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.

9. The method of claim 8, 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.

10. 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;

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 portable handheld apparatus as claimed in any one of claims 1 to 4; wherein each of said portable handheld apparatus being associated with a unique user, each unique user being registered with said system manager.

11. The system of claim 10 further comprising a plurality of registered emergency centers and a plurality of registered service providers in communication with said system manager, to be accessed by said plurality of users; and

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.

Second 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. 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.

3. 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;

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 portable handheld apparatus as claimed in claim 1; wherein each of said portable handheld apparatus being associated with a unique user, each unique user being registered with said system manager.

4. The system of claim 3 further comprising a plurality of registered emergency centers and a plurality of registered service providers in communication with said system manager, to be accessed by said plurality of users; and

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.

Main 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, 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 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 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.

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 portable handheld 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 porable handheld 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 portable handheld 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 portable handheld apparatus, including the identification data of said user, the personal medical data file of said user, and location of said user; or wherein said portable handheld 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 portable handheld 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 personal identification unit being operable to interphase with an external device for activation of various operations between the personal identification unit and the handheld apparatus, 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 personal identification unit 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 exrernal device and the operation of the personal identification unit 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 personal identification unit 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 said personal identification unit 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 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 the 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 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.

9. The method of claim 8, 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.

10. 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 portable handheld units as claimed in any one of claims 1 to 4; wherein each of said portable handheld apparatus being associated with a unique user, each unique user being registered with said system manager.

11. The system of claim 10 further comprising

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 portable handheld 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.

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

to communicate with said portable handheld units to compare the user's ID data file stored in the unique user's portable handheld 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 portable handheld 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 portable handheld unit to said user portable handheld unit, said portable handheld unit responding with a second string of coded alphanumeric data uniquely associated with said user portable handheld 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 portable handheld unit further comprises an emergency button in communication with said processing module and said communication and data connection means module;

wherein the portable handheld 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 portable handheld 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.

13. The system of claim 10, 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.

First Auxiliary Request

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 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 ~~said~~ an integrated processing module and ~~said~~ 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 ~~the~~ 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 ~~an~~ said 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 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 ~~body~~ 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.

45. 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~~

personal identification unit being operable to interphase with an external device for activation of various operations between the personal identification unit and ~~the handheld apparatus~~ 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 ~~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 personal identification unit~~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~~6. The method of claim 4~~5~~

wherein at least one of said plurality of life signs detectors includes a ~~body~~ 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.

~~67~~. The method of claim 45, wherein said personal identification unit ~~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 said personal identification unit ~~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 personal identification unit ~~apparatus~~ 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 ~~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 personal identification unit's ~~apparatus's~~ solid-state memory unit.

~~7~~8. The method of claim ~~4~~5, 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~~9. The method of claim ~~7~~8, 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 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.~~

10. 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;

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 portable handheld apparatus as claimed in any one of claims 1 to 4; wherein each of said portable handheld apparatus being associated with a unique user, each unique user being registered with said system manager.

11. The system of claim 10 further comprising a plurality of registered emergency centers and a plurality of registered service providers in communication with said system manager, to be accessed by said plurality of users; and

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.

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.

Main Request

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 being operable to interphase with an external device for activation of various operations between the external device and 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 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~~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 ~~an~~said 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 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.

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~~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 portable handheld 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 porable handheld 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 portable handheld 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 portable handheld apparatus, including the identification data of said user, the personal medical data file of said user, and location of said user; or wherein said portable handheld 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 portable handheld 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.

45. 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 personal identification unit being operable to interphase with an external device for activation of various operations between the personal identification unit and the handheld apparatus, 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 personal identification unit ~~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 to said exrernal device and the operation of the ~~apparatus~~ personal identification unit 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 ~~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~~6. The method of claim 4~~5~~

wherein at least one of said plurality of life signs detectors includes a ~~body~~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.

~~67~~. The method of claim 45, wherein said personal identification unit ~~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 personal identification unit ~~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 said personal identification unit ~~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~~ 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 ~~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~~ 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'~~sapparatus'~~ solid-state memory unit.

~~7~~8. The method of claim 45, 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~~9. The method of claim ~~7~~8, 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.

910. 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~~portable handheld units as claimed in any one of claims 1 to 4; wherein each of said ~~personal identification units~~portable handheld apparatus 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~~

11. The system of claim 10 further comprising

~~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~~ portable handheld 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~~12. The system according to claim 10, wherein said system manager is configured:

to communicate with said ~~personal identification~~ portable handheld units to compare the user's ID data file stored in the unique user's ~~personal identification~~ portable handheld 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~~ portable handheld 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~~ portable handheld unit to said user ~~personal identification~~portable handheld unit, said ~~personal identification~~ portable handheld unit responding with a second string of coded alphanumeric data uniquely associated with said user ~~personal identification~~ portable handheld 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~~ portable handheld unit further comprises an emergency button in communication with said processing module and said communication and data connection means module;

wherein the ~~personal identification~~ portable handheld 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~~ portable handheld 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~~13. The system of claim ~~9~~10, 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.

Second Auxiliary Request

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 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 ~~said~~ an integrated processing module and ~~said~~ 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 ~~the~~ 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 ~~an~~ said 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 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 body 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.~~

42. 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~~ personal identification unit being operable to interphase with an external device for activation of various operations between the personal identification unit and ~~the handheld apparatus~~ 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 ~~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 personal identification unit~~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 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.

6. The method of claim 4, wherein said personal identification unit 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 said personal identification unit 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 personal identification unit apparatus 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 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 personal identification unit's 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 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.~~

3. 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;

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 portable handheld apparatus as claimed in claim 1; wherein each of said portable handheld apparatus being associated with a unique user, each unique user being registered with said system manager.

4. The system of claim 3 further comprising a plurality of registered emergency centers and a plurality of registered service providers in communication with said system manager, to be accessed by said plurality of users; and

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~~:~~.

~~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	4187322
Application number	EP11752936.2
Date of receipt	11 March 2016
Receiving Office	European Patent Office, The Hague
Your reference	P105633EP00
Applicant	All applicants as on file

Documents submitted	
package-data.xml	ep-sfd-request.xml
epf1038.pdf (1 p.)	ORAL-1.pdf\P105633EP00 Written Submision Mar11.pdf (5 p.)
CLMS-1.pdf\P105633EP00 Main Request Clean Mar11.pdf (12 p.)	CLMS-HWA-1.pdf\P105633EP00 Main Request Markup Mar11.pdf (13 p.)
CLMS-2.pdf\P105633EP00 Claims Clean 1st Aux Mar11.pdf (9 p.)	CLMS-HWA-2.pdf\P105633EP00 Claims Markup 1st Auxiliary Mar11.pdf (14 p.)
CLMS-3.pdf\P105633EP00 Claims Markup 2nd clean Mar11.pdf (4 p.)	CLMS-HWA-3.pdf\P105633EP00 Claims Markup 2nd Auxil Mar11.pdf (13 p.)

Submitted by	CN=Paul Keane 36258
Method of submission	Online
Date and time receipt generated	11 March 2016, 12:17 (CET)
Message Digest	1F:B7:45:85:A3:49:08:79:54:6A:92:EA:46:D1:F1:0E:11:B2:67:CB

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/

VERZEND CONTROLE RAPPORT

TIJD : 30/03/2016 15:09
NAAM : EPO THE HAGUE
FAX : +31-70-340-4360
TEL :
SER NR: 000M8N778454

DATUM,TIJD	30/03 15:08
FAX NR./NAAM	00035316144756
TIJDSDUUR	00:01:03
PAGINA'S	03
RESULT	OK
MODE	STANDAARD ECM

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 30.03.2016

By FAX only

Reference	Application No./Patent No.
p105633ep00	11752936.2 - 1955 / 2545485
Applicant/Proprietor	
OS - New Horizon Personal Computing Solutions Ltd.	

BRIEF COMMUNICATION

Oral Proceedings on 13.04.16

Subject: ☒ Your letter of 11.03.2016

Communication:
- ☐ The summons to attend oral proceedings on 13.04.16 has been cancelled.
- ☐ The procedure will be continued in writing.
- ☒ The date fixed for oral proceedings is maintained.
- ☐ A new date will be set later.
- ☒ EPO Form 2906 enclosed (2 pages)

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

By FAX only

Date: 30.03.2016

Reference	Application No./Patent No.
p105633ep00	11752936.2 - 1955 / 2545485

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

BRIEF COMMUNICATION

Oral Proceedings on 13.04.16

Subject: ☒ Your letter of 11.03.2016

Communication:

- ☐ The summons to attend oral proceedings on 13.04.16 has been cancelled.
- ☐ The procedure will be continued in writing.
- ☒ The date fixed for oral proceedings is maintained.
- ☐ A new date will be set later.
- ☒ EPO Form 2906 enclosed (2 pages)

Please take note.

For the Examining Division

Europäisches Patentamt • European Patent Office • Office européen des brevets

Registered letter
EPO Form 2008A 12.07 (30/03/16)

CB03561

Europäisches Patentamt
European Patent Office
Office européen des brevets

European patent application No. 11752936.2

URGENT !
To be completed (under II.) and returned to the formalities officer immediately

Maintenance / Change of date / Cancellation of oral proceedings arranged for: day 13.04.16 at 09.30 hrs

I. **To the Examining / Opposition division**

1. ☐ The proprietor has requested the revocation (or the like) of his patent (date: .....).

2. ☒ The party / witness ..... has indicated (date: 11.03.2016.....) that he / she

   ☐ requests the date / time of oral proceedings to be changed.

   ☐ withdraws the request for oral proceedings.

   ☐ will not be attending.

   ☐ wishes to be heard by a national court.

   ☒ has filed amendments (in examination proceedings).

   ☐ has requested that the oral proceedings be held as a videoconference (in examination proceedings).

3. ☐ Two months before the oral proceedings the application is deemed to be withdrawn (in examination proceedings). The oral proceedings have to be cancelled.

14.03.2016
Date

Berthon, Claude
Formalities Officer

EPO Form 2088 06.14

CB03561

European patent application No. 11752936.2

II. To the Formalities Officer

1. ☒ The date / time fixed for oral proceedings is maintained.

   ☒ (if necessary) The reasons are indicated on enclosed EPO Form 2906/2906O, which is to be dispatched to the party with EPO Form 2008A/2310A.

2. ☐ At the instigation of the division the oral proceedings cannot take place on the arranged date for the reasons indicated on enclosed EPO Form 2906, which is to be dispatched to the party with EPO Form 2008A/2310A.

   Date _____ Director _____

3. ☐ The summons to attend oral proceedings on 13.04.16 should be cancelled.

   3.1 ☐ The proceedings will be continued in writing.

   3.2 ☐ A new date will be set later.

   3.3 ☐ A new date/time is set as follows:

   date ..... at ..... hrs.
   Parties' written submissions and amendments in preparation for the oral proceedings, if any, should be made not later than

   ..... month(s) before the date of the oral proceedings.

4. ☐ The request for the oral proceedings to be held as a videoconference

   4.1 ☐ is allowed.

   4.2 ☐ is rejected for the reasons indicated on enclosed EPO Form 2906, which is to be dispatched to the party with EPO Form 2008A.

5. ☐ The application is deemed to be withdrawn. The oral proceedings are cancelled.

30.03.2016
Date

Chairman _____ Second member _____ Primary Examiner _____ Legal member

III. Action taken by the formalities officer

☒ EPO Form 2008A/2310A has been dispatched, if applicable (see point II above) together with EPO Form 2906/2906O.

☐ A new summons has been dispatched.

☐ .....

30/03/16
Date

Formalities Officer

EPO Form 2088 06.14

CB03561

The preliminary opinion of the examining division on the amendments filed on 11-03-2016 is as follows:

Main Request

1. The amendments of the main request are not compliant with the requirements of Art.123(2) EPC, for the following reasons:

1.1. From the passage cited by the applicant, and the last passage on page 39, it is derivable that the apparatus is operable to interphase with a cellular phone or a host personal computer for activation of various operations between the cellular phone/host computer and the apparatus. However, it is not derivable that the apparatus is operable to interphase with any other external device; therefore, the amendment of claims 1 and 5: "the apparatus is operable to interphase with an external device" is not directly and unambiguously derivable from the description.

1.2. Furthermore, the applicant did not provide, and the examining division could not identify in the application as filed, the support for the amendment of the last feature of claims 1 and 5, namely, "access ... is denied to said external device".

2. Regarding the inventive step, the examining division maintains the opinion that document D2 discloses the distinguishing feature b), and maintains the problem-solution approach as presented in the summons.

2.1. Considering the feature introduced with the amendment, to the extent that it is present in the application as originally filed, namely, that the apparatus is operable to interphase with a cellular phone or a host personal computer for activation of various operations between the cellular phone/host computer and the apparatus, at the time of filing the present application the techniques for transferring data between a cell phone and computer were well known. Therefore, in the context of document D1, this feature represents a mere juxtaposition of a known technique and cannot be considered as basis of an inventive step.

3. As a consequence of the lack of inventive step, the objection regarding the unity of invention is maintained, and is extended to the subject-matter of new claim 4.

First and Second Auxiliary Request

4. The arguments presented for the main request apply also to the first and the second auxiliary request. In addition to the argument given in the section 2.1. above, it is noted that the use of a display and keyboard of a host personal computer for user's

interactions with the cell phone belongs to the techniques for transferring data between a cell phone and computer, so the argument given for the main request is valid also to the first and the second auxiliary request.

5. The preliminary opinion of the examining division is thus that none of the requests comply with requirements of Articles 123(2) and 56 EPC. The summons to oral proceeding is therefore maintained.

FRKELLY
EUROPEAN PATENT AND TRADE MARK ATTORNEYS

European Patent Office
D-80298 Munich
Germany

Your Ref : 11752936.2
Our Ref : P105633EP00

11 April 2016

Dear Sirs,

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

We wish to notify the Examining Division that we will not be attending the oral hearing scheduled for April 13 2016.

Furthermore, we request a decision according to the current state of the file, and we withdraw our request for an oral hearing.

Yours faithfully

Paul Keane
Representative

MARY H. BANNON
DAVID MCSWEENEY
PHILIP COYLE
ASSUMPTA DUFFY
GAVAN FERGUSON
CAROL GORMLEY
NIAMH HALL
PAUL KEANE
DONAL M KELLY
SUMI NADARAJAH
MAURA O'CONNELL
BRIAN O'NEILL
BRENDA O'REGAN
SHANE SMYTH
ALAN WALLACE
STEPHEN WALLER

ANNA HALLY
ALAN CASEY
DAVID FLYNN
STEPHEN MURPHY
JOHN O'FLAHERTY
BRONWYN O'HAGAN
MICHAEL SCANNELL
SHAUNA TILLEY

CONSULTANTS
LINDSAY J CASEY

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

ONLY BY FAX

Date: 11.04.2016

Reference	Application No./Patent No.
p105633ep00	11752936.2 - 1955 / 2545485

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

BRIEF COMMUNICATION

Oral Proceedings on 13.04.16

Subject: ☒ Your letter of 11.04.2016

Communication:
- ☒ The summons to attend oral proceedings on 13.04.16 has been cancelled.
- ☒ The procedure will be continued in writing.
- ☐ The date fixed for oral proceedings is maintained.
- ☐ A new date will be set later.
- ☐

Please take note. Please acknowledge receipt at your earliest convenience by return of fax to our fax server +49(0)892399-4465.

For the Examining Division

Europäisches Patentamt • European Patent Office • Office européen des brevets

Registered letter
EPO Form 2008A 12.07 (11/04/16)

VERZEND CONTROLE RAPPORT

TIJD : 11/04/2016 16:46
NAAM : EPO THE HAGUE
FAX : +31-70-340-4360
TEL :
SER NR: 000M8N778454

DATUM,TIJD	11/04 16:46
FAX NR./NAAM	00035316144756
TIJDSDUUR	00:00:35
PAGINA'S	01
RESULT	OK
MODE	STANDAARD ECM

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

ONLY BY FAX

Date: 11.04.2016

Reference	Application No./Patent No.
p105633ep00	11752936.2 - 1955 / 2545485

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

BRIEF COMMUNICATION

Oral Proceedings on 13.04.16

Subject: ☒ Your letter of 11.04.2016

Communication:
- ☒ The summons to attend oral proceedings on 13.04.16 has been cancelled.
- ☒ *The procedure will be continued in writing.*
- ☐ The date fixed for oral proceedings is maintained.
- ☐ A new date will be set later.
- ☐

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 Letter apr11.pdf	ORAL-1.pdf

Signatures

Place:

Date: **11 April 2016**

Signed by: **Paul Keane 36258**

Representative name: **Paul Keane**

Capacity: **(Representative)**

Europäisches Patentamt
European Patent Office
Office européen des brevets

European patent application No. 11752936.2

URGENT !
To be completed (under II.) and returned to the formalities officer immediately

Maintenance / Change of date / Cancellation of oral proceedings arranged for: day 13.04.16 at 09.30 hrs

I. To the Examining / Opposition division

1. ☐ The proprietor has requested the revocation (or the like) of his patent (date: .....).

2. ☒ The party / witness ..... has indicated (date: 11.04.2016 .....) that he / she

   ☐ requests the date / time of oral proceedings to be changed.

   ☒ withdraws the request for oral proceedings.

   ☒ will not be attending.

   ☐ wishes to be heard by a national court.

   ☐ has filed amendments (in examination proceedings).

   ☐ has requested that the oral proceedings be held as a videoconference (in examination proceedings).

   X Request a decision on the state of the file.

3. ☐ Two months before the oral proceedings the application is deemed to be withdrawn (in examination proceedings). The oral proceedings have to be cancelled.

11.04.2016
Date

Dahl, Pia
Formalities Officer

EPO Form 2088 06.14

PD04057

European patent application No. 11752936.2

II. To the Formalities Officer

1. ☐ The date / time fixed for oral proceedings is maintained.

   ☐ (if necessary) The reasons are indicated on enclosed EPO Form 2906/2906O, which is to be dispatched to the party with EPO Form 2008A/2310A.

2. ☐ At the instigation of the division the oral proceedings cannot take place on the arranged date for the reasons indicated on enclosed EPO Form 2906, which is to be dispatched to the party with EPO Form 2008A/2310A.

   Date _____ Director _____

3. ☒ The summons to attend oral proceedings on 13.04.16 should be cancelled.

   3.1 ☒ The proceedings will be continued in writing.

   3.2 ☐ A new date will be set later.

   3.3 ☐ A new date/time is set as follows:

   date ..... at ..... hrs.
   Parties' written submissions and amendments in preparation for the oral proceedings, if any, should be made not later than

   ..... month(s) before the date of the oral proceedings.

4. ☐ The request for the oral proceedings to be held as a videoconference

   4.1 ☐ is allowed.

   4.2 ☐ is rejected for the reasons indicated on enclosed EPO Form 2906, which is to be dispatched to the party with EPO Form 2008A.

5. ☐ The application is deemed to be withdrawn. The oral proceedings are cancelled.

11.04.2016
Date

Chairman _____ Second member _____ Primary Examiner _____ Legal member _____

III. Action taken by the formalities officer

☐ EPO Form 2008A/2310A has been dispatched, if applicable (see point II above) together with EPO Form 2906/2906O.

☐ A new summons has been dispatched.

☐ .....

Date _____ Formalities Officer _____

EPO Form 2088 06.14

PD04057

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	4258261
Application number	EP11752936.2
Date of receipt	11 April 2016
Receiving Office	European Patent Office, The Hague
Your reference	P105633EP00
Applicant	All applicants as on file
Documents submitted	package-data.xml epf1038.pdf (1 p.) ep-sfd-request.xml ORAL-1.pdf\P105633EP00 Letter apr11.pdf (1 p.)
Submitted by	CN=Paul Keane 36258
Method of submission	Online
Date and time receipt generated	11 April 2016, 11:22 (CEST)
Message Digest	F6:5A:C4:F1:93:20:E1:E4:14:8D:0D:83:7A:CC:82:83:8B:0A:50:2C

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/

Article 106
Decisions subject to appeal

(1) An appeal shall lie from decisions of the Receiving Section, Examining Divisions, Opposition Divisions and the Legal Division. It shall have suspensive effect.

(2) A decision which does not terminate proceedings as regards one of the parties can only be appealed together with the final decision, unless the decision allows a separate appeal.

(3) The right to file an appeal against decisions relating to the apportionment or fixing of costs in opposition proceedings may be restricted in the Implementing Regulations.

Rule 97
Appeal against apportionment and fixing of costs

(1) The apportionment of costs of opposition proceedings cannot be the sole subject of an appeal.

(2) A decision fixing the amount of costs of opposition proceedings cannot be appealed unless the amount exceeds that of the fee for appeal.

Rule 98
Surrender or lapse of the patent

The decision of an Opposition Division may be appealed even if the European patent has been surrendered in all the designated Contracting States or has lapsed in all those States.

Article 107
Persons entitled to appeal and to be parties to appeal proceedings

Any party to proceedings adversely affected by a decision may appeal. Any other parties to the proceedings shall be parties to the appeal proceedings as of right.

Article 108
Time limit and form

Notice of appeal shall be filed, in accordance with the Implementing Regulations, at the European Patent Office within **two months** of notification of the decision. Notice of appeal shall not be deemed to have been filed until the fee for appeal has been paid. Within **four months** of notification of the decision, a statement setting out the grounds of appeal shall be filed in accordance with the Implementing Regulations.

Further information concerning the filing of an appeal

(a) Notice of appeal can be filed in accordance with Rule 1 and Rule 2(1) EPC, by delivery by hand, by post, or by technical means of communication. The filing has to comply with the details and conditions and, where appropriate, any special formal or technical requirements laid down by the President of the European Patent Office (R. 99(3) EPC).

(b) The addresses of the filing offices of the European Patent Office are as follows:

(i) European Patent Office
D-80298 Munich
Germany

Fax: +49 89 2399-4465

(ii) European Patent Office
Postbus 5818
NL-2280 HV Rijswijk (ZH)
The Netherlands

Fax: +31 70 340-3016

(iii) European Patent Office
D-10958 Berlin
Germany

Fax: +49 30 259 01-840

(c) The notice of appeal must contain the name and address of the appellant in accordance with the provisions of Rule 41(2)(c) EPC, an indication of the decision impugned, and a request defining the subject of the appeal. In the statement of grounds of appeal the appellant shall indicate the reasons for setting aside the decision impugned, or the extent to which it is to be amended, and the facts and evidence on which the appeal is based (R. 99(1) and (2) EPC). The notice of appeal and any subsequent submissions stating the grounds for appeal must be signed (R. 50(3) EPC).

(d) The fee for appeal is laid down in the Rules relating to Fees. The schedule of fees and expenses of the EPO or a reference to the current version is regularly published in the Official Journal of the European Patent Office under the heading "Guidance for the payment of fees, expenses and prices". Fee information is also published on the EPO website under www.epo.org/fees.

I. Summary of Facts and Submissions

1 European patent application No. 11 752 936.2 having the title "A SECURED PERSONAL DATA HANDLING AND MANAGEMENT SYSTEM" was filed on 10-03-2011 . It claims priority of US 313145 filed on 12-03-2010. The applicant is
OS - New Horizon Personal Computing Solutions Ltd.
10/3 Efroni Street
P.O. Box 84275
90805 Mevasseret Zion
IL.

2 The Supplementary European search report identified lack of unity of invention and cited the following documents for the first invention:

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

US 6 957 337 B1 (CHAINER TIMOTHY JOSEPH [US] ET AL) 18 October 2005 (2005-10-18)

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

3 The European search opinion referred to documents D1: US2009/083847 and D2: US 5 229 764 from the search report. Objections under Articles 123(2) and 82 EPC were raised, as well as objections under Articles 56 and 84 EPC for the invention first mentioned in the claims.

4 In the response received on 28-08-2014 the applicant requested further examination on an amended set of claims 1-12 and provided arguments in support of the patentability of these claims. Oral proceedings were requested before any adverse decision.

5 In a communication under Article 94(3) EPC issued by the examining division on 05-01-2015, objections under Article 123(2) EPC were raised, and objections under Article 82 EPC, as well as under Article 56 EPC for the first invention, were maintained.

6 In the response received on 14-05-2015 the applicant requested further examination on an amended set of claims 1-12 and provided arguments in support of the patentability of the claims.

7 On 14-10-2015 the examining division issued a summons to attend oral proceedings on 13.04.2016. In the annex to the summons, objections under Article 123(2) EPC were raised. Objections under Article 82 EPC, as well as under Article 56 EPC for the first invention, were maintained. A reply to the applicant's arguments was also given.

8 In a response to the summons received on 11-03-2016 the applicant submitted one main and two auxiliary requests, and provided arguments in support of the patentability of the claims.

9 In a communication sent by telefax on 30-03-2016 the applicant was informed that the date fixed for oral proceedings was maintained. In an annex, the examining division expressed its preliminary opinion that none of the present set of claims was compliant with requirements of Article 123(2) EPC, and that, to the extent that the claimed subject-matter was present in the application as originally filed, it was not inventive. The arguments therefore were provided. The objection regarding the unity of invention was also maintained.

10 In an electronic communication on 11-04-2016 the representative informed the examining division that he would not be attending the oral hearing. The request for oral hearing was withdrawn, and a decision according to the current state of the file was requested.

11 With a telefax communication on 11-04-2016 the applicant was informed that the oral proceedings were cancelled.

12 The decision is based on the following request(s):

Main Request

Description, Pages

1-60	as published	

Claims, Numbers

1-13	filed in electronic form on	11-03-2016

Drawings, Sheets

1/9-9/9	as published	

Auxiliary Request 1

Description, Pages

1-60 as published

Claims, Numbers

1-11 filed in electronic form on 11-03-2016

Drawings, Sheets

1/9-9/9 as published

Auxiliary Request 2

Description, Pages

1-60 as published

Claims, Numbers

1-4 filed in electronic form on 11-03-2016

Drawings, Sheets

1/9-9/9 as published

13 The claims under consideration are attached to this decision. As to the other application documents, reference is made to the file.

II. Reasons for the Decision

Main Request

1 The amendments of the main request are not compliant with the requirements of Art.123(2) EPC, for the following reasons:

1.1 The amendment of claims 1 and 5: "the apparatus is operable to interphase with an external device" is not directly and unambiguously derivable from the description.

From the passage cited by the applicant, and the last passage on page 39, it is derivable that the apparatus is operable to interphase with a cellular phone or a host personal computer for activation of various operations between the cellular phone/host computer and the apparatus. However, it is not derivable that the apparatus is operable to interphase with any other external device, as claimed.

1.2 Furthermore, the applicant did not provide, and the examining division could not identify in the application as filed, the support for the amendment of the last feature of claims 1 and 5, namely, "access ... is denied to said external device".

2 The subject-matter of claims 1 and 5 of the main request (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 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 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 and the operation of the portable handheld 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 number 1 as 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.

2.4 Considering the feature introduced with the amendment, to the extent that it is present in the application as originally filed, namely, that the apparatus is operable to interphase with a cellular phone or a host personal computer for activation of various operations between the cellular phone/host computer and the apparatus, at the time of filing the present application the techniques for transferring data between a cell phone and computer were well known. Therefore, in the context of document D1, this feature represents a mere juxtaposition of a known technique and cannot be considered as basis of an inventive step.

3 The same reasoning applies, mutatis mutandis, to corresponding method claim 5.

Applicant's arguments

4 The applicant argues in his letter of reply dated 11-03-2016, page 3, 1st paragraph, that the merit of the invention is in that the personal information contained in a first device (handheld portable apparatus) is prevented from being accessed by the 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. The applicant then gives an example involving the heart rate of the user.

The examining division notes that this effect is obtained by the combination of teachings of documents D1 and D2. Even considering the example given by the applicant, although it is not present in the claims, the examining division notes that the heart rate of the user is a biological parameter measured in D1, in the passage already cited above, namely, par.[0057], "a user's pulse".

5 The applicant further argues in his letter of reply that there is no motivation in the prior art that would prompt a person skilled in the art to redesign the prior art to include all the features recited in claim 1.

However, the examining division maintains the opinion that such motivation for distinguishing feature b) is present in D2, as reasoned here above in section 2.3.2. For the remaining features, namely, the distinguishing feature a) and the feature related to interphase with an external device, the examining division maintains the opinion that it is a mere juxtaposition of features, since they do not produce any working inter-relationship.

First Auxiliary request

6 Claim 1 of the first auxiliary request corresponds to claim 1 of the main request with the addition of the feature:

"...while using a display and keyboard of the external device for user's interaction with the handheld apparatus"

The objection under Article 123(2) EPC raised against the main request applies also to the first auxiliary request, extended to the term "external device" in the feature recited here above.

7 The subject-matter of claims 1 and 5 of the first auxiliary request (excluding the features infringing Art.123(2) EPC) does not involve an inventive step within the meaning of Article 56 EPC, for the same reasons as the main request, presented here above in sections 2.1 - 2.4. In addition to the argument given in the section 2.4 above, it is noted that the use of a display and keyboard of a host personal computer for user's interactions with the cell phone belongs to the techniques for transferring data between a cell phone and computer, so the argument given for the main request is valid also for the first auxiliary request.

Second Auxiliary request

8 The subject-matter of claims 1 and 2 of the second auxiliary request is the same as the subject-matter of claims 1 and 5 of the first auxiliary request. Therefore, claims 1 and 2 of the second auxiliary request do not comply with requirements of Articles 123(2) and 56 EPC, the reasons being the same as for the first auxiliary requests.

III. Decision

For the reasons given in detail above, the application is refused under Article 97(2) EPC for infringing Article 123(2) EPC and for lack of an inventive step in the sense of Article 56 EPC for the main, the first, and the second auxiliary request.

IV. Further Remarks

1 For completeness, prior art documents XP055260933, XP055260935 and WO2006076658 are provided in support of the statement in section 2.4 that, at the time of filing the present application, the techniques for transferring data between a cell phone and a computer were well known. A copy of the documents is attached to this decision.

2 The main request lacks unity within the meaning of article 82 EPC, for the following reasons:

As shown here above in the section Reasons for the Decision, the independent claims 1 and 5 lack inventive step, leaving the dependent claims without a common inventive concept. The six inventions addressed by dependent claims are identified as follows:

I. Life sign detectors (claim 2 and part of claims 6 and 11):

II. Providing user data to emergency services (part of claims 3, 6 and 7, claim 13);

III. Interaction via the keyboard and display of a second device (part of claim 3);

IV. Connecting to a magnetic strip interface (part of claim 7);

V. Charging the apparatus and updating its data (claim 4 and part of claim 7);

VI. Centralized data management (claims 8-12).

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: Matias Garraz, Bruno
Tel: +31 70 340 - 4371
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 - 1955	p105633ep00	24.05.2016
Applicant: OS - New Horizon Personal Computing Solutions Ltd.		

Decision to refuse a European Patent application

The Examining Division has decided:

European Patent application No. 11 752 936.2 is refused.

Applicant/s:
OS - New Horizon Personal Computing Solutions Ltd.
10/3 Efroni Street
P.O. Box 84275
90805 Mevasseret Zion
IL

Title
A SECURED PERSONAL DATA HANDLING AND MANAGEMENT SYSTEM

The grounds for the decision are set out on the supplemental sheets annexed hereto.

Means of redress

This decision is open to appeal.
Attention is drawn to the attached text of Articles 106 to 108 EPC and Rules 97 and 98 EPC.

Registered letter with advice of delivery
EPO Form 2007 12.07 TRI

Examining Division:

Chairman: van Praagh, Kay
2nd Examiner: Sigolo, Alessandro
1st Examiner: Arbutina, Ljiljana

Matias Garraz, Bruno
Formalities Officer
Tel. No.: +31 70 340-4371 **Branch at The Hague**

Enclosure(s): 8 page/s reasons (Form 2916)
Form 2019
main, first and second auxiliary request filed on 11-03-2016
XP055260933, XP055260935, WO2006076658

to EPO postal service: 19.05.16

Registered letter with advice of delivery
EPO Form 2007 12.07TRI

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

Application No.: 11 752 936.2

Decision of the Examining Division

The examining division has decided:

The European patent application is refused on the basis of Article 97(2) EPC. The reasons for the decision are attached (Form(s) 2916).

26/4/2016
Date

van Praagh, Kay
Chairman

Arbutina, Ljiljana
1st examiner

Sigolo, Alessandro
2nd examiner

Enclosure(s): Form 2916
main, first and second auxiliary request filed on 11-03-2016
XP055260933, XP055260935, WO2006076658

INTERNET ARCHIVE Wayback Machine
http://www.wikihow.com/Send-Files-to-a-Cell/Mobile-Phone-Using-Bluetooth-Technology
Go
APR
178 captures
11 Apr 08 - 23 Mar 16
2008

How to Send Files to a Cell/Mobile Phone Using Bluetooth Technology

originated by:Claro, Anonymous, Horses4Ever, Maluniu (see all)

Article Edit Discuss View History

Do you want to have a ringtone on your phone? or have a picture from your laptop/computer on your phone? Read on if you do!

edit Steps

1. 1
   Make sure your computer is equipped with Bluetooth technology (either integrated into the machine or a USB dongle) and active.
2. 2
   Turn on Bluetooth on your mobile device. This option can often be found in the Settings or Connectivity menu of your phone.
3. 3
   Pair your computer with your mobile device by making both devices discoverable (also known as visible or unhidden) in the Bluetooth options. Once both are visible, search for Bluetooth devices on your mobile phone.
4. 4
   Locate the name of your computer in the results list and select it.
5. 5
   Enter a 4 to 8 digit passcode of your own choosing and press continue. If you are pairing with a Bluetooth headset or other screenless device, the passcode will be either 0000, or provided in the device's manual.
6. 6
   Once your devices are paired, you can send and receive files.
7. 7
   There are several methods to send a file to your mobile device. One method is to copy the file from your computer, navigate to your mobile device (often found in My Computer or My Bluetooth Places) and then paste the file to the phone. Another option is to right-click on the desired file and select Send To --> Bluetooth Device --> (mobile phone's name). Some phones (notably Verizon phones) do not support the necessary 'profile' to allow file transfers, and instead only offer support for Bluetooth headsets.
8. 8
   While the file is being transferred, you should see a progress bar on your computer and/or phone. Once the file is finished transferring, a message stating such should show up on your device's screen.

SDOCID: <XP_____55260935A__I_> 100124035235/http://www.wikihow.com/Send-Files-to-a-Cell/Mobile-Phone-Using-Bluetooth BIBL/DESC page 1

edit Tips

- Make sure that both your computer and your mobile device are on and have Bluetooth enabled. Most phones require user input to allow Bluetooth connections and operations.
- If you are having problems, try Googling your phone's model with the word "Bluetooth file transfer" or "Bluetooth OBEX" (Object Exchange profile). Some phones have specific methods or problems with Bluetooth file transfers, while others do not support the Bluetooth file transfer methods at all, instead only allowing Bluetooth headsets to work.

edit Warnings

- Sometimes MP3 files will not work on older phones or on phones that restrict file types. For example, some phones will only be able to play .WMA files while others can only play .MP3, .MIDI, or .WAV.
- Some phones do not allow for Bluetooth file transfers or have specific methods for transferring files. See the Tips section for more information.
- If you are not able to transfer a file with Bluetooth, depending on the file type and size you may be able to email it to your phone's email address, set up through your provider. See Email to a Cell Phone for more information.

edit Things You'll Need

- Phone with Bluetooth Support
- Computer with internal Bluetooth support or computer with an attached USB Bluetooth dongle.

edit Related wikiHows

- How to Not Be Nervous when Speaking to Strangers on the Phone
- How to Make it Appear You Are Talking on the Phone When You're Not
- How to Make a Better Impression on the Telephone
- How to Use the Telephone Buttons As a Code

Articles for You to Write

Here is a list of suggested articles that have not yet been written. You can help by researching and writing one of these articles.

- How to Use a Computer Headset
- How to Set Up Bluetooth on a Laptop
- How to Install Bluetooth on Your Computer
- How to Use Bluetooth Technology
- How to Set Up a Computer for Phone Use

Article Info

Last edited:
January 11, 2010 by Anonymous

Categories:
Ringtones and Other Downloads

Recent edits by: Elyne, Ttrickyy, Maluniu (see all)

Article Tools

Share this Article:

INTERNET ARCHIVE Wayback Machine 178 captures 11 Apr 08 - 23 Mar 16 Go APR 2008

- Watch
- Edit
- Send fan mail to authors

+ Embed this: Republish this entire article on your blog or website.

Thanks to all authors for creating a page that has been read 26,450 times.

Was this article accurate?

Yes No

Write An Article**Random Article**

Related wikiHows

- Not Be Nervous when Speaking to Strangers on the Phone
- Make it Appear You Are Talking on the Phone When You're Not
- Make a Better Impression on the Telephone
- Use the Telephone Buttons As a Code

Featured Articles



Clean Copper



Prevent Soggy Pastry Bases



Install Ubuntu on VirtualBox

Make Gluten Free Shortbread



Recent Changes

Want to join in?

- collapse Navigation

- Recent Changes
- Community Portal
- Forums
- Special pages
- Suggest a Topic
- List Suggested Topics

+ expand Editing Tools

+ expand My Pages

- Become our Fan on Facebook
- Follow us on Twitter

wikiHow

the how to manual that you can edit

- Home
- About wikiHow
- Help
- Terms of Use
- RSS
- Site map

Explore Categories

- Arts and Entertainment
- Cars and Other Vehicles
- Computers and Electronics
- Education and Communications
- Family Life
- Finance and Business
- Food and Entertaining
- Health
- Hobbies and Crafts
- Holidays and Traditions
- Home and Garden
- Other
- Personal Care and Style
- Pets and Animals
- Philosophy and Religion
- Relationships
- Sports and Fitness
- Travel
- wikiHow
- Work World
- Youth

CARBON NEUTRAL WEBSITE wikiHow is a carbon neutral website

SOME RIGHTS RESERVED All text shared under a Creative Commons License.

Powered by MediaWiki Powered by Mediawiki.

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

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.

9. The method of claim 8, 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.

10. 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;

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 portable handheld apparatus as claimed in any one of claims 1 to 4; wherein each of said portable handheld apparatus being associated with a unique user, each unique user being registered with said system manager.

11. The system of claim 10 further comprising a plurality of registered emergency centers and a plurality of registered service providers in communication with said system manager, to be accessed by said plurality of users; and

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.

Second 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. 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.

3. 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;

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 portable handheld apparatus as claimed in claim 1; wherein each of said portable handheld apparatus being associated with a unique user, each unique user being registered with said system manager.

4. The system of claim 3 further comprising a plurality of registered emergency centers and a plurality of registered service providers in communication with said system manager, to be accessed by said plurality of users; and

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.

How to Transfer Data Between a Cell Phone and Computer

originated by: Anonymous , AMIEE, Maluniu, Cheese319 (see all)

This guide will demonstrate how to retrieve and upload information and media from and to a cell phone from a PC.

Steps

edit

1 **Basic Instructions:** Contacts, Memo's, Pictures, Calander

1. Find/Purchase data link cable, something that has a prong for your cell phone on one end and a USB connector on the other. Try searching the make and model of your cell phone on Google or various online stores.
2. Install the drivers necessary for your cell phone; these should have come with the data link cable on a CD.
3. Download and install the BitPim software from http://www.bitpim.org/.
4. Plug your phone in, and run BitPim. It should automatically detect your phone.
5. The two buttons in the upper left tool bar are Get Phone Data and Send Phone Data; use these to quickly retrieve and send basic information stored on your phone's memory.

2 **Advanced Instructions:** Movies, Music, Memory Cards

1. Select View, then View Filesystems to open up more advanced possibilities
2. Look for folders that seem to contain useful information; on the Samsung a930, music and videos that are stored on the memory card are at /mmc1/MY_(FLIX /MP3S/MUSIC/PIC)
3. If you have several files (say, movies or pictures) you wish to remove at once, right click on the folder and select "Backup Directory". This will copy everything in that folder onto your computer.
4. Search online for advice about what can be done with your phone. Some phones are very limited on what file types they can use, others have size restrictions you need to know about. Every model of phone is different.

Tips

edit

- The Data Link Cable can also be used to charge your cell phone.
- Try searching online to find the "resolution" of your cell phones wall paper. That will make it easier to make properly sized images to use on your cell.
- The movie file type for cellphones vary, so you'll have to look online for a converter to and from more common file types. Youtube accepts a very wide variety of files, including .3g2, so it's possible to upload videos without a converter. For putting movies ON your phone, however, you will defiantly need something to convert it to your phones file type.
- If you're phone is having trouble connecting to your computer, it sometimes helps to try different USB ports.

Warnings

edit

Write An Article Random Article

Related wikiHows
- Unlock a Motorola Microtac 650E Cellphone
- Watch out for Long Term Agreements
- Automatically Sign Into Your Verizon Voicemail

Featured Articles
- Prepare for Childbirth With Yoga
- Cook in an Indoor Fireplace
- Reduce Energy Use While Cooking
- Survive in Federal Prison

Recent Changes

Want to join in?

Navigation -collapse
- Recent Changes
- Community Portal
- Forums
- Special pages
- Suggest a Topic
- List Suggested Topics

Editing Tools +expand

My Pages +expand

Become our Fan on Facebook

Follow us on Twitter

INTERNET ARCHIVE
Wayback Machine
85 captures
17 Apr 08 - 17 Mar 16
APR 2009 JUL 2011
Close
Help

Things You'll Need

edit

- Cellphone
- Computer
- Data Link Cable and Drivers

Related wikiHows

edit

- How to Unlock a Motorola Microtac 650E Cellphone
- How to Watch out for Long Term Agreements
- How to Automatically Sign Into Your Verizon Voicemail

Articles for You to Write

Here is a list of suggested articles that have not yet been written. You can help by researching and writing one of these articles.

- How to Use a USB Data Transfer Cable
- How to Sign Up for Verizon Email
- How to Download Music from a Computer to a Cell Phone
- How to Load Music Into a Samsung Cell Phone Memory Card
- How to How Do I Download Music to My Motorola Phone?

Article Info

Last edited:
October 2, 2009 by Milindo

Categories:
Ringtones and Other Downloads

Recent edits by: Lillian May, Chris Hadley, Sophie Caley (see all)

Article Tools

Share this Article

Discuss Print Email Watch Edit Send fan mail to authors

+ Embed this: Republish this entire article on your blog or website.

Thanks to all authors for creating a page that has been read 27,774 times.

Was this article accurate?

Yes **No**

wikiHow
the how to manual that you can edit

Home
About wikiHow
Help
Terms of Use
RSS
Site map

Explore Categories

Arts and Entertainment	Cars and Other Vehicles	Computers and Electronics	Education and Communications
Family Life	Finance and Business	Food and Entertaining	Health
Hobbies and Crafts	Holidays and Traditions	Home and Garden	Other
Personal Care and Style	Pets and Animals	Philosophy and Religion	Relationships
Sports and Fitness	Travel	wikiHow	Work World
Youth			

CARBON NEUTRAL WEBSITE wikiHow is a carbon neutral website
All text shared under a Creative Commons License.
Powered by MediaWiki. Powered by MediaWiki

\SDOCID: <XP_____55260933A__I_>0100115035122/http://www.wikihow.com/Transfer-Data-Between-a-Cell-Phone-and-Computer DESC page 1

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 July 2006 (20.07.2006)

PCT

(10) International Publication Number
WO 2006/076658 A2

(51) International Patent Classification:
H04M 15/00 (2006.01)

(21) International Application Number:
PCT/US2006/001375

(22) International Filing Date: 13 January 2006 (13.01.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/644,148 13 January 2005 (13.01.2005) US

(71) Applicant and
(72) Inventor: **POCRASS, Alan, L.** [US/US]; 41 Golden Glen Drive, Simi Valley, California 93065 (US).

(74) Agents: **BALDAUF, Kent, E.** et al.; The Webb Law Firm, 700 Koppers Building, 436 Seventh Avenue, Pittsburgh, Pennsylvania 15219-1845 (US).

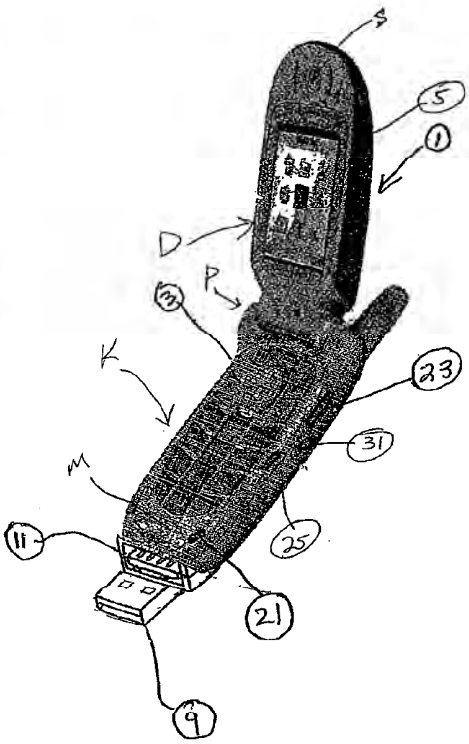
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: FLASH MEMORY CELL PHONE WITH INTEGRATED MALE AND FEMALE CONNECTORS



(57) Abstract: The invention is a cell phone (1) having a housing (3) operatively enclosing a keyboard K, a display D and cell phone circuitry C. A male USB connector (9) is at least partially enclosed by the housing (3) and a female USB connector (11) is at least partially enclosed by the housing (3). The cell phone circuitry C includes flash memory (13) and circuitry (15, 17) for enabling data to be transferred to or from the flash memory (13) via the male and female USB connectors (9 and 11).

WO 2006/076658 A2

FLASH MEMORY CELL PHONE WITH INTEGRATED MALE AND FEMALE CONNECTORS

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority from United States Provisional Patent Application No. 60/644,148, filed January 13, 2005, which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

[0002] Field of the Invention

[0003] The present invention relates to cell phones, and, more particularly, to a cell phone with integrated male and female connectors for transferring data to/from the cell phone.

[0004] Description of Related Art

[0005] Prior art cell phones do not include any means, other than wireless communication, for transferring data to/from the cell phone and another device, e.g., without limitation, another cell phone, without the use of a computer, a palm device or other like intelligent device. While the transfer of data utilizing wireless communication is possible with a number of different methods, such as Bluetooth, WiFi or cellular telephone technology, these methods limit the file sharing capabilities of the cell phone. Furthermore, these methods do not provide a fast means to transfer or copy data from one cell phone to another at high speeds.

[0006] Accordingly, a need exists for a cell phone that can transmit data stored therein or receive data for storage therein from another device, including another cell phone, via one or more connectors without the use of wireless communication or without the use of an intelligent device, like a computer, a palm device, etc. Still other needs that the present invention fulfills will become apparent to those of ordinary skill in the art upon reading and understanding the following Detailed Description.

SUMMARY OF THE INVENTION

[0007] The invention is a cell phone comprising at least one housing operatively enclosing a keyboard, a display and cell phone circuitry. A male connector is at least partially enclosed by the housing and a female connector, configured to mate with the male connector, is at least partially enclosed by the housing. The cell phone circuitry includes a flash memory and means for enabling data to be transferred to or from the flash memory via

the male and female connectors. At least one of said connectors is configured to mate with a mating connector of another device for transferring data to or from the flash memory.

[0008] The cell phone can include a battery coupled to provide power to the cell phone circuitry and/or a means for facilitating electrical connection of at least one of said connectors with the mating connector of the other device.

[0009] The device can be one of: another, like cell phone; a flash memory drive; a desktop or laptop computer; a palm device; a printer; a digital camera; and a scanner.

[0010] The cell phone can further include means for causing the transfer of data to or from the flash memory of the cell phone and/or means for setting the cell phone to transfer data to or from its flash memory.

[0011] A means for indicating that the transfer of data is in progress can also or alternatively be provided.

[0012] The cell phone can further include means for retrieving digital audio data from the flash memory; means for decoding the retrieved digital audio data; means for converting the decoded digital audio data into an analog signal; and an output connector for outputting the analog signal.

[0013] At least one of the male connector and the female connector can be a USB connector.

[0014] The invention is also a method of transferring data to/from a cell phone having integral male and female connectors from/to a device having a connector configured to mate with one of the connectors of the cell phone. The method includes mating one of the connectors of the cell phone with the mating connector of the device; and causing data to transfer from the cell phone to the device, or vice versa, via the mated connectors.

[0015] The method can further include setting the cell phone to be a master or a slave, wherein the data transfer occurs as a function of the setting of the cell phone as the master or the slave.

[0016] The male and female connectors of the cell phone can be USB connectors.

[0017] Lastly, the invention is a cell phone that comprises an enclosure; a male USB connector at least partially received within the enclosure; a female USB connector at least partially received within the enclosure; a flash memory disposed in the enclosure; and means disposed in the enclosure for transferring data to or from the flash memory via at least one of the male USB connector and the female USB connector when said connector is mated with a female USB connector or a male USB connector, respectively, of another device.

[0018] A battery can be coupled to provide power to the flash memory and the means for transferring.

[0019] The cell phone can further include means for causing the means for transferring to initiate the transfer of data to or from the flash memory; means for setting said cell phone as a master or a slave and for transferring data to or from the flash memory as a function of said setting; and/or means for facilitating electrical connection of at least one of the female USB connector and the male USB connector of the cell phone to the mating connector of the other device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] Fig. 1 is a perspective view of an exemplary cell phone 1 in accordance with the present invention including a male USB connector and a female USB connector;

[0021] Fig. 2 is a schematic of various components, electrical and mechanical, comprising the cell phone shown in Fig. 1;

[0022] Fig. 3 is a perspective view showing the mating of the male connector of one cell phone in accordance the present invention with the mating female connector of another cell phone in accordance with the present invention;

[0023] Fig. 4 is a perspective view of a cable having a male connector mating with the female connector of the cell phone in Fig. 1; and

[0024] Fig. 5 is a schematic of the circuits comprising the digital audio circuit shown in Fig. 2.

DETAILED DESCRIPTION OF THE INVENTION

[0025] The present invention will be described with reference to the accompanying figures where like reference numbers correspond to like elements.

[0026] With reference to Fig. 1, a cell phone 1 in accordance with the present invention includes a keyboard housing 3 configured to house a keyboard K having one or more buttons, a microphone M and related components and hardware required to electrically and physically support the operation of keyboard K, microphone M and the wireless transmitting and receiving functions of cell phone 1 in a manner known in the art. The illustrated embodiment of cell phone 1 further includes a display housing 5 configured to house a display D, a speaker S and related components and hardware required to electrically and physically support the operation of display D and speaker S in a manner known in the art.

[0027] The embodiment of cell phone 1 shown in Fig. 1 is a so-called flip-type phone wherein keyboard housing 3 and display housing 5 are pivotally joined together by a pivot joint P formed by the configuration and cooperation of keyboard housing 3 and display

housing 5 in a manner known in the art. However, this is not to be construed as limiting the invention since it is envisioned that another embodiment of cell phone 1 in accordance with the present invention can comprise a single housing (not shown) for housing the components and hardware described generally above in connection with the embodiment of cell phone 1 shown in Fig. 1. For purpose of describing the present invention, reference hereinafter will be made to the embodiment of cell phone 1 shown in Fig. 1. However, this is not to be construed as limiting the invention since the use of any configuration of a cell phone is envisioned.

[0028] In accordance with the present invention, cell phone 1 includes a male USB connector 9 and a female USB connector 11. Desirably connectors 9 and 11 are mini or mini-B type USB connectors. However, this is not to be construed as limiting the invention since it is envisioned that one or both of connectors 9 and 11 can be a USB-A type connector. Male USB connector 9 and female USB connector 11 are supported at least partially within keyboard housing K in any suitable manner known in the art, e.g., without limitation, via a printed circuit board.

[0029] Male USB connector 9 is configured to mate with a corresponding female USB connector of another device, such as, without limitation, another cell phone 1 in accordance with the present invention, a desktop or laptop computer, a palm device, an interface cable, etc. Female USB connector 11 is also configured to mate with a corresponding male USB connector of another device, such as, without limitation, another cell phone 1 in accordance with the present invention, an interface cable or a flash memory drive. The latter flash memory drive can either be a prior art flash memory drive, like the Lexar 256 MB USB 2.0 Jumpdrive, commercially available in the U.S. from the TigerDirect.com website, or a flash memory drive of the type disclosed in co-pending U.S. Patent Application No. 11/028,382, filed January 3, 2005, having an integrated male USB connector and a female USB connector, which is incorporated herein by reference, and which is commercially available in the U.S. under the trademark "Flashpoint Sharedrive" from the XMultiple.com website.

[0030] With reference to Fig. 2 and with continuing reference to Fig. 1, internal to keyboard housing 3 and/or display housing 5, cell phone 1 includes cell phone circuitry C, a battery B, a keyboard K, a microphone M, a display D and a speaker S. Cell phone circuitry C includes all of the necessary circuitry for supporting the software and hardware functions of cell phone 1 found in prior art cell phones, such as, without limitation, one or more flash memories, either integral on a chip with other circuits of cell phone circuitry C or as one or more standalone flash memories 13. For the purpose of describing the present invention, it

will be assumed hereinafter that cell phone circuitry C includes one or more standalone flash memory chips 13. However, this is not to be construed as limiting the invention since it is envisioned that the storage function performed by each standalone flash memory chip 13 can be incorporated into another chip of cell phone circuitry C.

[0031] In addition to including one or more flash memories 13, cell phone circuitry C of cell phone 1 includes a download/copy logic circuit 15 and a hub logic circuit 17, both of which support the transfer of data to or from flash memory chip 13 via male USB connector 9 and/or female USB connector 11 in a manner to be described hereinafter. Each of download/copy logic circuit 15 and hub logic circuit 17 can either be integral on a chip with other circuits of cell phone circuitry C or can be realized as standalone chips. For purpose of describing the present invention, it will be assumed hereinafter that cell phone circuitry C includes a standalone download/copy logic chip 15 and a standalone hub logic chip 17. However, this is not to be construed as limiting the invention since the function performed by one or both of chips 15 and 17 can be incorporated into another chip of cell phone circuitry C.

[0032] It is to be appreciated that battery B, cell phone circuitry C, including flash memory chip 13, download/copy logic chip 15 and hub logic chip 17, keyboard K, microphone M, display D and speaker S can be housed in keyboard housing 3 and/or display housing 5 of cell phone 1 in any manner deemed necessary and/or desirable by one skilled in the art. Moreover, the stacked arrangement of male and female USB connectors 9 and 11, respectively, extending from the microphone end of keyboard housing 3 in Fig. 1 is not to be construed as limiting the invention since it is envisioned that each said connector can be mounted anywhere in keyboard housing 3 or display housing 5 as deemed necessary and/or desirable by one skilled in the art. Accordingly, the stacked arrangement of connectors 9 and 11 at the microphone M end of keyboard housing 3 is not to be construed as limiting the invention.

[0033] Download/copy logic chip 15 is electrically connected to flash memory chip 13 for facilitating the transfer of data stored in flash memory chip 13 to and/or from another device such as, without limitation, the flash memory of another, like cell phone 1, a flash memory drive, a desktop or laptop computer, a palm device, a printer, a digital camera, a gaming device, a scanner, and the like. Hub logic chip 17 is connected and operative for facilitating connection of one or both of male USB connector 9 and female USB connector 11 to a universal serial bus having connected thereto said other device. Battery B provides electrical power to cell phone circuitry C, including flash memory chip 13, download/copy

logic chip 15 and hub logic chip 17, to support the electrical operation thereof when cell phone 1 is not attached to an external power source or the USB port of an externally powered device, such as a computer, a palm device, etc. Battery B providing electrical power to the combination of flash memory chip 13, download/copy logic chip 15 and hub logic chip 17 thereby enables data to be transferred to/from flash memory chip 13 from/to another device attached to male USB connector 9 or female USB connector 11 without the use of externally provided power. Cell phone circuitry C can include a charging circuit 19 that facilitates the charging of battery B when male USB connector 9 or female USB connector 11 is connected to an externally powered device.

[0034] The disclosure herein of cell phone 1 including battery B is not to be construed as limiting the invention since it is envisioned that cell phone 1 may also or alternatively include other power supplies, such as one or more solar cells, that can be utilized to power cell phone circuitry C. The circuits of cell phone circuitry C normally associated with the functions of a prior art cell phone as well as flash memory chip 2, download/copy logic chip 15, hub logic chip 17 and charging circuit 19 can be implemented on one or more integrated circuit chips in any suitable and/or desirable manner deemed necessary and/or desirable by one of ordinary skill in the art.

[0035] With reference to Fig. 3 and with continuing reference to Figs. 1 and 2, a first cell phone 1a and a second cell phone 1b, both in accordance with the present invention, can be communicatively joined together by mating the male USB connector 9a of first cell phone 1a with the female USB connector 11b of second cell phone 1b, or by mating the male USB connector 11a of second cell phone 1b with the female USB connector 9b of first cell phone 1a for the purpose of transferring or copying data from the flash memory chip 13 of first cell phone 1a to the flash memory chip 13 of second cell phone 1b, or vice versa.

[0036] Each cell phone 1 in accordance with the present invention can include a master/slave switch 21 coupled to download/copy logic chip 15 for setting cell phone 1 as either a master or a slave. In operation, when first cell phone 1a and second cell phone 1b are communicatively joined together, the cell phone 1 set to be the master (transmitting unit) by its master/slave switch transfers data from its flash memory chip 13 to the flash memory chip 13 of the cell phone 1 set to be the slave (receiving unit) by its master/slave switch under the control of download/copy logic chip 15 of the cell phone 1 set as the master. For example, first cell phone flash memory drive 1a can be set as the master and second cell phone 1b can be set as the slave using their respective master/slave switches 21. Hence, when first cell phone 1a (set as the master) and second cell phone 1b (set as the slave) are communicatively

joined together, data is transferred from the flash memory chip 13 of first cell phone 1a to the flash memory chip 13 of second cell phone 1b under the control of the download/copy chip 15 of cell phone 1a.

[0037] Desirably, download/copy logic chip 15 of each cell phone 1 set as a master controls the transfer of data from its flash memory chip 13 to another device connected to cell phone 1 by its male or female USB connector 9 or 11. Alternatively, when each cell phone 1 is set as a slave, download/copy logic chip 15 initially assumes a passive role in the download of data into its flash memory chip 13 when cell phone 1 is connected via its male or female USB connector 9 or 11 to another device. However, if the device connected to cell phone 1 is a passive device, such as a prior art flash memory drive, download/copy logic chip 15 can be configured to assume control of the download of data into the flash memory chip 13 of its cell phone 1 even when said cell phone 1 is set as a slave.

[0038] Also or alternatively, the function of switch 21 to set cell phone 1 as a master or a slave can be accomplished programmatically via cell phone circuitry C, keyboard K and display D of cell phone 1 whereupon switch 21 may be omitted. To this end, keyboard K, display D and cell phone circuitry C can be configured to enable a user of cell phone 1 to program cell phone 1 as a master or slave as desired.

[0039] Cell phone 1 in accordance with the present invention can also be utilized with flash memory drives such as prior art flash memory drives or flash memory drives of the type disclosed in co-pending U.S. Patent Application No. 11/028,382, filed January 3, 2005, having integrated male and female USB connectors which are commercially available in the U.S. under the trademark "Flashpoint Sharedrive" from the XMultiple.com website. To this end, when a cell phone 1 in accordance with the present invention is utilized with a flash memory drive having a USB connector thereof coupled with a mating USB connector of cell phone 1, cell phone 1 can be set as the master for transferring data from its flash memory chip 13 to the flash memory chip of the flash memory drive. Alternatively, cell phone 1 can be set as the slave for transferring data into its flash memory chip 13 from the flash memory chip of the flash memory drive. Desirably, when cell phone 1 is connected to a prior art flash memory drive that does not include an intelligent controller, download/copy logic chip 15 controls the transfer data into the flash memory chip 13 of its cell phone 1 when said cell phone 1 is set as a slave.

[0040] Cell phone circuitry C can be configured to enable a user of cell phone 1 to programmatically select via keyboard K and display D which data or data file to transfer

to/from its flash memory chip 13 from/to a device communicatively joined to cell phone 1 via its male or female USB connector 9 or 11.

[0041] When male USB connector 9 of a cell phone 1 in accordance with the present invention is mated with a female USB connector of another intelligent device, such as a computer, a palm device, and the like, the transfer of data to the flash memory chip 13 of cell phone 1 can be controlled via the device in a manner known in the art. Desirably, it is only when cell phone 1 is set as the master that download/copy logic chip 15 is operative for controlling the transfer of data from its flash memory chip 13. In contrast, when cell phone 1 is set as a slave, data can be transferred into its flash memory chip 13 under the control of another device, such as another cell phone 1 in accordance with the present invention, a computer, a palm device, etc., having the necessary intelligent controller for controlling such data transfer.

[0042] Each cell phone 1 can include a push button switch 23 accessible via keyboard housing 3 and coupled to download/copy logic circuit 15 which allows for manual activation of the transfer of data into or out of flash memory chip 13 of cell phone 1. For example, in response to activation of push button switch 23 of cell phone 1a set as a master, download/copy logic circuit 15 of first cell phone 1a transfers data from its flash memory chip 13 to another device communicatively joined thereto.

[0043] Also or alternatively, the function of push button switch 23 can be implemented programmatically via cell phone circuitry C, keyboard K and display D of cell phone 1 whereupon push button switch 23 may be omitted.

[0044] Each cell phone 1 can also include an optional lamp 25 that is illuminated and visible when data is being transferred to or from the flash memory chip 13 of cell phone 1. Lamp 25 may be selected from any light emitting device suitable for such an application, such as, without limitation, a light emitting diode (LED).

[0045] Also or alternatively, the notice provided by lamp 25 can be implemented by display D which can be operative under the control of cell phone circuitry C for displaying a suitable indication when data is being transferred to or from its flash memory chip 13, whereupon lamp 25 may be omitted. If desired, display D can display a first indication when data is being transmitted from cell phone 1 and can display a second indication when data is being received by cell phone 1.

[0046] With reference to Fig. 4 and with continuing reference to Figs. 1 and 2, cell phone 1 may also be used to maximize the available USB ports on a computer, a palm device, etc. Specifically, male USB connector 9 of cell phone 1 may be inserted into a female USB

port of a computer (not shown). Thereafter, female USB connector 11 of cell phone 1 can accept a male USB connector 27 of a USB cable. This enables peripheral devices, such as, without limitation, cameras, printers, scanners, flash memory drives, other cell phones in accordance with the present invention, and the like, to utilize the same USB port on the computer as cell phone 1.

[0047] With reference back to Fig. 2, if desired, cell phone 1 in accordance with the present invention can include a digital audio circuit 29, integral with another circuit of cell phone circuitry C or as a standalone chip, and an output connector 31, such as a headphone jack. Digital audio circuit 29 includes a digital signal processor (DSP), an amplifier 37 and a digital-to-analog converter (DAC) 35. DSP 33 can retrieve digital audio data from flash memory chip 13 and can decode said digital audio data utilizing a decompression algorithm, such as a MP3 or WMA decompression algorithm, that undoes the compression of the digital audio data stored in a corresponding format on flash memory chip 13. Then, DAC 35 converts the decompressed audio data back into analog audio data. Finally, amplifier 37 boosts the strength of the signal and sends it to output connector 31 or to speaker S. Keyboard K can include one or more buttons for controlling digital audio circuit 29. These buttons can perform such functions as increasing/decreasing volume, playing the digital audio data, stopping, pausing, skipping, rewinding, and the like.

[0048] Cell phone 1 of the present invention can be configured such that display D can display a visual indication of the title of the digital audio data, the time remaining in a song and/or other such digital audio data and other useful and desirable information. Display D can be a liquid crystal display (LCD), a plasma screen, and the like.

[0049] The present invention is also a method for transferring data to or from the flash memory chip 13 of cell phone 1 in accordance with the present invention. In the method, one of the connectors of cell phone in accordance with the present invention is mated with a mating connector of another device, such as, without limitation, another cell phone 1 in accordance with the present invention, a flash memory drive, a computer, a palm device, and the like. Thereafter, data is transferred into or out of cell phone according to the setting of the cell phone as a master or slave, wherein, when the cell phone is set as a master, data is transferred from the cell phone via the one of the connectors and, when the cell phone is set as a slave, data is transferred into the cell phone via the one of the connectors. The transfer of data into or out of the cell phone can be caused by the user activating one or more switches or buttons of the cell phone. The preceding method is illustrative of the transfer of data into

or out of cell phones in accordance with the present invention and is not to be construed as limiting the invention.

[0050] While the present invention was described with reference to preferred embodiments of the cell phone with integrated male and female connectors, those skilled in the art may make modifications and alterations to the present invention without departing from the scope and spirit of the invention. Accordingly, the above detailed description is intended to be illustrative rather than restrictive. The invention is defined by the appended claims, and all changes to the invention that fall within the meaning and range of equivalency of the claims are to be embraced by their scope.

THE INVENTION CLAIMED IS:

1. A cell phone comprising:

at least one housing operatively enclosing a keyboard, a display and cell phone circuitry;

a male connector at least partially enclosed by the housing; and

a female connector at least partially enclosed by the housing and configured to mate with the male connector, wherein:

the cell phone circuitry includes a flash memory and means for enabling data to be transferred to or from the flash memory via the male and female connectors; and

at said one of said connectors is configured to mate with a mating connector of another device for transferring data to or from the flash memory.

2. The cell phone of claim 1, further comprising a battery coupled to provide power to the cell phone circuitry.

3. The cell phone of claim 1, further comprising means for facilitating electrical connection of at least one of said connectors with the mating connector of the other device.

4. The cell phone of claim 1, wherein the other device is one of:

another, like cell phone;

a flash memory drive;

a desktop or laptop computer;

a palm device;

a printer;

a digital camera; and

a scanner.

5. The cell phone of claim 1, further comprising means for causing the transfer of data to or from the flash memory of the cell phone.

6. The cell phone of claim 1, further comprising means for setting the cell phone to transfer data to or from its flash memory.

7. The cell phone of claim 1, further comprising means for indicating that the transfer of data is in progress.

8. The cell phone of claim 1, further comprising:
means for retrieving digital audio data from the flash memory;
means for decoding the retrieved digital audio data;
means for converting the decoded digital audio data to an analog signal; and
an output connector for outputting the analog signal.

9. The cell phone of claim 1, wherein at least one of the male connector and the female connector is a USB connector.

10. A method of transferring data to/from a cell phone having integral male and female connectors from/to a device having a connector configured to mate with one of the connectors of the cell phone, the method comprising:
mating one of the connectors of the cell phone with the mating connector of the device; and
causing data to transfer from the cell phone to the device, or vice versa, via the mated connectors.

11. The method of claim 10, further comprising:
setting the cell phone to be a master or a slave, wherein the data transfer occurs as a function of the setting of the cell phone as the master or the slave.

12. The method of claim 10, wherein, the male and female connectors of the cell phone are USB connectors.

13. The method of claim 10, wherein the device is one of:
another, like cell phone;
a flash memory drive;
a desktop or laptop computer;
a palm device;
a printer;

BNSDOCID: <WO____2006076658A2_I_>

a digital camera; and

a scanner.

14. A cell phone comprising:

an enclosure;

a male USB connector at least partially received within the enclosure;

a female USB connector at least partially received within the enclosure;

a flash memory disposed in the enclosure; and

means disposed in the enclosure for transferring data to or from the flash memory via at least one of the male USB connector and the female USB connector when said connector is mated with a female USB connector or a male USB connector, respectively, of another device.

15. The cell phone of claim 14, further comprising a battery coupled to provide power to the flash memory and the means for transferring.

16. The cell phone of claim 14, further comprising means for causing the means for transferring to initiate the transfer of data to or from the flash memory.

17. The cell phone of claim 14, further comprising means for setting said cell phone as a master or a slave and for transferring data to or from the flash memory as a function of said setting.

18. The cell phone of claim 14, further comprising means for facilitating electrical connection of at least one of the female USB connector and the male USB of the cell phone to the mating connector of the other device.

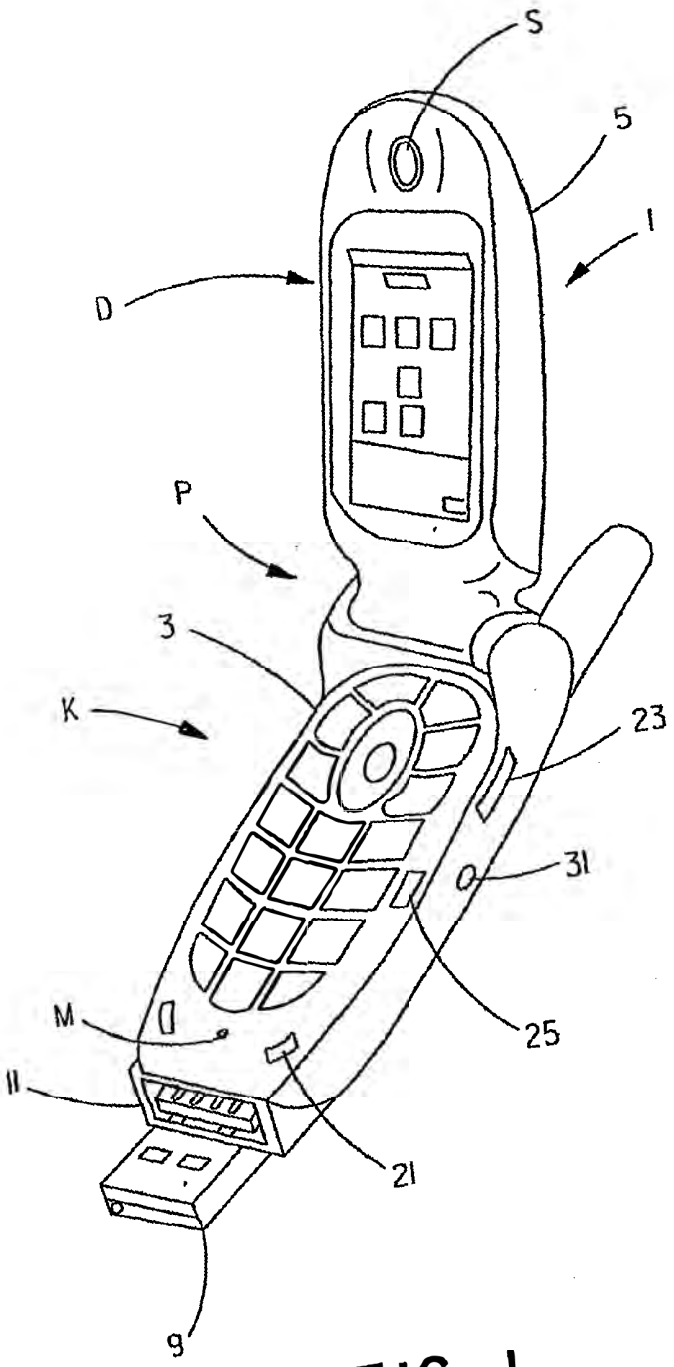


FIG. 1

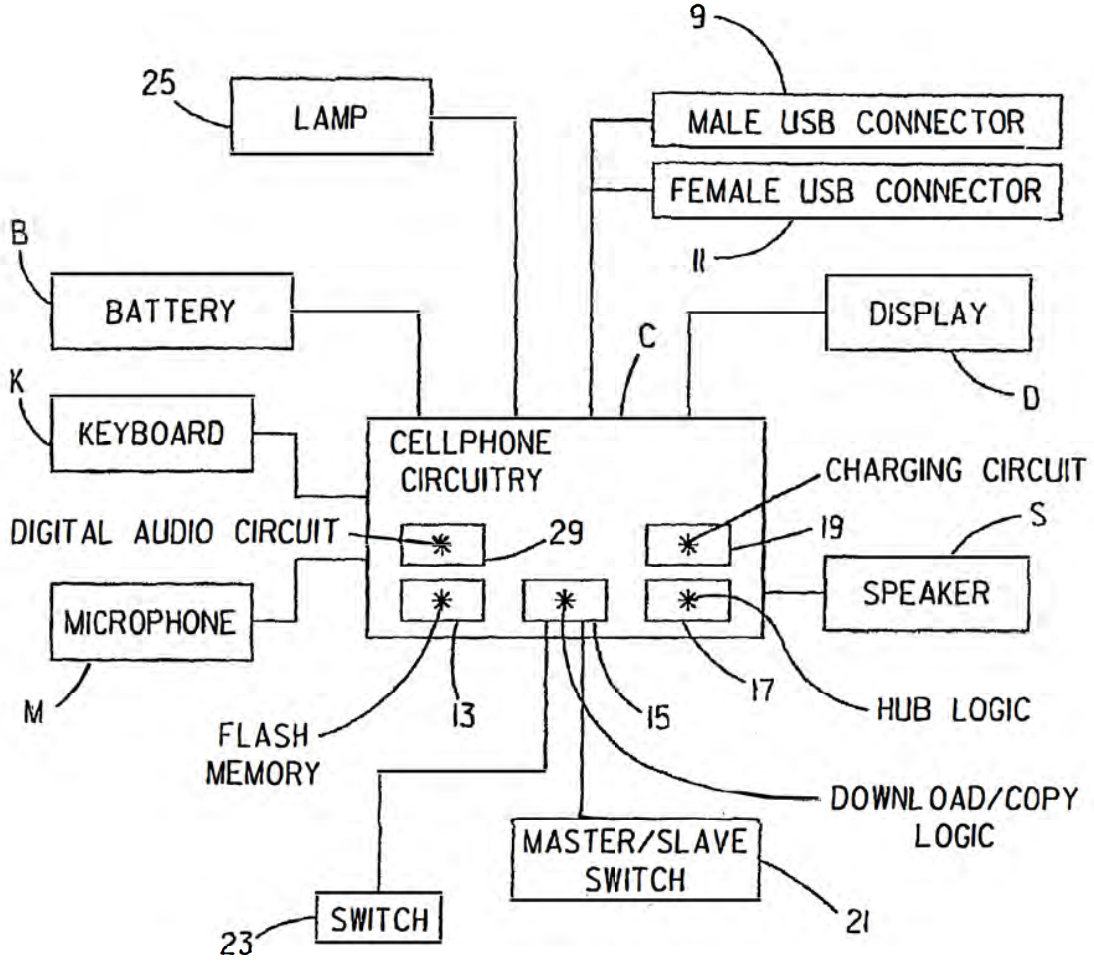

9
25
LAMP
MALE USB CONNECTOR
FEMALE USB CONNECTOR
11
B
BATTERY
DISPLAY
C
D
K
KEYBOARD
CELLPHONE CIRCUITRY
CHARGING CIRCUIT
DIGITAL AUDIO CIRCUIT
29
19
S
SPEAKER
MICROPHONE
M
FLASH MEMORY
13
15
17
HUB LOGIC
DOWNLOAD/COPY LOGIC
MASTER/SLAVE SWITCH
21
SWITCH
23

FIG. 2

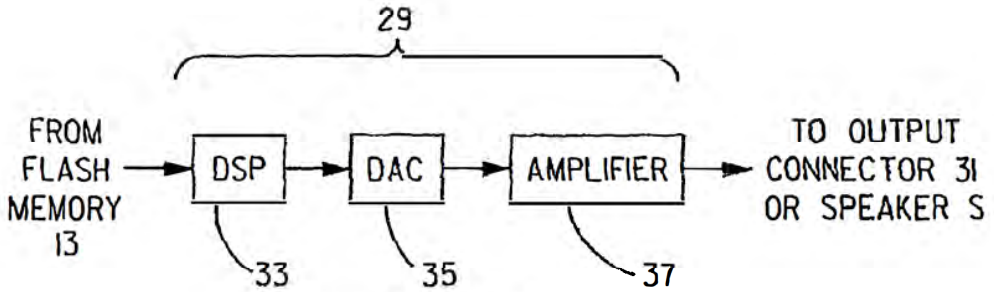
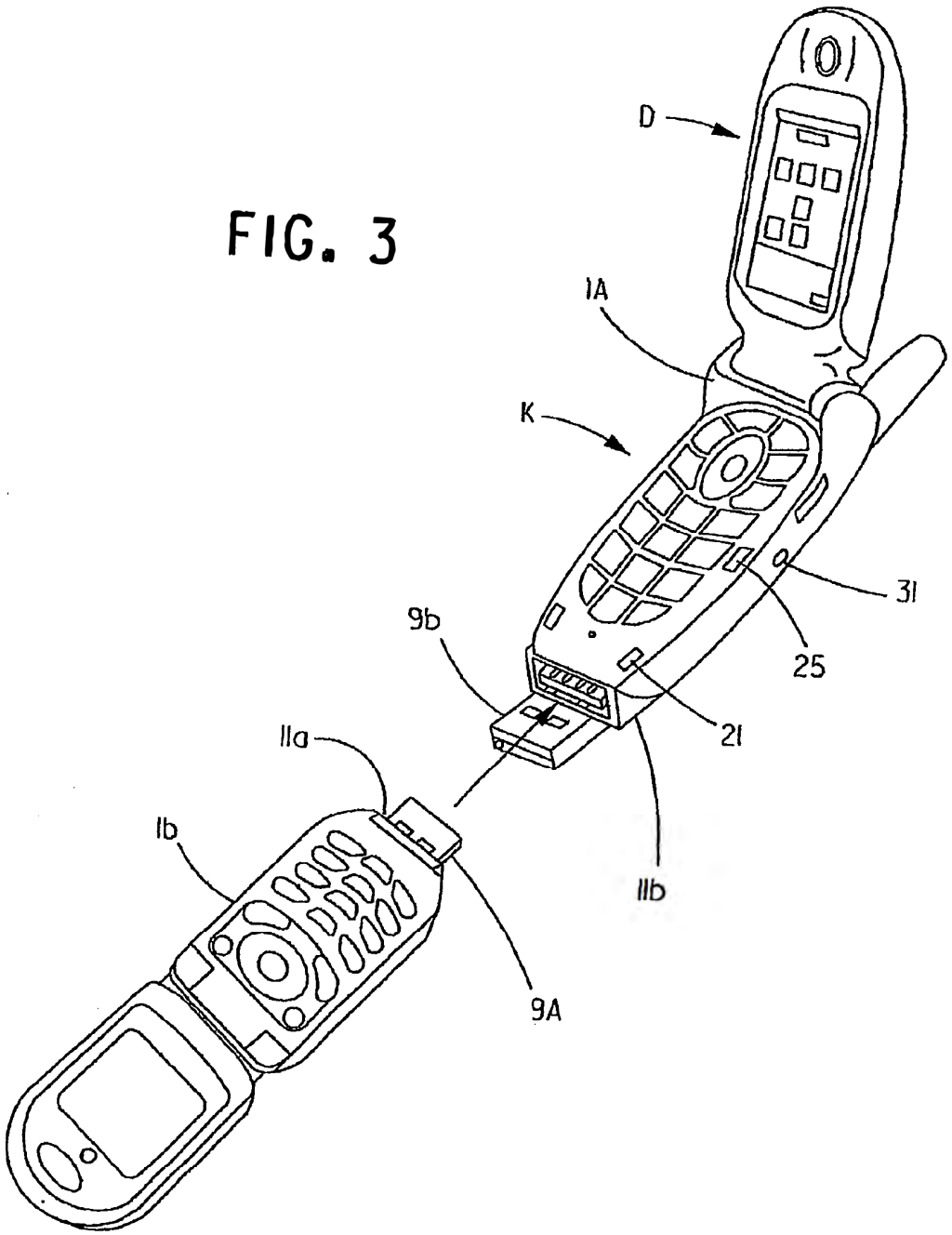

29
FROM FLASH MEMORY 13
DSP
DAC
AMPLIFIER
TO OUTPUT CONNECTOR 31 OR SPEAKER S
33
35
37

FIG. 5

FIG. 3



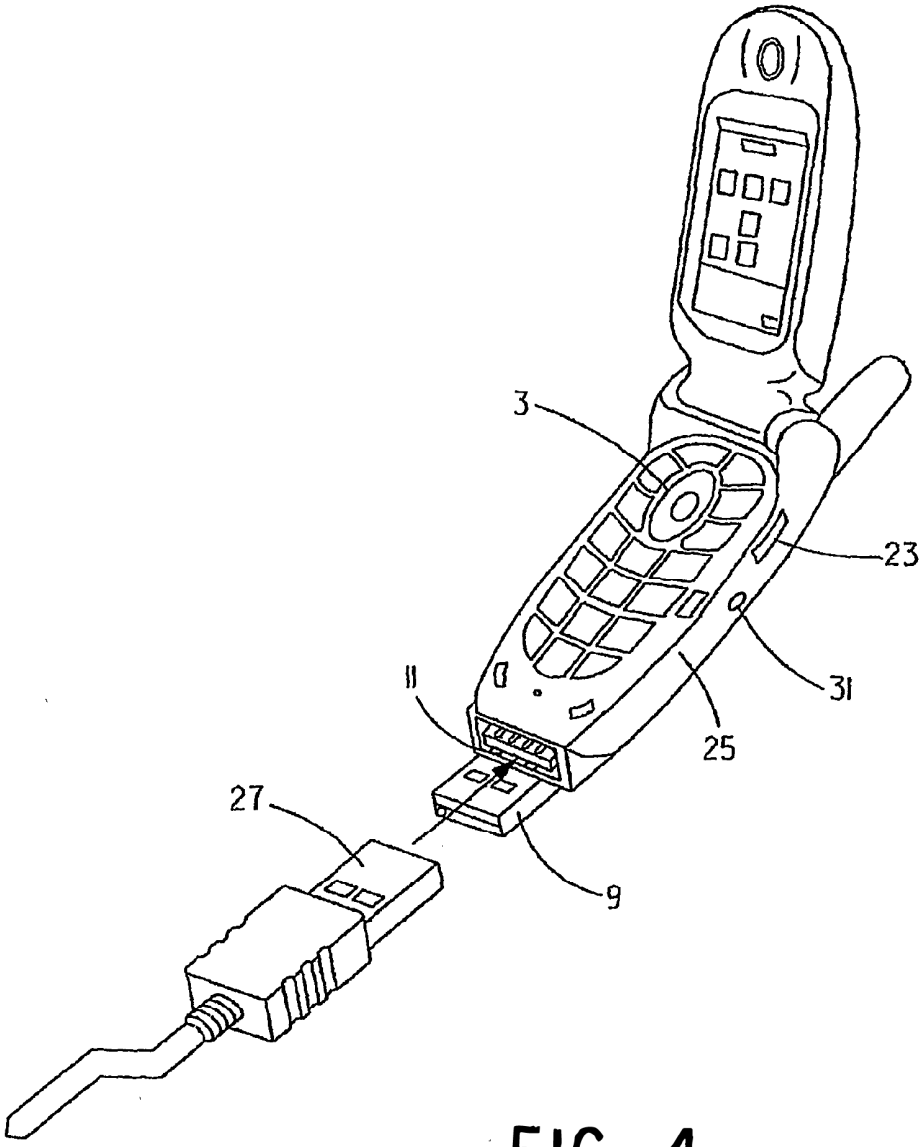


FIG. 4

Main 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, 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 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 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.

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 portable handheld 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 porable handheld 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 portable handheld 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 portable handheld apparatus, including the identification data of said user, the personal medical data file of said user, and location of said user; or wherein said portable handheld 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 portable handheld 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 personal identification unit being operable to interphase with an external device for activation of various operations between the personal identification unit and the handheld apparatus, 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 personal identification unit 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 exrernal device and the operation of the personal identification unit 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 personal identification unit 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 said personal identification unit 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 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 the 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 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.

9. The method of claim 8, 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.

10. 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 portable handheld units as claimed in any one of claims 1 to 4; wherein each of said portable handheld apparatus being associated with a unique user, each unique user being registered with said system manager.

11. The system of claim 10 further comprising

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 portable handheld 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.

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

to communicate with said portable handheld units to compare the user's ID data file stored in the unique user's portable handheld 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 portable handheld 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 portable handheld unit to said user portable handheld unit, said portable handheld unit responding with a second string of coded alphanumeric data uniquely associated with said user portable handheld 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 portable handheld unit further comprises an emergency button in communication with said processing module and said communication and data connection means module;

wherein the portable handheld 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 portable handheld 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.

13. The system of claim 10, 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

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
24.05.2016

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 : 2007 + 2916 + annexes

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

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: 24.05.2016

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 : 2007 + 2916 + annexes

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 :

27 May 2016

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

FRKELLY
EUROPEAN PATENT AND TRADE MARK ATTORNEYS

European Patent Office
D-80298 Munich
Germany

Your Ref : 11752936.2
Our Ref : P105633EP00

21 July 2016

Dear Sirs,

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

The Applicant of the above-referenced European patent application, namely:

OS - NEW HORIZON PERSONAL COMPUTING SOLUTIONS LTD.
10/3 Efroni Street
P.O. Box 84275
90805 Mevasseret Zion
Israel

hereby appeals the Decision of the Examining Division dated 24 May 2016.

The Decision is appealed in its entirety and we request that it be set aside and a patent granted according to the requests on file or as modified with the grounds of appeal to be filed in due course.

The Grounds of Appeal will follow shortly. The Appeal fee is being paid today from our deposit account using on-line fee payment.

Yours faithfully,

Paul Keane
Representative

MARY BLEAHENE
DAVID BROPHY
PHILIP COYLE
ASSUMPTA DUFFY
GAVAN FERGUSON
CAROL GORMLEY
NIAMH HALL
PAUL KEANE
DONAL M KELLY
SUMI NADARAJAH
MAURA O'CONNELL
BRIAN O'NEILL
BRENDA O'REGAN
SHANE SMYTH
ALAN WALLACE
STEPHEN WALLER

ANNA HALLY
ALAN CASEY
DAVID FLYNN
STEPHEN MURPHY
JOHN O'FLAHERTY
BRONWYN O'HAGAN
MICHAEL SCANNELL
SHAUNA TILLEY

CONSULTANT:
LINDSAY J CASEY

Europäisches Patentamt
European Patent Office
Office européen des brevets

Letter accompanying subsequently filed items

Representative:

Mr Paul Keane
FRKELLY
27 Clyde Road
D04 F838 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	Notice of appeal	P105633EP00 Notice of appeal July21.pdf	APPEAL.pdf

	Fees	Factor applied	Fee schedule	Amount to be paid
15-1	011 Fee for appeal	1	1 880.00	1 880.00
	Total:		**EUR**	**1 880.00**

	Payment	
1	Mode of payment	Debit from deposit account
	Currency:	EUR
	The European Patent Office is hereby authorised, to debit from the deposit account with the EPO any fees and costs indicated on the fees page.	
	Deposit account number:	28060009
	Account holder:	FRKELLY
2	Refund/Reimburserment	
	Reimbursement (if any) to be made to EPO deposit account:	28060009
	Account holder:	FRKELLY

Signatures

Place:

Date: **21 July 2016**

Signed by: **Paul Keane 36258**

Representative name: **Paul Keane**

Capacity: (Representative)

P105633EP00

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	4512653	
Application number	EP11752936.2	
Date of receipt	21 July 2016	
Receiving Office	European Patent Office, The Hague	
Your reference	P105633EP00	
Applicant	All applicants as on file	
Documents submitted	package-data.xml epf1038.pdf (2 p.)	ep-sfd-request.xml APPEAL.pdf\P105633EP00 Notice of appeal July21.pdf (1 p.)
Submitted by	CN=Paul Keane 36258	
Method of submission	Online	
Date and time receipt generated	21 July 2016, 17:59 (CEST)	
Message Digest	36:83:84:3F:8F:97:85:C8:86:29:52:83:F8:F1:DF:9F:B6:9F:87:36	

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

Letter accompanying subsequently filed items

Representative:

Mr Paul Keane
FRKELLY
27 Clyde Road
D04 F838 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

Annotations

Representative(FRKELLY; 26.09.2016)
1 Remark(Annotate)
Please update the register to reflect that the following representative is responsible for this Application

Keane, Paul Fachtna
FRKelly
27 Clyde Road
Dublin D04 F838 / IE

Signatures

Place:	
Date:	**26 September 2016**
Signed by:	**Paul Keane 36258**
Representative name:	**Paul Keane**
Capacity:	**(Representative)**

FRKELLY
EUROPEAN PATENT AND TRADE MARK ATTORNEYS

European Patent Office
D-80298 Munich
Germany

Your Ref : 11752936.2
Our Ref : P105633EP00

26 September 2016

Dear Sirs,

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

I refer to the notice of appeal which was filed on July 21 2016 in the connection with the above identified European Patent Application. The grounds of appeal are provided herewith and we have therefore completed the necessary action to validly file the appeal.

Requests for the Appeal

The Main Request, First Auxiliary Request, and Second Auxiliary Request correspond to the requests filed in preparation for the Oral Proceedings on 11.03.16.

We also wish to include a Third Auxiliary Request, a Fourth Auxilairy Request, a Fifth Auxiliary Request and a Sixth Auxiliary Request. The Third Auxiliary Request corresponds to the Main Request with the exception that the term "*external device*" has been replaced with the term "*mobile communication device or a personal computer*". The Fourth Auxiliary Request corresponds to the Main Request with the exception that the term "*external device*" has been replaced with the term "*mobile communication device*". The Fifth Auxiliary Request is based on the Second Auxiliary Request but has been further revised to address the added matter objections. The Sixth Auxiliary Request is based on the Second Auxiliary Request but has been further revised to address the added matter objections.

Reimbursement of the appeal fee is requested on the grounds that the Decision under appeal is not sufficiently reasoned and the Applicant's rights pursuant to Article 113 were violated, this representing a substantial procedural violation.

Summary of EPO Communications

(A) The Supplementary European search report identified lack of unity of invention and cited the following documents for the first invention:

D1: US 2009/083847 A 1
D2: US 6 957 337 B1
D3: US 5 229 764

MARY BLEAHENE
DAVID BROPHY
PHILIP COYLE
GAVAN FERGUSON
CAROL GORMLEY
NIAMH HALL
PAUL KEANE
DONAL M KELLY
SUMI NADARAJAH
MAURA O'CONNELL
BRIAN O'NEILL
BRENDA O REGAN
SHANE SMYTH
ALAN WALLACE
STEPHEN WALLER
ALAN CASEY
ANNA HALLY
EOGHAN MCNALLY
DAVID FLYNN
EMMA KELLY
SUSAN C KELLY
LUKE MAGHMAN
STEPHEN MURPHY
JOHN O'FLAHERTY
SIOBHAN O'HAGAN
MICHAEL SCANNELL
CAROLINE SHEEHAN
SHAUNA TULEY
LOUISE J CASEY
OFFICES: DUBLIN & BELFAST

FRKelly | 27 Clyde Road, Dublin D04 F838, Ireland | Tel: +353 1 231 4848 | Fax: +353 1 614 4756 | dublin@frkelly.com | www.frkelly.com

(B) In a communication under Article 94(3) EPC issued by the examining division on 05-01-2015, objections under Article 123(2) EPC were raised, and objections under Article 82 EPC, as well as under Article 56 EPC for the first invention, were maintained.

(C) On 14-10-2015 the examining division issued a summons to attend oral proceedings on 13.04.2016. In the annex to the summons, objections under Article 123(2) EPC were raised. Objections under Article 82 EPC, as well as under Article 56 EPC for the first invention, were maintained. A reply to the applicant's arguments was also given.

(D) In a communication sent by telefax on 30-03-2016 the applicant was informed that the date fixed for oral proceedings was maintained. In an annex, the examining division expressed its preliminary opinion that none of the present set of claims was compliant with requirements of Article 123(2) EPC, and that, to the extent that the claimed subject-matter was present in the application as originally filed, it was not inventive. The arguments therefore were provided. The objection regarding the unity of invention was also maintained.

(E) In an electronic communication on 11-04-2016 the representative informed the examining division that he would not be attending the oral hearing. The request for oral hearing was withdrawn, and a decision according to the current state of the file was requested.

(F) With a telefax communication on 11-04-2016 the applicant was informed that the oral proceedings were cancelled.

The decision is based on the following request(s):

Main Request
First Request
Second Request.

In Section IV of the Decision three additional prior art were cited:

(i) XP055260933,
(ii) XP055260935,
(iii) W02006076658.

Substantial Procedural Violation

These additional prior art documents are provided by the Examining Division to support the statement in section 2.4 of the Decision that, at the time of filing the present application, the techniques for transferring data between a cell phone and a computer were well known.

Section 2.4 of Decision states

Considering the feature introduced with the amendment, to the extent that it is present in the application as originally filed, namely, that the apparatus is

operable to interphase with a cellular phone or a host personal computer for activation of various operations between the cellular phone/host computer and the apparatus, at the time of filing the present application the techniques for transferring data between a cell phone and computer were well known. Therefore, in the context of document D1, this feature represents a mere juxtaposition of a known technique and cannot be considered as basis of an inventive step.

It is respectfully submitted that the Applicant's right to be heard pursuant to Article 113 (1) was violated as the Applicant did not have an opportunity to comment on the newly cited prior art documents

(i) XP055260933,
(ii) XP055260935,
(iii) W02006076658.

Documents (i)-(iii) represents new evidence which is relevant for assessing inventive step and unity of invention. The Examiner indicated in item 2 of Section IV (Final Remarks) that the main request lacks unity within the meaning of article 82 EPC, for the following reasons:

As shown here above in the section Reasons for the Decision, the independent claims 1 and 5 lack inventive step, leaving the dependent claims without a common inventive concept. The six inventions addressed by dependent claims are identified as follows:

I. Life sign detectors (claim 2 and part of claims 6 and 11):
II. Providing user data to emergency services (part of claims 3, 6 and 7, claim 13);
III. Interaction via the keyboard and display of a second device (part of claim 3);
IV. Connecting to a magnetic strip interface (part of claim 7);
V. Charging the apparatus and updating its data (claim 4 and part of claim 7);
VI. Centralized data management (claims 8-12).

The Applicant vigorously disagreed throughout the prosecution of the application that claims 1 and 5 lack an inventive step and lack unity. The lack of unity objection is based on the understanding by the Examining Division that claims 1 and 5 lack an inventive step which is contested by the Applicant.

As outlined below the Examining division incorrectly omitted the following features of claim 1 from the inventive step analysis on the grounds of added matter

"the apparatus is operable to interphase with an external device"

"access to the stored personal data files in said first memory module is denied to said external device"

It now appears that the three newly cited documents are used to provide a basis that the feature "*the apparatus is operable to interphase with an external device*" lacks an inventive step. Accordingly, these newly cited documents now seem to form the basis for maintaining the inventive step and unity objection objections.

As these newly cited documents were not cited during written proceedings the Applicant's right to be heard pursuant to Article 113 has been violated.

Article 113(1) EPC enshrines a party's right to be heard. Thus decisions may only be based on grounds or evidence on which the parties concerned have had an opportunity to present their comments. When a new document is first cited by the examining division as result of request for a decision according to the current state, this basic procedural right has not been observed in the present case.

The Applicant did not surrender their right to be heard pursuant to Article 113 by virtue of requesting a decision according to the current state of the file. As a consequence, the decision is fundamentally flawed in its non-observance of a fundamental procedural right.

Main Request

The Applicant's response to the reasons for the Decision follows the same numbering sequence as used in section II of the Decision

Added Matter

1. The Examining Division indicated that the amendments of the main request are not compliant with the requirements of Art.123(2) EPC. The Applicant disagrees with this assessment.

1.1 In particular, the Examining Division indicated that the amendment of claims 1 and 5: "*the apparatus is operable to interphase with an external device*" is not directly and unambiguously derivable from the description.

> "*From the passage cited by the applicant, and the last passage on page 39, it is derivable that the apparatus is operable to interphase with a cellular phone or a host personal computer for activation of various operations between the cellular phone/host computer and the apparatus. However, it is not derivable that the apparatus is operable to interphase with any other external device, as claimed.*"

The premise of the examiners' objection is that it is not derivable that the apparatus is operable to interphase with external devices other than a "host personal computer" or a "cellular phone". The Applicant disagrees.

Firstly, the Applicant wishes to point out that the description actually defines the cellular phone and host personal computer as being "external devices". For example, page 16 of the description lines 5-8 recites

"*wherein the computer or cellular phone have a keyboard and display units associated therewith, thereby allowing the user to interact with the memory module and with the processing module of the apparatus via the* ***external devices keyboard and display units.***"

A person skilled in the art would understand using normal daily english that the computer and cellular phone are described as being external devices. Accordingly, the "term external device" is directly and unambiguously derivable from the application as originally filed in accordance with Article 123(2).

Secondly, page 22 lines 18 to page 23 line 8 describes external devices other that a host computer or a cellular phone. "*Referring now to the drawings, Figure 1 illustrates the dedicated system 300 related to an embodiment of the present invention, when a pre-approved user is getting an access to the system through any one of the system server based* ***multi-user I/0 terminals 362, or through any kind of a host personal computer 360, or alternatively getting the access through a digital landline phone 365, or a cellular phone unit, 355****. Secured access to the system is enabled by passing the user through a sequence of at least three bio parameters measurement and authentication process, carried out by the user's apparatus 350.*"

Figure 1 is reproduced below for the examiner's convenience.

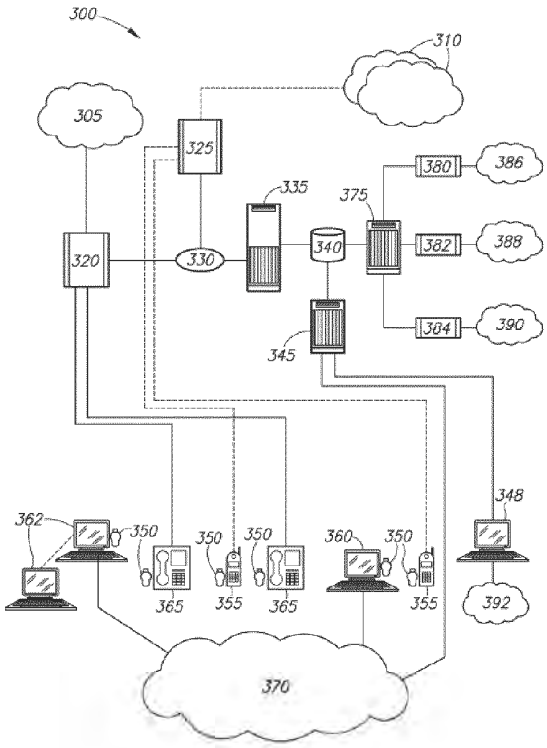


FIG.1

In Figure 1 the exemplary external devices are

1) multi-user I/0 terminals 362, or
2) a host personal computer 360, or
3) a digital landline phone 365, or
4) a cellular phone unit, 355.

It is respectfully submitted that the term 'external device' is recited in the original PCT claim 1 "*....connecting said apparatus with an external device*".

Furthermore, the original PCT claim 8 recites "*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***".

Additionally, the original PCT claim 15 recites "*The apparatus according to claim 1, further comprising 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 Applicant notes that page 15 lines 5 and 6 recites "*.....for connecting the apparatus with an external device. "*

It is respectfully submitted that a person skilled in the art would readily understand that in the context of the application as a whole the apparatus is operable to interphase with other external devices other than "a host personal computer" or "a cellular computer".

Furthermore, it would be unfair on the Applicant if he was forced to recite each specific type of external device in claim 1. In particular, bearing in mind the requirements of Article 84 which requires the claims to be "clear and concise".

The requirements of Article 123(2) requires that the claimed features to be directly and unambiguously derivable from the application as originally filed. It is respectfully submitted that this requirement is clearly met and therefore the added matter objection of paragraph 1.1 has been rendered moot.

1.2 The Examiner also seems to have raised an added matter objection in paragraph 1.2 where it is stated "*Furthermore, the applicant did not provide, and the examining division could not identify in the application as filed, the support for the amendment of the last feature of claims 1 and 5, namely, "access ... is denied to said external device".*

The Applicant submits that the Examining Division have not provided a reasoned statement supporting the objection of paragraph 1.2 which is a substantial procedural violation.

The rejected feature is reproduced below:

> *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.*

It is respectfully submitted that the flow charts of Figures 4 and 5 clearly show that access to the stored personal data files is denied to the external device, see blocks 405 and 505. The external device retrieves the personal data in step 410 in figure 4. However, if the authentication process fails, the process flow terminates at block 405 thereby preventing the data retrieving step 410 from occurring. Thus, it is inherent from the sequence of steps in the flow charts that access to the stored personal data files in said first memory module is denied to said external device if the apparatus is shut off in stage 405 which blocks the apparatus from further use.

It is respectfully submitted that the added matter objections of paragraphs 1.1 and 1.2 have been rendered moot in view of the above comments and should be withdrawn.

Overview of the Invention

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 external devi ce**. This functional separation is a very important aspect of the present application. The Examining Division did not appear to grasp this concept.

In an effort to clarify that the sensitive information is stored on a separate device to the external device. claim 1 of the Main Request recites; 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.

Inventive Step

2. The Examiner indicated that the subject-matter of claims 1 and 5 of the main request (**excluding the features infringing Art.123(2) EPC**) does not involve an inventive step within the meaning of Article 56 EPC.

Firstly, the Applicant submits that all the features of Claims 1 and 5 are directly and unambiguously derivable from the Application as filed as outlined in section 1 above. Accordingly, it is submitted that the inventive step analysis is fundamentally flawed as certain features were incorrectly omitted.

2.2 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.*

2.3 The examiner indicated that features a) and b) represent a mere juxtaposition of features, not producing any working inter-relationship, and were therefore be analysed separately. The Applicant disagrees with the assessment that features a) and b) are a mere juxtaposition of features.

The present invention as described on page 21 lines 25-27 provides an apparatus combining and supporting highly secured data encryption, personal sensitive data storage, transfer, management and handling. It is respectfully submitted that this is achieved as a result of the working relationship between:

1) first memory module,
2) processing module, and
3) encryption module.

The working relationship between these features is clearly defined in the following step of claim 1:

*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;*

Paragraph 2.1 of the decision states "

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);

The Examining Division appear to have omitted the fact that the first memory module is in communication with both the processing module **and** the encryption module.

The Examining Division acknowledges in paragraph 2.2 that D1 fails to disclose:

a) an encryption module in communication with the processing module and the memory module

Claim 1 does not actually recite the wording as indicated by the examiner in 2.2 (a). Claim 1 uses the following wording " an encryption module in communication with the processing module".

It is respectfully submitted that since the Examiner acknowledges that D1 fails to teach an encryption module in communciaiton with the processing module and the memory module. Thus D1 must also fail to disclose the *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".*

It is submitted that there is an **extremely important difference** between an "*aggregation of features*" and a "*combination of features*". An "*aggregation of features*" does not have functional interdependency between features, while a "combination of features" does. According to Guidelines G/VII/7 an invention must normally be considered as a **whole**. When a claim consists of a "*combination of features*", **it is not correct to argue** that the separate features of the combination taken by themselves are known or obvious and that "therefore" the whole subject-matter claimed is obvious.

2.3.1 The Examiner indicated that *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.*

The Applicant submits that the examining division did not provide any evidence to support this statement. Accordingly, the inventive step objections are not not fully reasoned which is a substantial procedural violation.

2.3.2 The Examiner relies on D2 for teaching feature b). The Applicant 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.

2.4 The Examiner provides the following comments in an effort to support that D1 lacks an inventive step.

> *Considering the feature introduced with the amendment, to the extent that it is present in the application as originally filed, namely, that the apparatus is operable to interphase with a cellular phone or a host personal computer for activation of various operations between the cellular phone/host computer and the apparatus, at the time of filing the present application the techniques for transferring data between a cell phone and computer were well known. Therefore, in the context of document D1, this feature represents a mere juxtaposition of a known technique and cannot be considered as basis of an inventive step.*

The above passage appears to be relying on the content of the newly cited documents:

(i) XP055260933,
(ii) XP055260935,
(iii) W02006076658.

It is submitted that the Examining Division fails to use the problem-and –solution to show how these newly cited documents could be combined with D1 and D2. Thus the Decision does not provide a sufficiently reasoned argument as to why the invention lacks an inventive step in view of the newly cited prior art documents. An insufficiently reasoned Decision is a substantial procedural violation (Case Law of the Boards of Appeal, 7th Ed., E-IV 8.3.4).

3. The arguments provided with refenerce to claim 1 also apply to claim 5, and as a consequence the objection of paragraph 3 has been rendered moot.

4. The Examining Dvision relies on the combination of D1 and D2 without providing a reasoned statement why a person skilled in the art would be motivated to combine D1 and D1 using the problem and solution approach.

5. The Applicant diagrees that features a) and b) are a mere juxaposition of features. Furthermore, the Examining Division's analysis paraphases the claimed features to an arrangement which is not actually recited in claim 1. Thus, the inventive step analysis is not correct. The working relationship of the relevant features is clearly defined in claim 1. However, the examiner appears to have purposely paraphrased the following features in claim 1 in a crude attempt to break the working relationship:

> *i) 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;*
>
> *ii) a processing module in communication with said **plurality of biometric sensors, said first memory module and said authentication unit**;*
>
> *iii) an **encryption module** in communication with the **processing module:***
>
> *iii) 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 Applicant submits that claim 1 should be analysed as recited and not using a paraphased version of claim 1. The paraphased version of claim 1 which is used by the examiner in section 2.1 rewrites steps i) and iii) as listed above as follows:

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

In particular, in the claimed arrangement the first memory module is in communication with the processing module and the **encryption module** for the storage of said user's data and documentation files. In the paraphrased version of 2.1 of the Decision the underlined encryption module has been removed which also removes the function of the encryption module in relation to the first memory module *for the storage of said user's data and documentation files.*

It is submitted that its the three elements 1) ***first memory module*** *in communication with said 2)* ***processing module*** ***and*** *said 3)* ***encryption module*** *which fulfill the function of "for the storage of said user's data and documentation files".*

First Auxiliary Request

6 Claim 1 of the first auxiliary request corresponds to claim 1 of the main request with the addition of the feature: " *... while using a display and keyboard of the external device for user's interaction with the handheld apparatus*"

It is submitted that page 16 lines 5-8 of the description recites " *wherein the computer or cellular phone have a* ***keyboard*** *and* ***display units*** *associated therewith, thereby allowing the user to interact with the memory module and with the processing module of the apparatus via the* ***external devices keyboard*** *and* ***display units***"

A person skilled in the art would understand using normal daily english that the computer and cellular phone are described as being external devices. Accordingly, the "term external device" is directly and unambiguously derivable from the application as originally filed in accordance with Article 123(2). The Applicant respectfully submits that the Article 123(2) objections against the auxiliary request has been rendered moot for the same reasons as provided with respect to the main request.

7. The Applicant submits that claims 1 and 5 of the first auxiliary request is inventive step for the same reasons as provided above with reference to the main request.

8. The Applicant submits that claims 1 and 2 of the second auxiliary request meets the requirements of Article 123(2) and 56 EPC for the same reasons as provided with reference to the main request.

Second Auxiliary Request

While the Applicant maintains that the claims of the main request meets and first auxiliary requests meets the requirements of Aricle 123(2) and Article 82, in a further effort to advance prosecuction to grant 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.

Third Auxiliary Request

While the Applicant maintains that claims of the main request meets the requirements of Aricle 123(2), in a further effort to advance prosecuction to grant, the term "external device" has been replaced with the term "mobile communication device or a personal compute" in the third auxiliary request.

Furthermore, the Applicant submits that the claims of the Third auxiliary request meets the requirments of Article 56 EPC for the same reasons as outlined above with reference to the main request.

Fourth Auxiliary Request

While the Applicant maintains that claims of the main request meets the requirements of Aricle 123(2), in a further effort to advance prosecuction to grant, the term "external device" has been replaced with the term "mobile communication device" in the Fourth Auxilairy Request.

Furthermore, the Applicant submits that the claims of the fourth auxiliary request meets the requirments of Article 56 EPC for the same reasons as outlined above with reference to the main request.

Fifth Auxiliary Request

While the Applicant maintains that cthe laims of the second auxiliary request meets the requirements of Aricle 123(2) and Article 82, in a further effort to advance prosecuction to grant, the term "external device" has been replaced with the term "computer or cellular phone".

Furthermore, the Applicant submits that the claims 1 and 2 of the fifth auxiliary request meets the requirments of Article 56 EPC for the same reasons as outlined above with reference to the main request.

Sixth Auxiliary Request

While the Applicant maintains that the claims of the second auxiliary request meets the requirements of Aricle 123(2) and Article 82, in a further effort to advance prosecuction to grant, the term "external device" has been replaced with the term "mobile communciation device".

Furthermore, the Applicant submits that the claims of the sixth auxiliary request meets the requirments of Article 56 EPC for the same reasons as outlined above with reference to the main request.

Final Remarks

I hereby take the precaution of requesting oral proceedings in the event that the Board is minded to take any decision adverse to the Applicant. Any amendments made in these proceedings, and the observations contained in this letter, are made solely for the purposes of the prosecution of this European patent application and without prejudice to the applicant in other jurisdictions.

Yours faithfully



Paul Keane
Representative

Europäisches Patentamt
European Patent Office
Office européen des brevets

Letter accompanying subsequently filed items

Representative:

Mr Paul Keane
FRKELLY
27 Clyde Road
D04 F838 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	Claims (appeal procedure)	P105633EP00 Main Request Clean Sept26.pdf	DG3-CLMS.pdf
2	Amended claims with annotations (appeal procedure)	P105633EP00 Main Request Markup Sept26.pdf	DG3-CLMS-HWA.pdf
3	Claims (appeal procedure)	P105633EP00 Claims Clean 1st Aux Sept26.pdf	DG3-CLMS-1.pdf
4	Amended claims with annotations (appeal procedure)	P105633EP00 Claims Markup 2nd Auxiliary-Sept26.pdf	DG3-CLMS-HWA-1.pdf
5	Claims (appeal procedure)	P105633EP00 3rd Request Clean Sept26.pdf	DG3-CLMS-2.pdf
6	Amended claims with annotations (appeal procedure)	P105633EP00 3rd Request Markup Sept26.pdf	DG3-CLMS-HWA-2.pdf
7	Claims (appeal procedure)	P105633EP00 Fourth Request Clean Sept26.pdf	DG3-CLMS-3.pdf
8	Amended claims with annotations (appeal procedure)	P105633EP00 Fourth Request Markup Sept26.pdf	DG3-CLMS-HWA-3.pdf
9	Claims (appeal procedure)	P105633EP00 5th Auxiliary Clean Sept26.pdf	DG3-CLMS-4.pdf
10	Amended claims with annotations (appeal procedure)	P105633EP00 5th Auxiliary Markup Sept26.pdf	DG3-CLMS-HWA-4.pdf
11	Claims (appeal procedure)	P105633EP00 Claims 6th Auxi clean Sept26.pdf	DG3-CLMS-5.pdf
12	Amended claims with annotations (appeal procedure)	P105633EP00 Claims Markup 6th Auxiliary Sept26.pdf	DG3-CLMS-HWA-5.pdf
13	Statement of grounds of appeal	P105633EP00 Grounds of Appeal finalised Sept26.pdf	APPEAL-GRDS-1.pdf
14	Claims (appeal procedure)	P105633EP00 Claims Markup 2nd	DG3-CLMS-6.pdf

		clean Sept26.pdf	
15	Amended claims with annotations (appeal procedure)	P105633EP00 Claims Markup 1st Auxiliary-Sept26.pdf	DG3-CLMS-HWA-6.pdf

Signatures

Place:	
Date:	**26 September 2016**
Signed by:	**Paul Keane 36258**
Representative name:	**Paul Keane**
Capacity:	**(Representative)**

Fifth 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 a host personal computer or cellular phone for activation of various operations between the host personal computer or cellular phone and the handheld apparatus, while using a display and keyboard of the host personal computer or cellular phone 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 host personal computer or cellular phone, 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 and the operation of the portable handheld apparatus is completely shut down.

2. 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 a host personal computer or cellular phone for activation of various operations between the personal identification unit and said host personal computer or cellular phone, while using a display and keyboard of the host personal computer or cellular phone 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.

3. 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;

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 portable handheld apparatus as claimed in claim 1; wherein each of said portable handheld apparatus being associated with a unique user, each unique user being registered with said system manager.

4. The system of claim 3 further comprising a plurality of registered emergency centers and a plurality of registered service providers in communication with said system manager, to be accessed by said plurality of users; and

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.

Sixth 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 a mobile communication device for activation of various operations between the mobile communication device and the handheld apparatus, while using a display and keyboard of the mobile communication 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 mobile communication 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 mobile communication device and the operation of the portable handheld apparatus is completely shut down.

mobile communication device

2. 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 a mobile communication device for activation of various operations between the personal identification unit and said mobile communication device, while using a display and keyboard of the mobile communication 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.

.3. 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;

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 portable handheld apparatus as claimed in claim 1; wherein each of said portable handheld apparatus being associated with a unique user, each unique user being registered with said system manager.

4. The system of claim 3 further comprising a plurality of registered emergency centers and a plurality of registered service providers in communication with said system manager, to be accessed by said plurality of users; and

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.

Second 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. 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.

3. 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;

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 portable handheld apparatus as claimed in claim 1; wherein each of said portable handheld apparatus being associated with a unique user, each unique user being registered with said system manager.

4. The system of claim 3 further comprising a plurality of registered emergency centers and a plurality of registered service providers in communication with said system manager, to be accessed by said plurality of users; and

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.

Third 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 mobile communication device or a personal computer for activation of various operations between the mobile communication device or a personal computer and 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 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 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 mobile communication device or personal computer, 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 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 mobile communication device or personal computer 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 portable handheld 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 porable handheld 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 portable handheld 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 portable handheld apparatus, including the identification data of said user, the personal medical data file of said user, and location of said user; or wherein said portable handheld 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 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 portable handheld 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 personal identification unit being operable to interphase with a mobile communication device or a personal computer for activation of various operations between the personal identification unit and the handheld apparatus, 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 personal identification unit 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 mobile communication device or personal computer and the operation of the personal identification unit 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;