~processor~~processing module for the encryption plus compression or decompression plus decryption of said user's data files; and

v. a storage unit in communication with said ~~processor~~processing module and said encryption module for the storage of said user's data and documentation files; and

vi. communication and data connection means in communication with said ~~processor~~processing module for connecting said plurality of personal identification units with said system manager and plurality of service providers.

11. The system according to claim 10, wherein said system manager is configured:

to communicate with said personal identification units to compare the user's ID data file stored in the unique user's personal identification units with the corresponding identification data stored in said storage unit, and

if the two sets of identification data match, then said system manager is configured to initiate a further level of security identification prior to full communication and data updating capability being enabled between said system manager and said user personal identification unit; and

wherein said further level of security identification comprises said system manager sending a first string of coded alphanumeric data uniquely associated with said user personal identification unit to said user personal identification unit, said personal identification unit responding with a second string of coded alphanumeric data uniquely associated with said user personal identification unit, and said system manager verifying the received

second string of coded alphanumeric data with a second string of coded alphanumeric data pre-stored in the memory sub-system; and

said system manager comparing for full matching for N consecutive times received additional different strings of coded alphanumeric data pre-stored in the memory of said personal identification unit associated with said unique user with counter generated additional strings of coded alphanumeric data pre-stored in the memory of sub-system; or

~~wherein said plurality of biometric sensors continuously read a plurality of personal biometric identification parameters associated with the user holding his unique personal identification units and in the event that a change occurs in any of the plurality of personal biological biometric identification parameters, access to the stored personal data files is denied and the operation of said identification units is completely shut down; or~~

wherein each personal identification unit further comprises an emergency button in communication with said ~~processor~~processing module and said communication and data connection means module;

wherein the personal identification unit is configured to transfer any of a group of data files containing information associated with the user, including files such as the identification data of the user, personal medical data file of the user, the measured set of life sign parameters of the user, associated with the user and an updated location of the user; and

wherein the personal identification unit is configured to initiate an emergency call to any of said plurality of registered emergency centers, whenever said emergency button is activated or whenever any of the group of life sign indicators detects a critical level.

12. The system of claim 9, wherein said system, further comprises:

a computerized call center configured to receive phone calls or emergency voice and data messages from any of said plurality of registered emergency centers and a plurality of registered service providers and to communicate with any of said plurality of cellular phone and host computers; and

wherein said call center is configured to communicate the user's location coordinates to an emergency rescue team and simultaneously said call center is configured to communicate with any of said plurality of registered emergency centers and service providers to receive said user's updated medical data and to transfer said data to and from the user's personal identification unit.

Europäisches Patentamt
European Patent Office
Office européen des brevets

# Acknowledgement of receipt

We hereby acknowledge receipt of the following subsequently filed document(s):

| | |
|---|---|
| Submission number | 3497923 |
| Application number | EP11752936.2 |
| Date of receipt | 14 May 2015 |
| Receiving Office | European Patent Office, The Hague |
| Your reference | P105633EP00 |
| Applicant | All applicants as on file |
| Documents submitted | package-data.xml<br>epf1038.pdf (1 p.)<br>CLMS-HWA-1.pdf\P105633EP00 Claims markup May 14.pdf (13 p.)<br>ep-sfd-request.xml<br>CLMS-1.pdf\P105633EP00 Claims clean May 14.pdf (12 p.)<br>EXRE3-1.pdf\P105633EP00 Response May14.pdf (5 p.) |
| Submitted by | CN=Paul Keane 36258 |
| Method of submission | Online |
| Date and time receipt generated | 14 May 2015, 13:22 (CEST) |
| Message Digest | AD:4C:34:92:63:02:E5:A0:13:C6:2A:5E:A2:AE:BC:EC:A8:1F:FE:5B |

**Correction by the EPO of errors in debit instructions filed by eOLF**
Errors in debit instructions filed by eOLF that are caused by the editing of Form 1038E entries or the continued use of outdated software (all forms) may be corrected automatically by the EPO, leaving the payment date unchanged (see decision T 152/82, OJ EPO 1984, 301 and point 6.3 ff ADA, Supplement to OJ EPO 10/2007).

/European Patent Office/

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
80298 MUNICH
GERMANY

**Questions about this communication ?**
Contact Customer Services at www.epo.org/contact

Coyle, Philip Aidan
F. R. Kelly & Co.
27 Clyde Road
Ballsbridge
Dublin 4
IRLANDE

Date
14-10-2015

| Reference | Application No./Patent No. |
|---|---|
| p105633ep00 | 11752936.2 - 1955 / 2545485 |

Applicant/Proprietor
OS - New Horizon Personal Computing Solutions Ltd.

**Summons to attend oral proceedings pursuant to Rule 115(1) EPC**

You are hereby summoned to attend oral proceedings arranged in connection with the above-mentioned European patent application.

The matters to be discussed are set out in the communication accompanying this summons (EPO Form 2906).

The oral proceedings, which will not be public, will take place before the Examining Division

on 13.04.16 at 09.30 hrs at the EPO in Rijswijk.
Rijswijk Main, Van Benthemlaan 16 , NL-2288 HV Rijswijk (ZH)

The actual room number and dedicated waiting area will be indicated to you at the reception desk, Van Benthemlaan 16.

**You are asked to report at the reception desk in good time before the starting time mentioned above. In particular, please take into account the relocation of the EPO main entrance as from autumn 2014 due to construction works (see OJ EPO 2014, A90 and www.epo.org).**

No changes to the date of the oral proceedings can be made, except on serious grounds (see OJ EPO 1/2009, 68). If you do not appear as summoned, the oral proceedings may continue without you (R. 115(2) EPC, see also OJ EPO 10/2008, 471).

Your attention is drawn to Rule 4 EPC, regarding the language of the oral proceedings, and to the Special edition No. 3 OJ EPO 2007, L.1., concerning the filing of authorisations for company employees and lawyers acting as representatives before the EPO.

**The final date for making written submissions and/or amendments (R. 116 EPC) is 11.03.16.**

| 1st Examiner: | 2nd Examiner: | Chairman: |
|---|---|---|
| Arbutina L | Sigolo A | van Praagh K |

**For the Examining Division**

Annexes:
Confirmation of receipt (Form 2936)
Communication (EPO Form 2906)
EP1914649, US2008/0059236

**Registered letter with advice of delivery**
EPO Form 2008 07.15 [ORAL03=A000] (09/10/15)

to EPO postal service: 09.10.15

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
Postbus 5818
2280 HV Rijswijk
NETHERLANDS
Tel: +31 70 340 2040
Fax: +31 70 340 3016

4. Request language service to provide simultaneous interpretation facilities as necessary

..... Date ..... Initials

5. Return the dossier to primary examiner with Form 2041 (15 days before the oral proceedings)

..... Date ..... Initials

6. Check that summons has been received (Form 2936 / advice of delivery)

7. 15 days before the oral proceedings:
- dispatch the dossier to the primary examiner.

28/9/2015
Date

| van Praagh, Kay | Sigolo, Alessandro | Arbutina, Ljiljana | |
|---|---|---|---|
| Chairman | 2nd examiner | 1st examiner | Legal member |

Enclosure(s):
EP 1 914 649
US 2008/059236

The examination is being carried out on the **following application documents**

**Description, Pages**

1-60 as published

**Claims, Numbers**

1-12 filed in electronic form on 14-05-2015

**Drawings, Sheets**

1/9-9/9 as published

Reference is made to the following documents used in the course of the procedure:

D1: US 2009/083847 A1 (FADELL ANTHONY [US] ET AL) 26 March 2009 (2009-03-26)

D2: US 5 229 764 A (MATCHETT NOEL D [US] ET AL) 20 July 1993 (1993-07-20)

D3: US 6 957 337 B1 (CHAINER TIMOTHY JOSEPH [US] ET AL) 18 October 2005 (2005-10-18)

The following documents are cited by the examining division. A copy of the documents is annexed to the communication.

D4 EP 1 914 649 A2 (ST MICROELECTRONICS INC [US]) 23 April 2008 (2008-04-23)

D5 US 2008/059236 A1 (CARTIER JOSEPH C [US]) 6 March 2008 (2008-03-06)

**Added Subject-Matter**

1. The amendments filed electronically on 14.05.2015 introduce subject-matter which extends beyond the content of the application as filed, contrary to Article 123(2) EPC. The amendments concerned are the following:

1.1. Claims 1, 4 and 9, amendment "while the apparatus is communicating with an external device"

For this amendment the applicant identified in his letter of reply dated 14.05.2015 (referred in the further communication as R1) the support on page 18, lines 13-17. The cited passage reads:

"FIG. 4 is a schematic illustration of an embodiment of the present invention related to one possible flowchart of the process for the use of the invention apparatus while interphasing to a cellular phone or a host personal computer for activation of various operations between the cellular phone and the apparatus, while using the cellular phone or the host computer display and keyboard hardware and functions;"

The examining division notes that neither

i) "managing personal and secured data and documentation files stored in the apparatus while the apparatus is communicating with an external device" (claim 1), nor

ii) "biometric sensors continuously reading a plurality of personal biological identification parameters associated with said user holding the apparatus while the apparatus is communicating with an external device" (claims 4 and 9)

is directly and unambiguously derivable from this passage.

The applicant indicated in R1, page 3, 5th paragraph, that this amendment was introduced for clarification. However, it introduces new subject-matter for the following reason:

First, it should be noted that in claim 1, in feature i) cited here above, it is not clear to which phase of managing personal and secured data and documentation files stored in the apparatus refers the limitation "while the apparatus is communicating with an external device". It would even appear that the amendment does not further limit the claimed scope. Indeed, the apparatus is claimed as being "for managing personal and secured data and documentation files stored in the apparatus", so it is reasonable to assume that it is managing the data always, therefore also "while the apparatus is communicating with an external device", as claimed. In this sense, the subject-matter of claim 1 is not compliant with Art.84.

However, from claims 4 and 9, feature ii) cited here above, it is clear that the amendment is associated with biometric reading. The examining division acknowledges that the application as filed discloses that there are periods of time in which the biometric sensors are continuously reading a plurality of personal biological identification parameters, and that there are periods when the apparatus is communicating with an external device. However, the application as filed does not disclose, nor is it directly and unambiguously derivable from it, that these two periods overlap, as claimed.

1.2. Claim 1, amendment "communication and data connection means for communicating with an external device, said communication and data connection means being controlled by and in communication with said processing module"

The applicant indicated in R1 step (f) of the original PCT claim 1 as support for this amendment. The feature (f) reads:

"communication and data connection means in communication with said processing module for connecting said apparatus with an external device".

As can be seen, this feature discloses that the communication and data connection means is in communication with said processing module, but not controlled by it.

1.3. Claims 1 and 4 (originally filed claim 1 and 21) were amended with originally filed claims 2 and 22 respectively. The features of the present claims 2 and 3, as well as claims 5-8, were originally in claim trees separate from the trees 1-2 and 21-22. Therefore, the subject-matter of claims 2, 3, 5-8 contains a new combination of features, which was not disclosed in the application as filed. In a similar way, the present claims 11 and 12 contain combination of originally filed claim 35 with the features of originally filed claims 34, 36 and 37, which were not disclosed in combination in the application as originally filed.

**Inventive Step**

2. The subject-matter of claims 1 and 4 (excluding the features infringing Art.123(2) EPC) does not involve an inventive step within the meaning of Article 56 EPC, for the following reason:

2.1. Document D1 discloses in accordance with the features of claim 1 (the references in parentheses applying to this document) a portable handheld apparatus for managing personal and secured data and documentation files stored in the apparatus (par.[0002] and [0003], lines 1-8), the apparatus comprising:

a plurality of biometric sensors for reading a plurality of personal biometric identification parameters of the user holding the apparatus, said plurality of biometric sensors being integrated within the apparatus (par.[0028], lines 1-5);

at least one life signs detector integrated within the apparatus, said life signs detector being configured to measure and record at least one of said user's life sign parameters (par.[0057]);

a first memory module in communication with said processing module for the storage of said user's data and documentation files (fig.1, elements 104 Storage and 106 Memory);

an authentication unit configured to compare the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-recorded set of personal biological biometric identification parameters (fig.1, element 112 Authentication System; lines 1-4 of par.[0041] and lines 11-13 of par.[0079]);

a processing module in communication with said plurality of biometric sensors, said first memory module and said authentication unit (fig.1, element 102, Processor; par. [0030], lines 1-3, and par.[0040]);

communication and data connection means for communicating with an external device, said communication and data connection means being controlled by and in communication with said processing module (fig.1, element 108, Communication Circuitry; par.[0033], lines 1-3);

wherein access to the personal data and documentation files stored in said first memory module is only enabled after said authentication unit positively matches each of the plurality of personal biometric biological identification parameters of the user holding the apparatus with the pre-recorded set of personal biological identification parameters (par.[0028] and [0095]).

2.2. The difference between the subject-matter of claim 1 and D1 is in the following:

a) an encryption module in communication with the processing module and the memory module; and

b) said plurality of biometric sensors are configured to continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied and the operation of the apparatus is completely shut down.

2.3. The above identified features represent a mere juxtaposition of features, not producing any working inter-relationship, and will therefore be analyzed separately (see Guidelines, G-VII, 5.2, last paragraph, and Annex, 2.1).

2.3.1. Considering feature a), the use of encryption for data protection is a well-known technique, and as such cannot be considered as having inventive contribution over the prior art.

2.3.2. Considering feature b), the technical effect is that turning over to an unauthorized user during an authorized session is prevented. Therefore, the objective technical problem to be solved can be formulated as to how to prevent turning over to an unauthorized user during an authorized session. This problem was solved in D2, see col.2, lines 58-61. Thus, a skilled person confronted with the above specified problem would identify D2 in the prior art, since it solves the problem at hand, and would use its teaching, which consists in continuously reading biometric data of the user, and shutdown of the system if the change in biometric data occurs after more

than a prescribed number of comparison tests, see D2, col.4, line 55 - col.5, line 6. When applying this teaching in the system of D1, it would be a matter of design choice to apply the continuous reading for the plurality of biometric sensors in D1, and to select 1 for the prescribed number of comparison tests. It is noted that the shutdown of the system implies denial of all the services provided by the system, therefore also the access the stored personal data. Therefore, starting from D1, and using the teaching of D2 to solve the problem of preventing the turn over to an unauthorized user during an authorized session, a skilled person would arrive to the subject-matter of claim 1 without using any inventive skills.

The same reasoning applies, mutatis mutandis, to corresponding method claim 4.

**Applicant's Arguments**

3. The applicant argues in R1, page 3, 3rd and 4th paragraphs, that the essential feature of the invention is in separating the user's sensitive data storage and management functions from the cell phone. He then alleges that D1 is not the closest prior art, since it fails to provide the sensitive information on a separate device to that with cellular functionality.

3.1. The examining division is of the opinion that in the case of the present application there are several valid points for the assessment of inventive step, because, firstly, the application indicates plurality of problems (multiple hardware token generators on page 3, lines 7-8; a third party with negative intentions getting access to a user's secured data, and connectivity to mobile phones on page 4, last four lines; capability to sense a live person, page 5, lines 5-6; initiating an emergency call, page 5, lines 15-17, to mention a few), and, secondly, even the applications mentions portable memories (page 3), and modern cellular phones (page 6) as the prior art. In such a case, according to Guidelines, G-VII, 5.1, 2nd paragraph, there is no need to discuss which document is "closest" to the invention; the only relevant question is whether the document used is a feasible starting point for assessing inventive step. The examining division is of the opinion that it is, since the application itself indicates modern cellular phones as a prior art, and since D1 deals with a generic problem of protecting personal data, see D1, lines 1-6 of par.[0003], which, according to the title, also appears to be the subject the subject of interest of the present application.

3.2. Furthermore, the examining division notes that there are no features in the claim that correspond to separating the user's sensitive data storage and management functions from the cell phone. However, since the applicant indicated this feature as being essential for his invention, it may be expected that further amendments will be

made in this direction. For the efficiency reasons, two further documents D4 and D5 are cited, which the examining division may decide to use, depending on the amendments.

4. The applicant further argues in R1, page 4, that it is mandatory under the EPC that the examiner demonstrates why one skilled in the art **would, not just could**, arrive at the claimed invention starting with the closest prior art, citing G-VII, 5.3, and G-VII, 8.

The examining division notes that in the inventive step assessment given here above in paragraph 3. the problem-and-solution approach was used, which is a well established practice used precisely for this purpose, namely, to ensure that one skilled in the art **would, not just could**, arrive at the claimed invention. As argued here above 2.3.2, the incentive that shows that a skilled person would have combined the elements from the prior art is in document D2, which solves the identified objective technical problem.

**Unity of Invention**

5. The application lacks unity within the meaning of Article 82 EPC, for the following reasons:

5.1. As shown here above in paragraph 3., the independent claims 1 and 4 lack inventive step, leaving he dependent claims 2, 3, 5-8, and independent claim 9 without a common inventive concept. The six inventions addressed by these claims are identified as follows:

5.2. From the comparison between the first invention (claim 2 and part of claim 5) and the prior art, the following features can be seen as making a contribution over the prior art:
said at least one of said user's life sign parameters is measured by any of a group of life sign indicators including a body pulse rate measurement indicator, a body 02 saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator.

Therefore, the objective problem to be solved by the first invention can be identified as how to implement the life sign detector.

5.3. From the comparison between the second invention (part of claims 3 and part of claims 5 and 6) and the prior art, the following features can be seen as making a contribution over the prior art:

whenever life sign indicator detects a critical level, or an emergency button of the apparatus is being activated, communication is initiated between said apparatus and any of a group of registered emergency centers, transmitting any of a group of data files containing information associated with the unique user of said apparatus.

The technical effect of this difference is that emergency services get information related to the user. Therefore, the objective problem to be solved by the second invention can be summarized as how to provide user related data to emergency services.

5.4. From the comparison between the third invention (part of claim 3) and the prior art, the following features can be seen as making a contribution over the prior art:

the apparatus comprises an integrated software module that automatically detects the operating system of the computer or cellular phone connected to said apparatus through one of said group of communicating devices through which the apparatus is connected, said computer or cellular phone having keyboard and display units associated therewith, thereby allowing the user to interact with said memory module and with said processing module of said apparatus via said keyboard and display units, whereby said computer or cellular phone is configured to utilize and interact with said memory module, said processing module and said sensor module of said apparatus.

The technical effect of this difference is that the keyboard and display of the host can be used, thereby simplifying the apparatus itself. Therefore, the objective problem to be solved by the third invention can be summarized as how to enable using of the keyboard and display of another device.

5.5. From the comparison between the fourth invention (part of claim 6) and the prior art, the following features can be seen as making a contribution over the prior art:

a magnetic strip element, wherein after positive authentication of said user's identification parameters, said magnetic strip is activated thereby allowing said magnetic strip to be read by any of group of devices including a credit card reader, an ATM, a point of sale, a magnetic strip or near field communicating reading device.

The technical effect of this difference is that apparatus can be connected to devices with a magnetic strip reader. Therefore, the objective problem to be solved by the fourth invention can be summarized as how to connect to a magnetic strip interface.

5.6. From the comparison between the fifth invention (part of claim 6) and the prior art, the following features can be seen as making a contribution over the prior art:
a power charging and data backup device, said device comprising a charging and power unit, an electronic sub unit and a mass memory solid-state memory unit, the method further comprising the steps of:
comparing the memory content of said apparatus first storage unit to the memory

content of said mass memory solid-state memory unit; and
if the first storage unit of the apparatus lacks data, updating the first storage unit with the last version of the data stored within the solid-state memory unit; and
if said solid-state memory unit of said device lacks data, updating the solid-state memory unit of said device with the last version of the data stored within said apparatus's solid-state memory unit.

The technical effect of this difference is that the apparatus gets charged and data updated. Therefore, the objective problem to be solved by the fifth invention can be summarized as how to charge the apparatus and update the data.

5.7. From the comparison between the sixth invention (claim 7 and part of claim 9) and the prior art, the following features can be seen as making a contribution over the prior art:

a system manager for managing and updating personal data of said system plurality of unique users and for full-duplex communication with each of said plurality of unique users and a plurality of service providers; and
a storage system connected to said system manager to store updated personal data of each of said plurality of unique users; and

a plurality of personal identification units, each of said personal identification units being associated with a unique user, each unique user being registered with said system manager; and
a plurality of computer hosts and cellular phones in communication with said system manager, enabling the direct connection by said system manager with said plurality of unique users through their corresponding personal identification unit;

said system manager registering each unique user and storing the personal ID data file of each unique user in a memory sub-system connected to said centralized system; and
said registration further includes the step wherein said system manager generates for each system user N pairs of two different randomly selected characters strings, each of said strings is a combination of n alphanumeric characters in length; and
said system manager storing said N pairs in said system memory sub-system and sending said n characters strings pairs to be stored in said unique user personal identification unit memory module; and
said personal identification unit generating a secret access code of L alphanumeric characters to be further stored in said system memory within a special partition containing the list of said secret access codes for said plurality of unique users without assigning any identification or link between the associated users to his registered secret access code; and

wherein said system manager's access to and communication with the personal data and documentation files stored in said personal identification units associated with each said unique user and to the personal data and documentation files stored by said group of service providers is only enabled after positive authentication of each of said unique user's personal biometric biological identification parameters by said authentication unit and measuring the normal measured output of each one of said user's life sign parameters;
The technical effect of this difference is the centralized management of personal data of the user. Therefore, the objective problem to be solved by the sixth invention can be summarized as how to provide centralized data management.

5.8. The above analysis shows that the special technical features disclosed by the identified six inventions are not the same. Furthermore, a comparison of the objective problems shows that these objective problems are different and have no corresponding technical effect. Consequently, the technical relationship between the subject-matter of claims belonging to the four identified inventions, required by Rule 30, is lacking, and the requirement for the unity of invention referred to in Article 82 EPC is not fulfilled.

**Applicant's Arguments**

6. In R1, page 2, the applicant identified four differentiating features between the claim and the prior art, as follows:

1) a portable handheld apparatus for managing personal and secured data and documentation files stored in the apparatus while the apparatus is communicating with an external device;

2) an encryption module in communication with said processing module;

3) communication and data connection means for communicating with an external device, said communication and data connection means being controlled by and in communication with said processing module;

4) wherein said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied and the operation of the apparatus is completely shut down.

The applicant further alleges that the lack of unity can only arise if claim 1 lacks novelty in light of D1.

In reply, the examining division notes that, to the extent that the subject-matter is allowable, the features 1) and 3) are present in D1. Anyhow, according to the Guidelines, F-V, 7., the unity of invention "a posteriori" should be assessed in the case that there is novelty *or inventive step* in an independent claim, which is the case of the present invention.

**Closing Remarks**

7.0. Since after a couple of exchanged communications no common understanding on main issues could be reached, the examining division is of the view that, for efficiency reasons, oral proceedings are the appropriate next procedural step.

7.1. In the case of further amendments submitted to the examining division, the applicant should be aware that any amendments will be allowed into the procedure at the examining division's discretion (Rule 137(3) EPC).

7.2.In order to facilitate the examination of the conformity of the amended application with the requirements of Article 123(2) EPC, the applicant is requested to clearly identify the amendments carried out, irrespective of whether they concern amendments by addition, replacement or deletion, and to indicate the passages of the application as filed on which these amendments are based.

7.3. In case of amendments, the applicant is also invited to specify in an accompanying letter the **technical difference** between the independent claims and the prior art, what **technical problem** is solved by said difference, and why the proposed solution is **not obvious** to the skilled person.

7.4. Whilst the examining division is aware of the need for economy and the costs linked to the presence of parties at Oral Proceedings, as well as the costs borne by the EPO, it is their view that this is the most appropriate course of action in the present case. Should the applicant so wish, an appealable decision on the file as it stands may be requested. Such a decision is given in standard form, referring to the previous communications including objections to which the applicant has had opportunity to comment and to the request, which must be made in writing (see GL C V 15 and E IX 4.4). In the event of timely request and issuance of such a decision, the Oral Proceedings would no longer take place. The applicant should realise that filing further amendment or argumentation in response to the summons to oral proceedings may preclude the examining division from acceding to such a request.

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
80298 MUNICH
GERMANY

**Questions about this communication ?**
Contact Customer Services at **www.epo.org/contact**

Coyle, Philip Aidan
F. R. Kelly & Co.
27 Clyde Road
Ballsbridge
Dublin 4
IRLANDE

Date
14-10-2015

| Reference | Application No./Patent No. |
|---|---|
| p105633ep00 | 11752936.2 - 1955 / 2545485 |

Applicant/Proprietor
OS - New Horizon Personal Computing Solutions Ltd.

EPA/EPO/OEB Formblatt/Form/Formulaire : 2008, 2906, EP1914649, US2008/0059236

**Empfangsbescheinigung über den Zugang des vorstehend bezeichneten Schriftstücks**
**Acknowledgement of receipt of the document specified above**
**Récépissé du document spécifié ci-dessus**

Unter Bezugnahme auf die Mitteilung im ABl EPA 7/2010, 377 wird gebeten, die Empfangsbescheinigung mit Empfangsdatum und Unterschrift zu versehen und **umgehend** an das EPA zurückzusenden:

With reference to the Notice in OJ EPO 7/2010, 377, you are requested to date and sign the acknowledgement of receipt and return it to the EPO **immediately**:

Conformément au communiqué paru au JO OEB 7/2010, 377, vous êtes prié d'indiquer sur le récépissé la date de réception du document, de signer le récépissé et de le renvoyer **sans délai** à l' OEB:

- **über die Online-Dienste des EPA** (als Anlage zu EPA Form 1038) / **through EPO Online Services** (as annex to EPO Form 1038) / **par les services en ligne de l'OEB** (en tant que pièce jointe au formulaire OEB 1038),
- **per Fax / by fax / par téléfax (+49 (0) 89 2399-4465 or +31 (0) 70 340-3016)**
- oder per Post / or by post / ou par courrier.

Empfangen am / Received on / Reçu le :

Unterschrift / Signature:

Empfangsberechtigter/authorised recipient/
le destinataire ou la personne dûment mandatée

Rücksende-Adresse / Return address / Adresse de retour
(Umschlag / envelope / enveloppe ISO C4 / DL / C6/C5 / C6)

Europäisches Patentamt
80298 MÜNCHEN
DEUTSCHLAND

Rücksende-Adresse / Return address / Adresse de retour

EPA/EPO/OEB Form 2936 08.10

PD04057

postnl

## Bericht van ontvangst/Handtekening Retour
Advice of receipt

EPA EPO OEB
tel: (070)3403060
21 -10- 2015
A.R.
Mailroom 12

CN 07

Stempel van kantoor van terugzending
Stamp of the office returning the advice

Designated operator of the Netherlands

**Op kantoor van verzending in te vullen /** To complete at office of posting

| **Kantoor van verzending**<br>Office of posting | **Datum**<br>Date 14.10.2015 |
|---|---|
| **Geadresseerde van de zending**<br>Addressee of the item | Coyle, Philip Aidan<br>F. R. Kelly & Co.<br>27 Clyde Road<br>Ballsbridge<br>Dublin 4<br>IRLANDE |

12

**Priority/By Airmail**

**Aard van de zending /** Nature of the item

**Aangetekend nr. :**
Registered No. of item
RD118795114 NL

☐ **Evt. bedrag en valuta Waarde-aangifte/Verzekerd Vervoer**
Opt. insured amount and currency

**Op plaats van bestemming in te vullen /** To sign on place of destination

**Naam, datum en handtekening**
Name, date and signature
19-10-15

* Afhankelijk van de voorschriften in het land van bestemming wordt het bericht getekend door de geadresseerde of zijn gemachtigde of door de postmedewerker

**Terugzenden aan (in te vullen door de afz.) /** Return to

**Naam of firma**
Name
E.P.O.

**Straat en huisnummer**
Street and No.
Patentlaan 2

**Postcode en plaats**
Postal code and town
2288 E.E. Rijswijk

**Land**
Country
Netherlands

2925211

P 2162 (versie 0513)
PostNL BV Handelsregister K.v.K. Haaglanden nr. 27124700

FRKELLY
EUROPEAN PATENT AND TRADE MARK ATTORNEYS

European Patent Office
D-80298 Munich
Germany

**Your Ref :** 11752936.2
**Our Ref :** P105633EP00

11 March 2016

Dear Sirs,

**European Patent Application No. 11752936.2**
**"A Secured Personal Data Handling and Management System"**
**OS - NEW HORIZON PERSONAL COMPUTING SOLUTIONS LTD.**

---

With reference to the summons to attend oral proceedings which issued pursuant to Rule 115(1), the applicant wishes to make the following requests:

1. Main Request,
2. First Auxiliary Request, and
3. Second Auxiliary Request.

The auxiliary requests are provided without prejudice to the merit of the main request and are included herein in the unlikely event that the Division has any objection to the main request.

**Main Request**

We enclose a revised claim set for replacing the claim set currently on file. An annotated version of the replacement claims is also provided showing the revisions. New claim 4 is based on original PCT claim 27. It is submitted that the claims of the main request are direclty and unambiguously derivable from the Application as originally filed.

**Added Matter**

1. The Examiner has indicated that the amendments filed electronically on 14.05.2015 introduce subject-matter which extends beyond the content of the application as filed, contrary to Article 123(2) EPC. The amendments concerned the phrase "while the apparatus is communicating with an external device" in Claims 1, 4 and 9.

While not acquiescing to the merits of the rejection, the offending phrase has been deleted and replaced with the phrase "*the apparatus being operable to interphase with an external device for activation of various operations between the external device and the handheld apparatus1*". Support for this revision may be found at least on page 18 lines 13-17.

Accordingly, the added matter object has been rendered moot.

**Inventive Step**

The Examiner has indicated that the subject-matter of claims 1 and 4 do not involve an inventive step.The Applicant respectfully disagrees with this assessment. However, in an effort

MARY FLEMING
HAZEL BROWNE
PHILIP KELLY
ASHUMITA DUTTA
GRAHAM FERGUSON
CAROL GONNELLY
MARK HALL
PAUL KEANE
DERMOT MOLLOY
NUNU NADARAJAH
NIAMH O'CONNELL
BRIAN O'NEILL
LINDA O'REGAN
H HANEWITH
ALAN WALLACE
STEPHEN WALLER

ANNA HALLY
ALAN CASEY
DAVID FLYNN
STEPHEN MURPHY
ROBIN O'FEARGHTY
BRONWYN O'HAGAN
MICHAEL SPAIN
SHAUNA TULLY

CONSULTANT
EMERITUS CLERK

to advance prosecution claims 1 and 4 have been revised. To better understand the user's benefits of using the claimed invention, it is required to understand that presently users are frequently losing their saved personal and important data files, due to mechanical or electrical failures of their electromagnetic driven hard-discs, or suffer from sensitive data files failure or damages related to malfunctions of their personal computers or smart cell phones.

Another source for lost sensitive data files is due to software malfunction problems while running on the users' personal computers or smart cell phones. All these problems can be eliminated by the present invention which provides a solution by **separating the user's sensitive data storage and management functions from the cell phone**. This functional separation is a very important aspect of the present application.

In an effort to clarify that the sensitive information is stored on a separate device to the external device, claim 1 has been revised to recite; inter alia:

> *the apparatus being operable to interphase with an external device for activation of various operations between the external device and the handheld apparatus*
>
> *wherein said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with said user holding the portable handheld apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files in said first memory module is denied to said external device and the operation of the portable handheld apparatus is completely shut down.*

The Examiner acknowledges that D1 fails to disclose, hint or suggest:

> ***a)*** *an encryption module in communication with the processing module and the memory module; and*
> ***b)*** *said plurality of biometric sensors are configured to continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied and the operation of the apparatus is completely shut down.*

The Examiner indicated that there are no features in claim 1 that correspond to separating the user's sensitive data storage and management functions from the cell phone. The Applicant wishes to thank the Examiner for these helpful comments. It is respectfully submitted that the applicant has revised claim 1 to make it absolutely clear that the first memory module of the portable handheld device stores the user's data and documentation file and in the event that a change occurs in any of the plurality of personal biological identification parameters of the person holding handheld apparatus, **access to the stored personal data files in said first memory module is denied to said external device and the operation of the portable handheld apparatus is completely shut down**. This is a very important aspect of the invention which does not appear to have been appreciated by the Examiner.

The Examiner relies on D2 for teaching feature b). The Applicant strongly disagrees with this assessment. It is respectfully submitted that D2 fails to disclose, hint of suggest *wherein said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with said user holding the portable handheld apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files in said first memory module is denied to said external device and the operation of the portable handheld apparatus is completely shut down.*

A person skilled in the art would understand that in the claimed invention personal information contained on a first device (handheld portable apapratus) is prevented from being accessed by a second device (external device) if a change occurs in any of the plurality of personal biological identification parameters associated with a user holding the first device. An important aspect of the present invention is that the second device who may have been authorised access to the personal information can be denied access if the biological identification parameters of person holding the frst device changes. For example, this may happen if the heart rate of the user holding the first device is raised as a result of a stressful scenario such as a robbery. It is respectfully submitted that there is absolutely no motivation to combine D2 with D1. Furthermore, even if D2 is combined with D1 it would not teach this inventive concept. For the appropriate test for Article 56, the Applicant notes that it is mandatory under the EPC that the Examiner demonstrates why one skilled in the art **would, not just could,** arrive at the claimed invention starting with the closest prior art bearing in mind the objective technical problem to be solved.

When constructing an inventive step objection it is necessary to show (G-VII, 5.3):

> *In other words, the point is not whether the skilled person could have arrived at the invention by adapting or modifying the closest prior art, but whether he **would have done** so because the prior art incited him to do so in the hope of solving the objective technical problem or in expectation of some improvement or advantage (see T 2/83, OJ 6/1984, 265).*

The Examiner is again reminded as to the Guidelines requirements for a valid inventive step objection and specifically G-VII, 8 where it states:

> *In all cases he should attempt to visualise the overall state of the art confronting the skilled person before the applicant's contribution, and he should seek to make a "real-life" assessment of this and other relevant factors. He should take into account all that is known concerning the background of the invention and give fair weight to relevant arguments or evidence submitted by the applicant. If, for example, an invention is shown to be of considerable technical value, and particularly if it provides a technical advantage which is new and surprising and which is not merely achieved as a bonus effect in a "one-way street" situation (see 11.10.2), and this technical advantage can convincingly be related to one or more of the features included in the claim defining the invention, the examiner should be hesitant in pursuing an objection that such a claim lacks inventive step.*

It is respectfully submitted that there is no hint or suggestion in D1 of the specific limitations in claim 1 above, and of the advantage that this provides.

It is respectfully submitted that there is not a scintilla of motivation in the prior art that would prompt a person skilled in the art to redesign the prior art to include all the features as recited in claim 1. Examiners should be wary of ex post-facto analysis.

The Applicant respectfully reminds the Examining Division that they are obliged under the EPC to grant the application unless there is a valid basis to refuse. The onus is on the Examining Division to establish beyond doubt that the objection is valid and to substantiate all objections. In doing so, the Division must refrain from using hindsight, assumption or innuendo which is not permissible under the EPC.

As is evident from the above argument the Examiner has not provided sufficient anticipation of the claimed features or reasoning why the person of skill in the art would be motivated upon reading the prior art to modify it to arrive at the claimed features.

This omission of D1 is not compensated or addressed by the teaching of D2 which similarly fail to direct the person of skill to the specifics of the claimed teaching. In the absence of D1 or the

secondary references providing any teaching or motivation to the person of skill in the art to provide a method such as that now claimed, it is respectfully submitted that independent claim 1 of the present application is inventive.

For at least the above reasons, it is respectfully submitted that D1 to D2 do not disclose, hint or suggest the subject matter of independent claim 1 of the present application and accordingly claim1 currently on file is both novel and inventive, thereby meeting the requirements of Article 52(1) EPC, Article 54(1) and (2) EPC and Article 56 EPC. It is respectfully submitted that the examiner handling the counterpart U.S. application, which issued as U.S. Patent No. 8,401,875 considered the subject matter of claim 1 to be inventive.

**Unity of Invention**

The Examiner has raised a unity of invention objection against claims 2, 3, 5-8 and 9. The Applicant strongly disagrees with this assessment. The lack of unity objection is based on the understanding that claims 1 and 4 lack an inventive step. As outlined above, the combination of D1 and D2 fails to disclose, hint or suggest the problem solved by the present application. Accordingly, the Applicant strongly disagrees with the Examiner's assessment of lack of unity.

It is respectfully submitted that the unity objections against claims 2, 3, 5-8 and 9 have been rendered moot in view of the fact that the revised claim 1 and 5 are inventive in light of the combination of D1 and D2.

**Main Request Final Comments**

The Applicant respectfully requests that that the Application be allowed proceed to grant based on main request

**First Auxiliary Request**

In the unlikely event that the Division has some fault with claim 1 of the main request and purely as a precaution the Applicant also wishes to include a first auxiliary request. Claim 1 of the first auxiliary request substantially corresponds to claim 1 of the main request with the addition of the following feature:

> *while using a display and keyboard of the external device for user's interactions with the handheld apparatus*

The arguments supplied supporting the patentability of the main request equally apply to the first auxiliary request. It is respectfully submitted that the claims of the first auxiliary request meets the requirements of the EPC.

**Second Auxiliary Request**

In the unlikely event that the Division has some fault with the previous request and purely as a precaution the Applicant also wishes to include a second auxiliary request. Claims 2-3 and 5-8 has been deleted in an effort to overcome the unity objections. Independent system claim 9 (revised claim 3) has been revised to include the subject matter of claim 1 thereby rendering the unity objection against the independent system claim moot.

The arguments supplied supporting the patentability of the main request equally apply to the second auxiliary request. It is respectfully submitted that the claims of the second auxiliary request meets the requirements of the EPC.

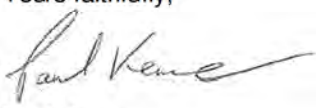
**Cancellation of Oral Proceedings**

We do not believe it will be necessary to put the Applicant or the EPO to the expense of conducting an oral proceedings in this instance, and we hereby request cancellation of the Oral Proceedings. The Applicant has made a real and serious effort to revise address all the issues raised by the examiner.

FRKELLY

**General**
Favourable reconsideration of this application is requested. It is believed that the present submission properly overcomes all remaining objections and that the application is in order for grant. However, if there are any remaining objections which may be usefully dealt with by telephone, the Examiner is invited to call me on **+353 1 231 4862**.

Yours faithfully,



Paul Keane
Representative
Partner
p.keane@frkelly.com

Europäisches Patentamt
European Patent Office
Office européen des brevets

# Letter accompanying subsequently filed items


Representative:

**Mr Paul Keane**
**FRKELLY**
**27 Clyde Road**
**D4 Dublin**
**Ireland**

**Phone: +353 1 231 4862**
**Fax: +353 1 614 4756**
**E-mail: p.keane@frkelly.com**

80298 Munich
Germany
Tel. +49(0)89 2399-0 | Fax -4465

P.O. Box 5818
NL-2280 HV Rijswijk
Netherlands
Tel. +31(0)70 340-2040 | Fax -3016

10958 Berlin
Germany
Tel. +49(0)30 25901-0 | Fax -840


The document(s) listed below is (are) subsequently filed documents pertaining to the following application:

| | |
|---|---|
| Application number | 11752936.2 |
| Applicant's or representative's reference | P105633EP00 |

| | Description of document | Original file name | Assigned file name |
|---|---|---|---|
| 1 | Letter dealing with Oral proceedings | P105633EP00 Written Submision Mar11.pdf | ORAL-1.pdf |
| 2 | Amended claims (clean copy) | P105633EP00 Main Request Clean Mar11.pdf | CLMS-1.pdf |
| 3 | Amended claims with annotations | P105633EP00 Main Request Markup Mar11.pdf | CLMS-HWA-1.pdf |
| 4 | Amended claims (clean copy) | P105633EP00 Claims Clean 1st Aux Mar11.pdf | CLMS-2.pdf |
| 5 | Amended claims with annotations | P105633EP00 Claims Markup 1st Auxiliary Mar11.pdf | CLMS-HWA-2.pdf |
| 6 | Amended claims (clean copy) | P105633EP00 Claims Markup 2nd clean Mar11.pdf | CLMS-3.pdf |
| 7 | Amended claims with annotations | P105633EP00 Claims Markup 2nd Auxil Mar11.pdf | CLMS-HWA-3.pdf |

**Signatures**

| | |
|---|---|
| Place: | |
| Date: | **11 March 2016** |
| Signed by: | **Paul Keane 36258** |
| Representative name: | **Paul Keane** |
| Capacity: | **(Representative)** |

## First Auxiliary Request

### Claims

1. A portable handheld apparatus for managing personal and secured data and documentation files stored in the apparatus , the apparatus being operable to interphase with an external device for activation of various operations between the external device and the handheld apparatus, while using a display and keyboard of the external device for user's interactions with the handheld apparatus; the apparatus comprising:

a plurality of biometric sensors for reading a plurality of personal biometric identification parameters of the user holding the apparatus, said plurality of biometric sensors being integrated within the apparatus;

at least one life signs detector integrated within the apparatus, said life signs detector being configured to measure and record at least one of said user's life sign parameters;

a first memory module in communication with an integrated processing module and an integrated encryption module for the storage of said user's data and documentation files;

an authentication unit configured to compare the reading of the plurality of personal biological biometric identification parameters of the user holding the apparatus with a pre-recorded set of personal biometric identification parameters;

a processing module in communication with said plurality of biometric sensors, said first memory module and said authentication unit;

an encryption module in communication with the processing module;

communication and data connection means for communicating with said external device, said communication and data connection means being in communication with said processing module;

wherein access to the personal data and documentation files stored in said first memory module is only enabled after said authentication unit positively matches each of the plurality of personal biometric identification parameters of the user holding the apparatus, with the pre-recorded set of personal identification parameters; and

wherein said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied to said external device and the operation of the portable handheld apparatus is completely shut down.

2. The apparatus according to claim 1, wherein said at least one of said user's life sign parameters is measured by any of a group of life sign indicators including a heart pulse rate measurement indicator, a body O2 blood saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator.

3. The apparatus according to claim 1,

wherein, whenever any of the group of life sign indicators detects a critical level, the apparatus is configured to:

initiate an emergency call to any of a group of registered emergency centers and send to said registered emergency centers any of a group of data files containing information associated with the user, including the identification data file of the user, personal medical file of the user, the measured set of life sign parameters of the user and location of the user, or

the apparatus further comprises an encryption unit in communication with said processing module for the encryption plus compression and for the decompression plus decryption of said user's data files; or

an emergency button in communication with said processing module and said communication and data connection means module; wherein on said emergency button being activated, communication is initiated between said apparatus and any of a group of registered emergency centers, said emergency call transmitting any of a group of data files containing information associated with the unique user of said apparatus, including the identification data of said user, the personal medical data file of said user, and location of said user; or

wherein said apparatus is configured to communicate with any of a group of service providers, said group of service providers including banks, credit card companies, clinics, hospitals and medical insurance companies, municipal and utility entities and websites frequently accessed by said user; thereby allowing said user to access and manage personal data and documentation files, associated with said user; or

wherein said external device comprises any one of a group including a remote server, a local server, a host computer, voice or data communication means and a cellular phone; or

wherein said emergency call is initiated via any one of a group of communication means including a secured server, directly via the internet by said apparatus connection and communication means, via the internet through any host computer, via a voice and data communication device and via any cellular phone network; or

wherein said communication and data connection means comprises at least one of a group of connection and communication devices including a data interface connector attached to a host computer, a Mini USB, a compatible industrial data interface connector attached to a cellular phone, a near field wireless communication interface, a Bluetooth communication interface, a magnetic reader interface, and a smart card reader based on a contact-less communication interface using induction or RF communication; or

further comprising an stored software module that automatically detects the operating system of the computer or cellular phone connected to said apparatus through one of said group of communicating devices through which the apparatus is connected, said computer or cellular phone having keyboard and display units associated therewith, thereby allowing the user to interact with said first memory module and with said processing module of said apparatus via said keyboard and display units, whereby said computer or cellular phone is configured to utilize and interact with said memory module, said processing module and said sensor module of said apparatus.

4. The apparatus of claim 1, wherein said apparatus further comprises an associated power charging and data backup device, said device comprising a charging and power unit, an electronic sub unit and a mass memory solid-state memory unit, wherein said apparatus whenever connected to said device said apparatus battery power recharging is generated and a data backup process is generated, further comprising the steps of:

comparing the memory content of said apparatus first memory module to the memory content of said backup memory unit; and

if the first memory module of the apparatus lacks data, said electronc unit updating the first memory module with the last version of the data stored within said mass memory solid-state backup memory unit; and

if said solid-state memory unit of said device lacks data, updating the solid-state memory unit of said device with the last version of the data stored within said apparatus's solid-state memory unit.

5. A method for managing personal and secured data and documentation files of a plurality of unique users, each one of said plurality of unique users having a personal identification unit uniquely associated with said one user for storing each user's personal data and documentation files, each personal identification unit being operable to interphase with an external device for activation of various operations between the personal identification unit and

said external device, while using a display and keyboard of the external device for user's interactions with the personal identification unit; each of said personal identification units comprising:

a plurality of biometric sensors stored within the personal identification unit;

at least one life signs detector, stored within the personal identification unit, said life signs detector being configured to measure and record at least one of said user's life sign parameters;

a processing module in communication with said plurality of biometric sensors;

an authentication unit in communication with the processing module;

an encryption unit in communication with said processing module;

a first memory module in communication with said processing module and said encryption unit; wherein said plurality of biometric sensors continuously read a plurality of personal biological identification parameters associated with said user holding the apparatus and in the event that a change occurs in any of the plurality of personal biological identification parameters, access to the stored personal data files is denied and the operation of the apparatus is completely shut down; and

communication and data connection means in communication with said processing module; the method comprising the steps of:

a. the plurality of biometric sensors reading a plurality of personal identification parameters of the user holding the personal identification unit;

b. at least one life signs detector, integrated within the personal identification unit, measuring and recording at least one of said user's life sign parameters;

c said authentication unit comparing each of the personal biological identification parameters of said user with a pre-recorded set of personal biological identification parameters stored in said authentication unit; and

d. if said authentication unit positively identifies said user, allowing said user access to said user's personal data and documentation files stored in said first memory module and allowing said user to communicate with other communication means through said personal identification unit.

6. The method of claim 5

wherein at least one of said plurality of life signs detectors includes a heart pulse rate measurement indicator, a body O2 blood saturation level indicator, a body heat measurement indicator, an electro-dermal activity indicator, a body respiration indicator and a physical or emotional stress indicator, the method further comprising the steps of:

initiating an emergency call to any of a group of registered emergency centers, whenever any of the life sign indicators detects a critical level; and

wherein said emergency call transmits any of a group of data files information associated with the user, including identification of the user, personal medical data file of the user, the measured set of life sign parameters of the user and location of the user; or

wherein the method further comprises the step of:

said personal identification unit communicating, via any one of a group of communication means, with any of a group of service providers including banks, credit card companies, clinics, hospitals and medical insurance companies, municipal and utility entities and websites frequently accessed by said user thereby allowing said user to access and manage said user's personal data and documentation files stored by said group of service providers.

7. The method of claim 5, wherein said personal identification unit further comprises an emergency button in communication with said processing

module and said communication and data connection means, the method further comprising the steps of:

when said emergency button is activated, a call is initiated between said apparatus and any of a group of registered emergency centers; and

said emergency call transmitting any of a group of data files information associated with the user, including identification data of the user, the personal medical data file of the user, and location of the user; or

wherein the apparatus further comprises a magnetic strip element, the method further comprising the step of:

after positive authentication of said user's personal identification parameters, activating said magnetic strip thereby allowing said magnetic strip to be read by any of group of devices including a credit card reader, an ATM, a point of sale, a magnetic strip or near field communication reading device (NFC); or

wherein said personal identification unit further comprises a power charging and data backup device, said device comprising a charging and power unit, an electronic sub unit and a mass memory solid-state memory unit, the method further comprising the steps of:

comparing the memory content of said personal identification unit first memory module to the memory content of said mass memory solid-state memory unit; and

if the first memory module of said personal identification unit lacks data, updating the first memory module with the last version of the data stored within the solid-state memory unit; and

if said solid-state memory unit of said device lacks data, updating the solid-state memory unit of said device with the last version of the data stored within said personal identification unit's solid-state memory unit.

8. The method of claim 5, wherein each of said plurality of unique users is in communication with a system manager, said system manager managing a