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 , 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.

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 external 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.

Fourth 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, 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, 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 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 mobile communication 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 mobile communication 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 mobile communication deviceand 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 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.

mobile communication device

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.

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.~~

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 ~~an external device~~ host personal computer or cellular phone for activation of various operations between the ~~external device~~ host personal computer or cellular phone and the handheld apparatus, while using a display and keyboard of the ~~external device~~ 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 ~~external device~~ 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 ~~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~~ host personal computer or cellular phone for activation of various operations between the personal identification unit and said ~~external device~~ host personal computer or cellular phone, while using a display and keyboard of the ~~external device~~ 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.

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 external 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.

78. 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.

89. The method of claim 78, 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~~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 ~~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.

Fourth 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 a mobile communication device for activation of various operations between the mobile communication 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~~mobile communication 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 mobile communication 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~~mobile communication 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 mobile communication 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~~mobile communication 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 mobile communication 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's~~apparatus'~~ 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~~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 ~~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~~mobile communication 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.

Sixth 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 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 ~~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~~mobile communication 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 mobile communication 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 devicemobile communication 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 a mobile communication device for activation of various operations between the personal identification unit and ~~the handheld apparatus~~ said ~~external device~~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 ~~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, e abling 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.~~

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 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.

~~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.

Third 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 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 ~~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~~mobile communication device or personal computer,

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 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 ~~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 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 ~~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 mobile communication device or personal computer 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's~~apparatus'~~ 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~~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 ~~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.

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	4670546
Application number	EP11752936.2
Date of receipt	26 September 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 (2 p.)	DG3-CLMS.pdf\P105633EP00 Main Request Clean Sept26.pdf (12 p.)
DG3-CLMS-HWA.pdf\P105633EP00 Main Request Markup Sept26.pdf (13 p.)	DG3-CLMS-1.pdf\P105633EP00 Claims Clean 1st Aux Sept26.pdf (9 p.)
DG3-CLMS-HWA-1.pdf\P105633EP00 Claims Markup 2nd Auxiliary-Sept26.pdf (13 p.)	DG3-CLMS-2.pdf\P105633EP00 3rd Request Clean Sept26.pdf (12 p.)
DG3-CLMS-HWA-2.pdf\P105633EP00 3rd Request Markup Sept26.pdf (13 p.)	DG3-CLMS-3.pdf\P105633EP00 Fourth Request Clean Sept26.pdf (12 p.)
DG3-CLMS-HWA-3.pdf\P105633EP00 Fourth Request Markup Sept26.pdf (13 p.)	DG3-CLMS-4.pdf\P105633EP00 5th Auxiliary Clean Sept26.pdf (4 p.)
DG3-CLMS-HWA-4.pdf\P105633EP00 5th Auxiliary Markup Sept26.pdf (4 p.)	DG3-CLMS-5.pdf\P105633EP00 Claims 6th Auxi clean Sept26.pdf (4 p.)
DG3-CLMS-HWA-5.pdf\P105633EP00 Claims Markup 6th Auxiliary Sept26.pdf (13 p.)	APPEAL-GRDS-1.pdf\P105633EP00 Grounds of Appeal finalised Sept26.pdf (14 p.)

	DG3-CLMS-6.pdf\P105633EP00 Claims Markup 2nd clean Sept26.pdf (4 p.)	DG3-CLMS-HWA-6.pdf\P105633EP00 Claims Markup 1st Auxiliary-Sept26.pdf (14 p.)
Submitted by	CN=Paul Keane 36258	
Method of submission	Online	
Date and time receipt generated	26 September 2016, 13:12 (CEST)	
Message Digest	A4:1F:A0:8B:67:B8:0D:04:E3:17:AB:5C:C0:96:D5:36:D1:8E:32:8A	

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

Acknowledgement of receipt

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

Submission number	4671931	
Application number	EP11752936.2	
Date of receipt	26 September 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
Submitted by	CN=Paul Keane 36258	
Method of submission	Online	
Date and time receipt generated	26 September 2016, 17:08 (CEST)	
Message Digest	E6:27:D6:D5:4F:0F:5A:65:11:4E:B0:05:97:86:09:D9:A5:85:94:22	

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

/European Patent Office/

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at **www.epo.org/contact**

Keane, Paul Fachtna
FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Date
11.10.16

Reference	Application No./Patent No.
P105633EP00	11752936.2 - 1955 / 2545485
Applicant/Proprietor	
OS - New Horizon Personal Computing Solutions Ltd.	

Communication of amended entries concerning the representative (R. 143(1)(h) EPC)

As requested, for the above-mentioned European patent application / European patent the entries concerning the representative have been amended as follows:

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

The amendment will be recorded in the Register of European Patents.

For the Examining Division

Europäisches Patentamt • European Patent Office • Office européen des brevets

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
80298 MUNICH
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Keane, Paul Fachtna
FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Datum/Date
13.10.16

Zeichen/Reference/Référence	Anmeldung Nr./Application No./Demande n°//Patent Nr./Patent No./Brevet n°
P105633EP00 APPR	11752936.2 / 2545485
Anmelder/Applicant/Demandeur//Patentinhaber/Proprietor/Titulaire	
OS - New Horizon Personal Computing Solutions Ltd.	

File number: **T2287/16-3.5.06**

Commencement of proceedings before the Board of Appeal

The letter dated 21.07.16 filed by the applicant
against the decision of the European Patent Office of 24.05.16
has been referred to Board of Appeal 3506.

The reference number is mentioned above.

Any further communications should be addressed to Directorate-General 3 of the European Patent Office and should quote this reference number.

The Registrar S. Sánchez Chiquero
Tel.: 089 / 2399 - 3561

Annex:
Registered letter

EPO Form 3204 01/11

European Patent Office
80298 MUNICH
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Appeal number: T2287/16-3.5.06

Order

1. In accordance with the business distribution scheme of the Technical Boards of Appeal, the following shall hear the above appeal:

   Chairman: (legally qualified member) W. Sekretaruk

   technically qualified member: M. Müller

   technically qualified member: G. Zucka

   In the case of an extended Board:

   technically qualified member: _____

   legally qualified member: _____

2. The rapporteur shall be: M. Müller

3. The additional rapporteur shall be: _____

4. Back to the Registry for further action.

Munich, 21.02.17

The Chairman W. Sekretaruk

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**

Keane, Paul Fachtna
FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Date
08.05.17

Reference	Application No./Patent No.
P105633EP00	11752936.2 - 1871 / 2545485
Applicant/Proprietor	
OS - New Horizon Personal Computing Solutions Ltd.	

Notice drawing attention to Rule 51(2) EPC, Article 2 No. 5 of the Rules relating to Fees,
- Payment of the renewal fee plus additional fee -

The renewal fee for the 07. year fell due on 31.03.17 unless this date falls within the period covered by an interruption of the proceedings in accordance with Rule 142(1) EPC, or a request for re-establishment of rights is pending (Art. 122, R. 51(4) EPC).

The current rate of the renewal fee amounts to **EUR 1165,00** (see current Schedule of fees and costs).

The renewal fee was not paid by the due date.
The renewal fee may still be validly paid **up to the last day of the sixth calendar month** following the due date, provided that the additional fee (**50%** of the renewal fee) is paid at the same time, see OJ EPO 2008, 5.

Within the above period, which cannot be extended, the following fees are to be paid:

Renewal fee for the 07. year:	EUR	1165,00
Additional fee:	EUR	582,50
TOTAL AMOUNT	EUR	1.747,50

If the renewal fee and the additional fee are not paid in due time, the European patent application shall be deemed to be withdrawn (Art. 86(1) EPC).

Note to users of the automatic debiting procedure
The normal time limit for payment of the above renewal fee had already expired when the automatic debit order was received. The renewal fee and the surcharge will be debited automatically on the last day of the six-month period (supplementary publication 3 - OJ EPO 2015).

Important information concerning fee amounts
Following any amendment to the Rules relating to Fees, the amount(s) mentioned in this communication may be different from the amount(s) **actually due on the date of payment.** The latest version of the Schedule of fees and expenses, published as a Supplement to the Official Journal of the EPO, is also available on the EPO website (**www.epo.org**) and can be found under **www.epo.org/schedule-of-fees**, which allows the viewing, downloading and searching for individual fee amounts, both current and previous.
Please note that procedural fees are usually adjusted every two years, on even years, with effect from 1 April.

Payments by cheque delivered or sent direct to the EPO are no longer accepted as from 1 April 2008 (see OJ EPO 2007, 626).

Important information in case of a PACE request
If, for an application being processed under the PACE programme the payment of the renewal fee has not been received by the due date stipulated in Rule 51(1) EPC, the accelerated prosecution of the application is suspended until the payment of the renewal fee with additional fee has been received (see OJ EPO 2015, A93, point 5).

For the Examining Division



FRKELLY
EUROPEAN PATENT AND TRADE MARK ATTORNEYS

European Patent Office
D-80298 München
Germany

FAO: Ms Claudia Weber, Client Data Services

Your Ref : 519
Our Ref : XMK1002IE00

By Fax
00498923994465

31 July 2017

Dear Sirs

Request to transfer all European Applications and Patents
FRKelly
Association No 519

We hereby request that all European Applications and Patents in the name of any professional representative at FRKelly are transferred to:

FRKelly
Association No 519
27 Clyde Road
Dublin D04 F838 / IE

This request relates to all European Applications and Patents before the EPO for which a professional representative at FRKelly has been authorised to act.

We request that the change takes immediate effect.

Please let us know if you have any queries or require anything further.

Yours faithfully

Donal M Kelly PhD
Professional Representative

d.kelly@frkelly.com
+353 1 231 4871

MARY B DARNE
DAVID BROPHY
PAUL DUFFY
EAMONN EDGECOMBE
FIONA GIBNEY
MARTIN HALL
PAUL KEANE
EDWARD KELLY
EVE MCCARTHY
MARIA MCCORMACK
RICHARD MILLS
PATRICIA NEENAN
SHANE SMYTH
ALAN WALLACE
STEPHEN WALSH

ALAN CASEY
ANNA HALLY
CATHERINE LAFFEY

DAVID LYNN
NEIL KELLY
SUSANNE KELLY
JANE MCMAHON
STEPHEN MURPHY
CIARA O'LAOGHAIRE
RICHARD O'REGAN
MICHAEL PURCELL
CAROLINE SHEEHAN
SUSAN KELLY

MARY CLANCY
OFFICES: DUBLIN & BELFAST

Duration: 31.07.2017 18:06:43 - 31.07.2017 18:06:50. This page 1 of 1 was completed at 31.07.2017 18:06:50
Received at the EPO on Jul 31, 2017 18:06:50. Page 1 of 1

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

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Date
04.08.17

Reference	Application No./Patent No.
P105633EP00	11752936.2 - 1871 / 2545485
Applicant/Proprietor	
OS - New Horizon Personal Computing Solutions Ltd.	

Communication of amended entries concerning the representative (R. 143(1)(h) EPC)

As requested, for the above-mentioned European patent application / European patent the entries concerning the representative have been amended as follows:

FRKelly
27 Clyde Road
Dublin D04 F838
IE

The amendment will be recorded in the Register of European Patents.

For the Examining Division



Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Appeal number: T2287/16-3.5.06

Order

Oral proceedings are to be held

on 09.10.18

at 09:00 hours

Room N° OP12

Munich 17.01.18

The Chairman W. Sekretaruk

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Appeal number: T2287/16-3.5.06

Communication of the Board of Appeal pursuant to Article 15(1) of the Rules of Procedure of the Boards of Appeal

The Rapporteur Martin Müller

This document: 13 page(s) including this page

Annex(es):

Communication text

A preliminary study of the present appeal has been carried out. The following observations are made without prejudice to the final decision of the board.

1. The appeal is against the decision of the examining division, dispatched with reasons dated 24 May 2016, to refuse European patent application No. 11 752 936.2 for added subject-matter (Article 123(2) EPC) and lack of inventive step (Article 56 EPC) over the documents

D1: US 2009/083847 A1 and
D2: US 5 229 764 A.

Further documents D3-D5 were cited in the decision but not relied upon in the reasons. In a section entitled "Further Remarks", the decision mentions three further documents (XP055260933, XP055260935 and WO2006076658)

"in support of" a statement made in the reasons, and raises an objection of non-unity *a posteriori* in view of the finding that the independent claims lacked inventive step. For ease of reference, the three documents are referred to hereinbelow as D6-D8, respectively.

2. The appellant requests that the decision be set aside, that a patent be granted on the basis of claims 1-13 according to a main request or auxiliary requests 3 and 4, claims 1-11 according to auxiliary request 1, or claims 1-4 according to auxiliary requests 2, 5 and 6, all as filed with the grounds of appeal, in combination with the description (pages 1-60) and the drawings (sheets 1-9) as published, and that the appeal fee be reimbursed because the decision was insufficiently reasoned and the appellant's right to be heard was violated.

The invention

3. The application relates to the fact that users need to have "easy, affordable, and immediate" access to personal data some of which is sensitive (such as medical records) and must hence be specially protected (page 1, paragraph 1).

3.1 The application discloses that, as a solution, security tokens are known to store and protect sensitive data (see page 1, paragraph 2). Some such tokens are discussed in detail, esp. the "Medicard", which require biometric authentication before providing access to the stored data (see page 3, last paragraph, to page 4, paragraph 1). Known tokens are said to have a number of shortcomings such as lacking "connectivity" and liveness detection (see the paragraph bridging pages 4 and 5).

3.2 The invention proposes a particular such security token (see page 9, paragraph 2, and figures 3a and 3b). It provides encryption so that the sensitive data need not be stored in plain text. It provides different biometric, liveness and affect sensors, so that access to the data can be limited to authorized users and, possibly, dependent on their emotional or physiological state (see e.g. page 14, last paragraph, to page 15, paragraph 2; page 26, paragraph 2, to page 28, paragraph 2; page 37, paragraph 2). It may act as a "mass memory" of private data for its owner (page 12, paragraph 1; page 13, lines 9-12 and 26-32; pages 33 and 39, paragraph 3) and may, insofar, replace other portable devices (see page 14, paragraph 2). It may also offer further functionality such as initiating an emergency call, e.g. through a connected cell phone, and communicating the device location (page 12, paragraph 2; page 15, last paragraph; page 24, paragraph 3; page 28, last paragraph, to page 29, paragraph 2; page 34, paragraph 2).

3.3 The envisaged typical use scenario is depicted in figure 1 (see page 23, penultimate paragraph, to page 24, paragraph 1). The token may be attached to one of several "external" devices, such as a smartphone (355), and landline phone (365), a computer terminal (360) or multi-user I/O terminals (362), each of which is connected to some service network, be it a landline or cellular telephone communication network (305, 310) or the Internet (370). When the token is attached to an external device and held by an authorized user, the external device can retrieve data from the token's memory or write into it (see page 41, lines 16-19).

3.4 It is also disclosed that biometric data can be obtained and verified "continuously" and that, if this fails, further access to the personal data may be

denied and the token may "completely" shut down (see original claim 2).

Article 11 RPBA, Rule 103(1)(a) EPC, alleged substantial procedural violations

4. The appellant requests that the appeal fee be reimbursed because two substantial procedural violations occurred in examination.

4.1 It argues that its right to be heard under Article 113(1) EPC was violated because it could not comment on documents D6-D8, which were mentioned first in the reasoned decision (see the grounds of appeal, page 3, paragraph 2; page 4, paragraphs 1-2).

4.2 And it takes the view that the decision was insufficiently reasoned (Rule 111(2) EPC), because

- the examining division justified an Article 123(2) EPC objection to a feature merely with the statement that "the applicant did not provide, and the examining division could not identify in the application as filed", disclosure of that feature (see page 6, last paragraph, to page 7, paragraph 1),
- it did not provide evidence for its statement that "the use of encryption for data protection is a well known technique" (see the grounds of appeal, page 8, point 2.3.1), and
- it did not use, as would have been required, the problem-solution-approach to show why the skilled person would have combined D1 and D2 (see page 10, point 4) or these two with any of D6-D8 (see page 10, point 2.4).

5. As regards the alleged violation of the appellant's right to be heard, the board's preliminary opinion is as follows.

5.1 The board follows the appellant insofar as the mention of new documents only with the reasoned decision may cause avoidable misunderstandings.

5.2 That said, the board notes that point 2.4 of the reasons, to which documents D6-D8 refer, relates to a feature which the examining division considered to contravene Article 123(2) (see reasons 1.1). Ignoring this feature, the examining division came to its conclusion that claim 1 lacked inventive step with point 2.3 of the reasons.

5.3 The board has no objection against ignoring a feature from the inventive-step assessment that was found to contravene Article 123(2) EPC. More specifically, the board considers that the examining division is not obliged to anticipate the replacement of such a feature with a similar one that might be originally disclosed and provide a speculative inventive step assessment of a so-amended claim.

5.4 The board thus tends to consider that point 2.4 of the reasons is - and is easily recognisable as being - an *obiter dictum* itself and not to form part of the reasons for the inventive-step objection. It would seem to follow that potential deficiencies as indicated by the appellant cannot be fundamental ones within the meaning of Article 11 RPBA or substantial procedural violations according to Rule 103(1)(a) EPC.

5.5 The board further notes that the argument put forward in point 2.4 of the reasons was already given in the communication of 30 March 2016 (point 2.1) without reference to any written evidence. The appellant not

having responded to this communication, the examining division was entitled to maintain its opinion without having to produce evidence for it. And that the examining division has maintained its opinion seems to follow from the fact that the newly cited documents were introduced in a section clearly separate from the reasons for the decision.

5.6 Finally, the board notes that while the appellant stresses that it should have been given an opportunity to study D6-D8, it does not, in its grounds of appeal, contradict the substantive assumption about the common knowledge in the art which D6-D8 were cited to support (reasons 2.4 and remarks 1). Even from the grounds of appeal, thus, it would seem that this assumption *per se* is uncontroversial.

6. With regard to the allegedly insufficient reasoning, the board takes the following view.

6.1 The board tends to consider that an Article 123(2) EPC objection may well be sufficiently reasoned by saying that the appellant did not provide any basis for an amendment and noting that such basis was not apparent to the examining division by itself.

6.2 In the present case, the board also notes that the examining division had already raised that point in its communication dated 30 March 2016 (point 1.2), to which the appellant chose not to respond.

7. In view of the foregoing, the board cannot presently see any fundamental deficiency in the first instance proceedings that would require an immediate remittal of this case to the first instance under Article 11 RPBA or that could make reimbursement of the appeal fee equitable under Rule 103(1)(a) EPC.

Clarity and claim construction

8. The board notes that the term "interphase" does not seem to exist in the art and takes it that "interface" is meant instead.

9. The independent claims of all requests specify that the claimed "apparatus [is] operable to [interface] with an external device for various operations" without specifying the kind of operations or whether or how they interact with the security mechanism specified in the remainder of the claims.

10. The independent claims state that "access to the stored data files in said first memory module is denied to said external device and the operation of the portable handheld apparatus is completely shut down". This phrase is ambiguous between saying that access is denied "by way of" shutting down the device or access is denied independently of the shutdown.

11. The independent claims specify that "access [...] is only enabled" after successful authentication of the user. The board notes that his phrase seems to refer to any access, not just access by the external device.

12. The independent claims specify continuous biometric authentication and the detection of a "change" in the biometric parameters. Illustrating the notion of change, the appellant refers to a device that detects a change in the user's heart rate, takes this to indicate that the user is under duress and shuts down the device to protect the data (see page 10, paragraph 2). The board notes that the claim wording is much broader than that: Specifically, if the apparatus was handed over to a different user after the first authentication, a

"change" in the measured biometric parameters would also be detected.

Added subject-matter, Article 123(2) EPC

13. The examining division found that an interface with an external device was more general than what was disclosed in the description, which referred only to interfacing with a cellular phone or a host personal computer" (reasons 1.1). The board rather tends to agree with the appellant that the description discloses (esp. in figure 1 and the accompanying description) that "external devices" as disclosed could also be "landline phones" or "multi-user I/O terminals" and that a general reference to "external devices" in the claims complies with Article 123(2) EPC.

14. As regards the denial of access "to said external devices" (reasons 1.2), the board agrees with the decision that no action seems to be disclosed that would be specific for the external device, i.e. beyond the evident fact that shutting down the apparatus has the effect of "denying" any access whatsoever. To the extent that the phrase "access [...] is denied to said external device" suggests the contrary, it seems to contravene Article 123(2) EPC. The appellant's arguments in this respect do not address this point (see grounds of appeal, page 7, upper half).

Non-unity

15. In the section "Further Remarks" the examining division raised a non-unity objection to the dependent claims on the basis of (i.e. *posterior* to) the finding that the independent claims lacked inventive step. This means that the non-unity objection would fall if the inventive-step objection were to fall, and that the non-unity objection would be immaterial for the

allowability of the claimed invention if the inventive-step objection were to stand. In the following, therefore, no further reference will be made to this objection. Moreover, the deletion of dependent claims from auxiliary requests 1, 5 and 6 (vis-à-vis the main request and auxiliary request 3 and 4) appears not to address any issue presently at stake.

The prior art

16. D1 discloses an electronic device, preferably a mobile phone (see figures 6 and 7), with several biometric and liveness sensors for controlling access to its data (see paragraph 25, 28, 41, 57, 75 and 76).

17. D2 discloses a protected system that requires continuous biometric authentication for a user to get and keep access to the system (see column 2, lines 41-66, and column 3, lines 21-26). It also discloses that the system may shut down when the user "fails more than a prescribed number of [biometric] comparison tests" (see column 5, lines 4-6), possibly after having performed an additional, "more highly accurate test" (column 7, lines 24-28).

Inventive step

18. In a nutshell, the invention is a mobile data storage for sensitive data which can be attached to all kinds of "external devices" to provide these external devices with access to the sensitive data. Access is controlled by biometric and liveness sensors and further protected by encryption. The central idea is that the mobile device's primary function is to keep data storage separate from the applications running on the external devices (see the grounds of appeal, page 7, paragraph 4 from the bottom).

18.1 D1 discloses a smartphone storing sensitive data access to which is controlled by biometric and liveness sensors, i.e. providing the claimed data storage functionality and the biometric access protection. The data access being controlled appears to be mainly "local", i.e. relating to a user manipulating the smartphone, and not to involve any "external device". However, it would seem to be commonly known that smartphone data can be accessed from an "external device", via its display and keyboard, for example in order to backup the smartphone memory or to transfer pictures to a PC. It is known in this context that the data on the phone can only be accessed from the PC when the user has logged in at the phone. The board considers that this statement does not require documentary evidence but is prepared to provide such evidence if the appellant were to challenge it in substance. For the moment it seems sufficient to point out that the first iPhone was launched in 2007.

18.2 It would therefore appear to be common practice in the art - and thus obvious in the context of D1 - that all access control mechanisms provided on the phone also control access to the data from external devices.

18.3 In view of the foregoing, the board tends to agree with the assessment in the decision under appeal (see reasons 2.2), that the claimed invention differs from D1 by

a) an encryption module for the storage of user's data,
b) continuous biometric (re-)authentication, and
c) shutdown of the apparatus should biometric re-authentication fail.

18.4 The appellant stresses that the "working relationship" between the "processing module", the "memory module", the "encryption module" and the biometric sensors is

very specific and provides a link between the above differences (see the grounds of appeal, page 11, point 5). On this account the board notes that it is obvious that the "processing module" be "in communication" with all the other components. The board tends not to accept that any further interaction between the difference features can be derived from the claimed subject-matter.

18.5 As regards feature a), the board tends to agree with the decision under appeal(reasons 2.3.1) that "the use of encryption for data protection" in computer memory is well-known in the art. Although the appellant has pointed out that the examining division did not provide any evidence for this statement, it seems not to have challenged it in substance (grounds of appeal, point 2.3.1).

18.6 As regards features b) and c), the board notes that there is no clear difference between "repeated" and "continuous" re-authentication, and recalls (see point 12 above) that the notion of "change" is very vague and subsumes the situation that biometric data has changed because the apparatus was handed to a different user. From this perspective, the board tends to agree that D2 provides a solution to the problem given by the examining division, namely to avoid an unauthorized change of users (see reasons 2.3.2). In response to the appellant's remark under point 4 in its grounds of appeal, the board takes the view that it would have been sufficient prompt for the skilled person to combine D1 with D2 that D2 solves a problem that would arise in the context of D1.

18.7 The board therefore comes to the preliminary conclusion that none of features a) to c) establishes an inventive step of the claimed invention over D1, Article 56 EPC.

Auxiliary requests

19. The auxiliary requests differ from the main request in referring to the external device's display or keyboard (auxiliary request 1), in limiting the "external device" to, respectively, "a mobile communication device or a personal computer" or simply "a mobile communication device" (auxiliary requests 3, 4, 5, 6), and in the deletion of dependent claims (auxiliary requests 2, 5 and 6).

19.1 As already stated (see point 15 above), the deletion of dependent claims is immaterial to the deficiencies of the independent claims. Also, the assessment of the main request has assumed the external device to be a personal computer. Therefore, the assessment of the main request seems to apply directly to auxiliary requests 1-3 and 5.

19.2 The fact that the independent claims in auxiliary requests 4 and 6 are limited to external access to the claimed apparatus by a "mobile communication device" does not seem to have any impact on the claimed apparatus itself. And even if it had, it would seem to the board that it was an obvious trend in the art that "mobile communication devices" could carry out more and more functions which used to be limited to desktop computers. Either way, the board tends to consider that this difference cannot render the claimed invention non-obvious either.

20. In summary, the subject-matter of the independent claims of all requests being obvious over D1, D2 and common knowledge, it would seem that the appeal will have to be dismissed.

The appellant's attention is, in particular, drawn to Articles 13(1) and 15(3) RPBA. Any amendments to its case

should be submitted at the latest one month before the appointed date.

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Date
22.01.18

Zeichen/Reference/Référence	Anmeldung Nr./Application No./Demande n°//Patent Nr./Patent No./Brevet n°
P105633EP00 APPR	11752936.2 / 2545485
Anmelder/Applicant/Demandeur//Patentinhaber/Proprietor/Titulaire	
OS - New Horizon Personal Computing Solutions Ltd.	

Appeal number: **T2287/16-3.5.06**

Summons to oral proceedings pursuant to Rule 115(1) EPC

You are hereby summoned to the oral proceedings concerning the above appeal.
The proceedings are scheduled to take place

on 09.10.18 at 09:00 hrs in Room OP12

Richard-Reitzner-Allee 8, 85540 Haar (DE)

The proceedings will be public.

A main waiting area is located at the entrance, directly after the security check. Further waiting rooms are located near to the oral proceedings rooms.

You are requested to attend outside the appointed room **10 minutes** before the hearing.

Registered letter with advice of delivery

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Appeal number: **T2287/16-3.5.06**

You are reminded that

- if a party who has been duly summoned to oral proceedings does not appear, the proceedings may continue without that party (Rule 115(2) EPC).
- oral proceedings will only be postponed at the request of a party for serious reasons (see Notice in Special edition No. 3 OJ EPO 2007, 115).
- as regards filing authorisations for representatives or company employees, see Decision of the President of the EPO dated 12.7.2007 on the filing of authorisations in Special edition No. 3 OJ EPO 2007, 128.
- concerning the language of the proceedings, attention is drawn to Rule 4 EPC. Notice given pursuant to Rule 4(1) EPC before the first instance is not valid in proceedings before the Boards of Appeal.
- According to Rule 103(2) EPC it is possible to obtain a 50% reimbursement of the appeal fee if the appeal is withdrawn under certain circumstances (OJ EPO 2014, A3).

Composition of the Board

Chairman: W. Sekretaruk

Member: Martin Müller

Member: G. Zucka

For all urgent communications in connection with the oral proceedings please use only EPO Online Services (preferably) or fax No. + 49 (0) 89 2399 3014.

If you are planning not to attend the oral proceedings or if you are aware of any matter that could have a bearing on the appointment of interpreters, you are requested to inform the Board of this, preferably in writing, at the earliest possible opportunity.

The Registrar B. Atienza Vivancos

Tel.: 089 / 2399 - 3561

Annex(es): ☑ Confirmation of receipt Form 3936

☑ Communication pursuant to Article 15(1) of the Rules of Procedure of the Boards of Appeal

☐

Registered letter with advice of delivery

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Boards of Appeal

The Registry
Name: B. Atienza Vivancos
Tel.: 089 / 2399 - 3561

Date: 22.01.18

Zeichen/Reference/Référence	Anmeldung Nr./Application No./Demande n°//Patent Nr./Patent No./Brevet n°
P105633EP00 APPR	11752936.2 / 2545485
Anmelder/Applicant/Demandeur//Patentinhaber/Proprietor/Titulaire	
OS - New Horizon Personal Computing Solutions Ltd.	

Appeal number: T2287/16-3.5.06

EPA/EPO/OEB Formblatt/Form/Formulaire: 3011.1 - 3350

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)

Beschwerdekammern des
Europäischen Patentamts
Richard-Reitzner-Allee 8
85540 HAAR
DEUTSCHLAND

Rücksende-Adresse / Return address / Adresse de retour

EPA Form 3936 08/17

Sendungsnummer / No de l'envoi / Item number

Art der Sendung / Nature de l'envoi / Type

☐ Brief / Lettre / Letter - Einschreiben / Recommandé / Registered

☐ Paket / Colis / Parcel (nur Vertragskunden)

RH 22 01 18 IE

Bitte diesen Aufkleber auf der Vorderseite der Sendung anbringen.

11752936.2

FRKelly
de Road
Dublin Du4 F838
IRLANDE

T2287/16-3506
F.3011.1

RH22 677 889 2DE

Am Bestimmungsort auszufüllen /
A remplir par le bureau de destination /
To completed by office of destination

O.g. Sendung wurde ordnungsgemäß ausgeliefert
L'envoi mentionné ci-dessus a été dûment livré /
The article mentioned above was duly delivered

Datum und Unterschrift* / Date et signature* / date and signature*

2.2.18 FRKelly dest

* Dieser Rückschein kann vom Empfänger oder wenn die Vorschriften des Bestimmungslandes dies vorsehen, von einem Beauftragten oder Mitarbeiter des Postunternehmens im Bestimmungsland unterschrieben werden.

* Cet avis pourra être signé par le destinataire ou, si les règlements du pays de destination le prévoient, par une autre personne autorisée ou par l'agent du bureau de destination.

* This receipt must be signed by the adressee or a person authorized to sign under the regulations of the country of destination or if those regulations so provide, by the employee of the office of destination.

Name in Großbuchstaben (oder andere eindeutige Identifikation)
Nom du destinataire en lettres majuscules (ou autre moyen clair d'identification)
Name of recipient in capital letters (or other clear identification)

CN 07 | UPU - RL 141

Deutsche Post AG
Entreprise des Postes allemandes S.A.

RÜCKSCHEIN / Avis de réception / Advice of delivery

Postsache
Service des Postes
Postal service



PRIORITAIRE
By Airmail
Par avion

Stempel der Post, die den Schein zurücksendet.
Timbre di bureau renvoyant l'avis.
Postmark of the office returning the receipt.

Zurücksenden an / Renvoyer à / return to

Europäisches Patentamt
80298 MÜNCHEN
DEUTSCHLAND / ALLEMAGNE / GERMANY

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49(0)89 2399-4465

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Fax No. +353 1 614 4756
No. of pages: 2

ONLY by FACSIMILE on | Datum/Date 22.02.18

Zeichen/Reference/Référence		Anmeldung Nr./Application No./Demande n°//Patent Nr./Patent No./Brevet n°
P105633EP00	APPR	11752936.2 / 2545485
Anmelder/Applicant/Demandeur//Patentinhaber/Proprietor/Titulaire		
OS - New Horizon Personal Computing Solutions Ltd.		

Appeal number: **T2287/16-3.5.06**

Missing advice of delivery

Subject: Decision of
Summons to oral proceedings dated 22.01.18
Communication of

No advice of delivery has been received. Please acknowledge the receipt of the above-mentioned document with mention of the date of receipt

- **through EPO Online Services (as annex to EPO Form 1038)**
- by Fax (+49 (0) 89 2399-4465)
- or by post.

The Registrar B. Atienza Vivancos
Tel.: 089 / 2399 - 3561

Beschwerdekammern des Europäischen Patentamts · Boards of Appeal of the European Patent Office · Chambres de recours de l'Office européen des brevets

EPO Form 3937 01/11

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Boards of Appeal

The Registry

Name: B. Atienza Vivancos

Tel.: 089 / 2399 - 3561

Date: 22.01.18

Zeichen/Reference/Référence	Anmeldung Nr./Application No./Demande n°//Patent Nr./Patent No./Brevet n°
P105633EP00 APPR	11752936.2 / 2545485
Anmelder/Applicant/Demandeur//Patentinhaber/Proprietor/Titulaire	
OS - New Horizon Personal Computing Solutions Ltd.	

Appeal number: T2287/16-3.5.06

EPA/EPO/OEB Formblatt/Form/Formulaire: 3011.1 - 3350

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)

Beschwerdekammern des
Europäischen Patentamts
Richard-Reitzner-Allee 8
85540 HAAR
DEUTSCHLAND

Rücksende-Adresse / Return address / Adresse de retour

EPA Form 3936 08/17

SENDEBERICHT

ZEIT : 22/02/2018 11:14
NAME : EPO BOARDS OF APPEAL
FAX : 00498923993014
TEL :
S-NR. : E71294H6J323661

DATUM/UHRZEIT	22/02 11:13
FAX-NR./NAME	00035316144756
Ü.-DAUER	00:01:00
SEITE(N)	02
ÜBERTR	OK
MODUS	STANDARD ECM

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Fax No. +353 1 614 4756
No. of pages: 2

ONLY by FACSIMILE on | Datum/Date 22.02.18

Zeichen/Reference/Référence		Anmeldung Nr./Application No./Demande n°//Patent Nr./Patent No./Brevet n°
P105633EP00	APPR	11752936.2 / 2545485
Anmelder/Applicant/Demandeur//Patentinhaber/Proprietor/Titulaire		
OS - New Horizon Personal Computing Solutions Ltd.		

Appeal number: **T2287/16-3.5.06**

Missing advice of delivery

Subject: Decision of

Summons to oral proceedings dated 22.01.18

Communication of

No advice of delivery has been received. Please acknowledge the receipt of the above-mentioned document with mention of the date of receipt

- **through EPO Online Services (as annex to EPO Form 1038)**
- by Fax (+49 (0) 89 2399-4465)

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Fax No. +353 1 614 4756
No. of pages: 2

Reminder 08.03.18

ONLY by FACSIMILE on | Datum/Date 22.02.18

Zeichen/Reference/Référence		Anmeldung Nr./Application No./Demande n°//Patent Nr./Patent No./Brevet n°
P105633EP00	APPR	11752936.2 / 2545485
Anmelder/Applicant/Demandeur//Patentinhaber/Proprietor/Titulaire		
OS - New Horizon Personal Computing Solutions Ltd.		

Appeal number: **T2287/16-3.5.06**

Missing advice of delivery

Subject: Decision of
Summons to oral proceedings dated 22.01.18
Communication of

No advice of delivery has been received. Please acknowledge the receipt of the above-mentioned document with mention of the date of receipt

- **through EPO Online Services (as annex to EPO Form 1038)**
- by Fax (+49 (0) 89 2399-4465)
- or by post.

The Registrar B. Atienza Vivancos
Tel.: 089 / 2399 - 3561

Beschwerdekammern Boards of Appeal Chambres de recours

EPO Form 3937 01/11

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Boards of Appeal

The Registry

Name: B. Atienza Vivancos

Tel.: 089 / 2399 - 3561

Date: 22.01.18

Zeichen/Reference/Référence		Anmeldung Nr./Application No./Demande n°//Patent Nr./Patent No./Brevet n°
P105633EP00	APPR	11752936.2 / 2545485
Anmelder/Applicant/Demandeur//Patentinhaber/Proprietor/Titulaire		
OS - New Horizon Personal Computing Solutions Ltd.		

Appeal number: T2287/16-3.5.06

EPA/EPO/OEB Formblatt/Form/Formulaire: 3011.1 - 3350

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)

Bescheinigung des
Europäischen Patentamts
Richard-Reitzner-Allee 8
85540 HAAR
DEUTSCHLAND

Rücksende-Adresse / Return address / Adresse de retour

EPA Form 3936 08/17

SENDEBERICHT

ZEIT : 08/03/2018 08:44
NAME : EPO BOARDS OF APPEAL
FAX : 00498923993014
TEL :
S-NR. : E71294H6J323661

DATUM/UHRZEIT	08/03 08:43
FAX-NR./NAME	00035316144756
Ü.-DAUER	00:01:00
SEITE(N)	02
ÜBERTR	OK
MODUS	STANDARD ECM

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Fax No. +353 1 614 4756
No. of pages: 2

Reminder 08.03.18

ONLY by FACSIMILE on | Datum/Date 22.02.18

Zeichen/Reference/Référence	Anmeldung Nr./Application No./Demande n°//Patent Nr./Patent No./Brevet n°
P105633EP00 APPR	11752936.2 / 2545485
Anmelder/Applicant/Demandeur//Patentinhaber/Proprietor/Titulaire	
OS - New Horizon Personal Computing Solutions Ltd.	

Appeal number: **T2287/16-3.5.06**

Missing advice of delivery

Subject: Decision of
Summons to oral proceedings dated 22.01.18
Communication of

No advice of delivery has been received. Please acknowledge the receipt of the above-mentioned document with mention of the date of receipt

- **through EPO Online Services (as annex to EPO Form 1038)**
- by Fax (+49 (0) 89 2399-4465)

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Fax No. +353 1 614 4756
No. of pages: 2

Reminder 03.04.18

Reminder 08.03.18

ONLY by FACSIMILE on | Datum/Date 22.02.18

Zeichen/Reference/Référence	Anmeldung Nr./Application No./Demande n°//Patent Nr./Patent No./Brevet n°
P105633EP00 APPR	11752936.2 / 2545485
Anmelder/Applicant/Demandeur//Patentinhaber/Proprietor/Titulaire	
OS - New Horizon Personal Computing Solutions Ltd.	

Appeal number: **T2287/16-3.5.06**

Missing advice of delivery

Subject: Decision of
Summons to oral proceedings dated 22.01.18
Communication of

No advice of delivery has been received. Please acknowledge the receipt of the above-mentioned document with mention of the date of receipt

- **through EPO Online Services (as annex to EPO Form 1038)**
- by Fax (+49 (0) 89 2399-4465)
- or by post.

The Registrar B. Atienza Vivancos
Tel.: 089 / 2399 - 3561

Beschwerdekammern des Europäischen Patentamts
Boards of Appeal of the European Patent Office
Chambres de recours de l'Office européen des brevets

EPO Form 3937 01/11

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Boards of Appeal

The Registry

Name: B. Atienza Vivancos

Tel.: 089 / 2399 - 3561

Date: 22.01.18

Zeichen/Reference/Référence	Anmeldung Nr./Application No./Demande n°//Patent Nr./Patent No./Brevet n°
P105633EP00 APPR	11752936.2 / 2545485
Anmelder/Applicant/Demandeur//Patentinhaber/Proprietor/Titulaire	
OS - New Horizon Personal Computing Solutions Ltd.	

Appeal number: T2287/16-3.5.06

EPA/EPO/OEB Formblatt/Form/Formulaire: 3011.1 - 3350

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)

Beschwerdekammern des
Europäischen Patentamts
Richard-Reitzner-Allee 8
85540 HAAR
DEUTSCHLAND

Rücksende-Adresse / Return address / Adresse de retour

EPA Form 3936 08/17

SENDEBERICHT

ZEIT : 03/04/2018 16:00
NAME : EPO BOARDS OF APPEAL
FAX : 00498923993014
TEL :
S-NR. : E71294H6J323661

DATUM/UHRZEIT	03/04 15:59
FAX-NR./NAME	00035316144756
Ü.-DAUER	00:00:59
SEITE(N)	02
ÜBERTR	OK
MODUS	STANDARD ECM

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Fax No. +353 1 614 4756
No. of pages: 2

Reminder 03.04.18

Reminder 08.03.18

ONLY by FACSIMILE on Datum/Date 22.02.18

Zeichen/Reference/Référence	Anmeldung Nr./Application No./Demande n°//Patent Nr./Patent No./Brevet n°
P105633EP00 APPR	11752936.2 / 2545485
Anmelder/Applicant/Demandeur//Patentinhaber/Proprietor/Titulaire	
OS - New Horizon Personal Computing Solutions Ltd.	

Appeal number: T2287/16-3.5.06

Missing advice of delivery

Subject: Decision of
Summons to oral proceedings dated 22.01.18
Communication of

No advice of delivery has been received. Please acknowledge the receipt of the above-mentioned document with mention of the date of receipt

- **through EPO Online Services (as annex to EPO Form 1038)**
- by Fax (+49 (0) 89 2399-4465)

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Boards of Appeal

The Registry

Name: B. Atienza Vivancos
Tel.: 089 / 2399 - 3561

Date: 22.01.18

Zeichen/Reference/Référence	Anmeldung Nr./Application No./Demande n°//Patent Nr./Patent No./Brevet n°
P105633EP00 APPR	11752936.2 / 2545485
Anmelder/Applicant/Demandeur//Patentinhaber/Proprietor/Titulaire	
OS - New Horizon Personal Computing Solutions Ltd.	

Appeal number: T2287/16-3.5.06

EPA/EPO/OEB Formblatt/Form/Formulaire: 3011.1 - 3350

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:

2/2/18

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)

Bschwerdekammern des
Europäischen Patentamts
Richard-Reitzner-Allee 8
85540 HAAR
DEUTSCHLAND

Rücksende-Adresse / Return address / Adresse de retour

Received at the EPO on Apr 06, 2018 12:15:47. Page 2 of 2
Duration: 04.06.2018 12:14:49 PM - 04.06.2018 12:15:47 PM. This page 2 of 2 was completed at 04.06.2018 12:15:47 PM

FRKELLY
EUROPEAN PATENT AND TRADE MARK ATTORNEYS

European Patent Office
D-80298 Munich
Germany

Your Ref : 11752936.2
Our Ref : P105633EP00

2 October 2018

Dear Sirs,

European Patent Application No. 11752936.2
"A Secured Personal Data Handling and Management System"
OS - NEW HORIZON PERSONAL COMPUTING SOLUTIONS LTD.
Appeal No. T2287/16-3.5.06

As a matter of courtesy, I wish to advise the Board of Appeal that I will not be attending the Oral Hearing scheduled for October 9 2018 in connection with the above-identified Application.

I request that the Oral Hearing proceeds in our absence.

Yours faithfully

Paul Keane
Representative

p.keane@frkelly.com
+353 1 231 4862

MARY BLEAHENE
DAVID BROPHY
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
DAVID FLYNN
PAUL KELLY
SUSAN C. KELLY
LUKE MAISHMAN
ROISIN MCNALLY
STEPHEN MURPHY
JOHN O'FLAHERTY
RICHARD RANKIN
MICHAEL SCANNELL
CAROLINE SHEERAN
SHAUNA TILLEY
BEN TOLLEY

CONSULTANT:
PHILIP COYLE

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

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
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 during the appeal procedure	P105633EP00 Letter.pdf	APPEAL-ORAL.pdf

	Payment	
1	Method of payment	Not specified

Signatures

Place:	
Date:	**02 October 2018**
Signed by:	**Paul Keane 36258**
Representative name:	**Paul Keane**
Capacity:	**(Representative)**

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	6771423	
Application number	EP11752936.2	
Date of receipt	02 October 2018	
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 APPEAL-ORAL.pdf\P105633EP00 Letter.pdf (1 p.)
Submitted by	CN=Paul Keane 36258	
Method of submission	Online	
Date and time receipt generated	02 October 2018, 18:34 (CEST)	
Message Digest	3C:8E:41:FC:6B:56:AE:46:62:6F:6A:89:79:EC:D5:DA:8C:F7:0A:F5	

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/

FRKELLY
EUROPEAN PATENT AND TRADE MARK ATTORNEYS

European Patent Office
D-80298 Munich
Germany

Your Ref : 11752936.2
Our Ref : P105633EP00

2 October 2018

Dear Sirs,

European Patent Application No. 11752936.2
"A Secured Personal Data Handling and Management System"
OS - NEW HORIZON PERSONAL COMPUTING SOLUTIONS LTD.
Appeal No. T2287/16-3.5.06

I wish to withdraw the request for oral proceedings as I will not be attending due to financial costs that would be incurred by the Applicant if I was to attend.

While I will not be attending the oral hearing, I wish to convey to the Board of Appeal that it is my genuine belief that the present application was unfairly prejudiced against as a result of the Unity Objection which was raised in the Search Opinion dated February 5 2014. The Search Opinion indicated that the claims related to nine separate inventions. As a consequence, a significant about of claims/subject matter had to be deleted in order to overcome the unity objection which was detrimental to the prospect of present application proceeding to grant during examination.

I wish to convey to the Board of Appeal that I strongly disagree that the application did not comply with Unity of Invention requirements (Rule 44 EPC, Art 82 EPC)).

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

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

REFERENCE TABLE [ADDED MATTER? Rejection]

	Description, Page refs	Figs.	Fig. Ref No
Biometric	26, line 19- 28, line 20	2	124; 126
	40, lines 7- 23	4	403
	45, lines 15-23	5	503
Plurality of biometric sensors being integrated within the apparatus	30, lines 23-24; 34, lines 18-20; 36, lines 16-17; 39, lines 13-14		

MARY BLEAHENE
DAVID BROPHY
GAVAN FERGUSON
CAROL GORMLEY
[illegible]
PAUL KEANE
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]

[illegible]
[illegible]
PAUL KELLY
SUSAN C. KELLY
[illegible]
[illegible]
STEPHEN MURPHY
JOHN O'FLAHERTY
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]

CONSULTANT:
PHILIP COYLE

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

second storage unit (configured to store a ...personal biological biometric identification parameters)	28, line 22; 30, lines23-28; 36, line 28; 45, line 26	2	140
Life signs detector detects a critical level... prevents access	40, lines 7- 23 to page 41 line 3	4	403

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

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

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

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

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

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

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

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

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

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

FRKELLY

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

In view of the foregoing, I wish for the present application to be remitted to the Examining Division so that all the subject matter which was deleted from the claims in view of the unity objection is fully examined in accordance with the European Patent Convention.

Yours faithfully

Paul Keane
Representative

p.keane@frkelly.com
+353 1 231 4862

Europäisches Patentamt
European Patent Office
Office européen des brevets

Letter accompanying subsequently filed items

Representative:

FRKelly
519
27 Clyde Road
D04 F838 Dublin
Ireland

Phone: +353 1 231 4848
Fax: +353 1 614 4756
E-mail: docketing@frkelly.com

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

P.O. Box 5818
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 during the appeal procedure	Appeal letter Unity.pdf	APPEAL-ORAL.pdf

	Payment	
1	Method of payment	Not specified

Signatures

Place:	
Date:	**04 October 2018**
Signed by:	**Paul Keane 36258**
Association:	**FRKelly**
Representative name:	**Paul keane**
Capacity:	**(Representative)**

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	6776706	
Application number	EP11752936.2	
Date of receipt	04 October 2018	
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 APPEAL-ORAL.pdf\Appeal letter Unity.pdf (3 p.)
Submitted by	CN=Paul Keane 36258	
Method of submission	Online	
Date and time receipt generated	04 October 2018, 14:39 (CEST)	
Message Digest	33:14:F4:BB:56:9A:76:6A:15:9C:D6:DD:32:C3:30:52:37:A5:BF:EB	

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/

SENDEBERICHT

ZEIT : 08/10/2018 13:30
NAME : EPO BOARDS OF APPEAL
FAX : 00498923993014
TEL :
S-NR. : E71294H6J323666

DATUM/UHRZEIT	08/10 13:29
FAX-NR./NAME	00035316144756
Ü.-DAUER	00:00:53
SEITE(N)	02
ÜBERTR	OK
MODUS	STANDARD

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Date
08.10.18

only by facsimile on
Fax No. +353 1 614 4766

Zeichen/Reference/Référence	Anmeldung Nr./Application No./Demande n°//Patent Nr./Patent No./Brevet n°
P105633EP00 APPR	11752936.2 / 2545485

Anmelder/Applicant/Demandeur//Patentinhaber/Proprietor/Titulaire
OS - New Horizon Personal Computing Solutions Ltd.

Appeal number: T2287/16-3.5.06

Cancellation

1. ☑ The oral proceedings appointed for 09.10.18 have been cancelled.

2. ☐ The oral proceedings appointed for

have been rescheduled to: at .

will now be in Room No.

The other provisions in the summons of 22.01.18 remain unchanged.

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Date
08.10.18

only by facsimile on
Fax No. +353 1 6144756

Zeichen/Reference/Référence	Anmeldung Nr./Application No./Demande n°//Patent Nr./Patent No./Brevet n°
P105633EP00 APPR	11752936.2 / 2545485
Anmelder/Applicant/Demandeur//Patentinhaber/Proprietor/Titulaire	
OS - New Horizon Personal Computing Solutions Ltd.	

Appeal number: T2287/16-3.5.06

Cancellation

1. ☑ The oral proceedings appointed for 09.10.18 have been cancelled.

2. ☐ The oral proceedings appointed for

have been rescheduled to: at .

will now be in Room No.

The other provisions in the summons of 22.01.18 remain unchanged.

The Registrar B. Atienza Vivancos
Tel.: 089 / 2399 - 3561

Annex(es): ☑ Acknowledgement of receipt - EPO Form 3936

Beschwerdekammern des Europäischen Patentamts ★ Boards of Appeal of the European Patent Office ★ Chambres de recours de l'Office européen des brevets

EPO Form 3017 01/11

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Boards of Appeal

The Registry

Name: B. Atienza Vivancos

Tel.: 089 / 2399 - 3561

Date: 08.10.18

Zeichen/Reference/Référence		Anmeldung Nr./Application No./Demande n°//Patent Nr./Patent No./Brevet n°
P105633EP00	APPR	11752936.2 / 2545485
Anmelder/Applicant/Demandeur//Patentinhaber/Proprietor/Titulaire		
OS - New Horizon Personal Computing Solutions Ltd.		

Appeal number: T2287/16-3.5.06

EPA/EPO/OEB Formblatt/Form/Formulaire: 3017

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)

Beschwerdekammern des
Europäischen Patentamts
Richard-Reitzner-Allee 8
85540 HAAR
DEUTSCHLAND

Rücksende-Adresse / Return address / Adresse de retour

EPA Form 3936 08/17

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Appeal number: T2287/16-3.5.06

Order

Oral proceedings to be held on 09.10.18

☑ are cancelled.

☐ are rescheduled for at hours

Room N°

Munich, 08.10.18

The Chairman W. Sekretaruk

EPO Form 3014 08/17

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

Datum/Date
12.11.18

Zeichen/Reference/Référence	Anmeldung Nr./Application No./Demande n°//Patent Nr./Patent No./Brevet n°
P105633EP00 APPR	11752936.2 / 2545485
Anmelder/Applicant/Demandeur//Patentinhaber/Proprietor/Titulaire	
OS - New Horizon Personal Computing Solutions Ltd.	

Appeal number: **T2287/16-3.5.06**

Please find enclosed a copy of the decision of 09.10.18.

The Registrar U. Bultmann
Tel.: 089 / 2399 - 3561

Annex(es): ☑ Acknowledgement of receipt - EPO Form 3936
☐

Registered letter with advice of delivery

EPO Form 3032 01/11

Internal distribution code:

(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 9 October 2018

Case Number: T 2287/16 - 3.5.06

Application Number: 11752936.2

Publication Number: 2545485

IPC: G06F21/32, G06F21/62

Language of the proceedings: EN

Title of invention:
A SECURED PERSONAL DATA HANDLING AND MANAGEMENT SYSTEM

Applicant:
OS - New Horizon Personal Computing Solutions Ltd.

Headword:
Secured personal data handling system/OS NEW HORIZON

Relevant legal provisions:
EPC Art. 56, 113(1)
EPC R. 103(1)(a), 111(2)
RPBA Art. 11

Keyword:
Inventive step (no)
Substantial procedural violation (no)
Remittal to the department of first instance (no)

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Decisions cited:

Catchword:

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Beschwerdekammern
Boards of Appeal
Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 2287/16 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 9 October 2018

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

Representative:
FRKelly
27 Clyde Road
Dublin D04 F838 (IE)

Decision under appeal:
Decision of the Examining Division of the European Patent Office posted on 24 May 2016 refusing European patent application No. 11752936.2 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman W. Sekretaruk
Members: M. Müller
G. Zucka

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division, dispatched with reasons dated 24 May 2016, to refuse European patent application No. 11 752 936 for added subject-matter (Article 123(2) EPC) and lack of inventive step (Article 56 EPC) over the documents

D1: US 2009/083847 A1 and
D2: US 5 229 764 A.

Documents D3-D5 were cited in the decision but not relied upon in the reasons. In a section entitled "Further Remarks", the decision mentions three further documents (XP055260933, XP055260935 and WO2006076658) "in support of" a statement made in the reasons, and raises an objection of non-unity *a posteriori* in view of the finding that the independent claims lacked inventive step. For ease of reference, the three documents are referred to as D6-D8 hereinbelow.

II. The appellant requested that the decision be set aside, that a patent be granted on the basis of claims 1-13 according to a main request or auxiliary requests 3 and 4, claims 1-11 according to auxiliary request 1, or claims 1-4 according to auxiliary requests 2, 5 and 6, all as filed with the grounds of appeal, in combination with the description (pages 1-60) and the drawings (sheets 1-9) as published, and that the appeal fee be reimbursed because the decision was insufficiently reasoned and the appellant's right to be heard was violated.

III. Claim 1 of the *main request* reads as follows:

"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, 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, 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 and the operation of the portable handheld apparatus is completely shut down."

Claim 1 of *auxiliary request 1* differs from claim 1 of the main request in that the preamble states the apparatus to be operable to "interphase" 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 ..."

and that the "processing module" and the "encryption module" are marked as "integrated". Moreover, in the last paragraph of claim 1 the first occurrence of "portable handheld" is deleted, and so is the feature that the personal data files are "in said first memory module".

Auxiliary request 2 differs from auxiliary request 1 in that most dependent claims are deleted. Claim 1 of auxiliary request 2 is identical to that of auxiliary request 1.

Claim 1 of *auxiliary requests 3 and 4* is identical to that of the main request, except that the term "external device" is replaced by "mobile communication device or a personal computer" or "mobile communication device", respectively.

Claim 1 of *auxiliary requests 5 and 6* is identical to that of the main request, except that the term "external device" is replaced by "computer or cellular phone" or "mobile communication device", respectively.

IV. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that no fundamental deficiency was apparent that required the board under Article 11 RPBA to remit the case to the examining division without an assessment of its merits. In substance, the board took the preliminary view that the independent claims of all requests lacked inventive step over D1 and D2, Article 56 EPC, and noted that the unity objection *a posteriori* was secondary to the inventive step objection against the independent claims and therefore presently not decisive for the case.

V. In a letter dated and received on 2 October 2018, the representative informed the board that he would not be attending the oral proceedings but requested that the oral proceedings be held in the appellant's absence. In a further letter, received on 4 October 2018, the representative withdrew the request for oral proceedings but provided arguments for the board's consideration. In particular it stated that "a significant [part] of claims/subject matter had to be deleted in order to overcome the unity objection" and requested that the application be remitted to the examining division "so that all the subject matter

which was deleted from the claims in view of the unity objection [was] fully examined".

VI. The appellant did not, however, address the inventive step objection raised by the board.

VII. The oral proceedings were then cancelled.

Reasons for the Decision

The invention

1. The application relates to the fact that users need to have "easy, affordable, and immediate" access to personal data, some of which may be sensitive (such as medical records) and must hence be specially protected (page 1, paragraph 1).

1.1 The application discloses that, as a solution, security tokens are known to store and protect sensitive data (see page 1, paragraph 2). Some such tokens are discussed in detail, esp. the "Medicard", which require biometric authentication before providing access to the stored data (see page 3, last paragraph, to page 4, paragraph 1). Known tokens are said to have a number of shortcomings such as lacking "connectivity" and liveness detection (see the paragraph bridging pages 4 and 5).

1.2 The invention proposes a particular such security token (see page 9, paragraph 2, and figures 3a and 3b). It provides encryption so that the sensitive data need not be stored in plain text, and different biometric,

liveness and affect sensors, so that access to the data can be limited to authorized users, possibly depending on their emotional or physiological state (see e.g. page 14, last paragraph, to page 15, paragraph 2; page 26, paragraph 2, to page 28, paragraph 2; page 37, paragraph 2). The security token may act as a "mass memory" of private data for its owner (page 12, paragraph 1; page 13, lines 9-12 and 26-32; pages 33 and 39, paragraph 3) and may, insofar, replace other portable devices (see page 14, paragraph 2). It may also offer further functionality such as initiating an emergency call, e.g. through a connected cell phone, and communicating the device location (page 12, paragraph 2; page 15, last paragraph; page 24, paragraph 3; page 28, last paragraph, to page 29, paragraph 2; page 34, paragraph 2).

1.3 The envisaged typical use scenario is depicted in figure 1 (see page 23, penultimate paragraph, to page 24, paragraph 1). The token may be attached to one of several "external" devices, such as a smartphone (355), a landline phone (365), a computer terminal (360) or multi-user I/O terminals (362) connected to some service network, be it a landline or cellular telephone communication network (305, 310) or the Internet (370). When the token is attached to an external device and held by an authorized user, the external device can retrieve data from the token's memory or write into it (see page 41, lines 16-19).

1.4 It is also disclosed that biometric data can be obtained and verified "continuously" and that, if this fails, further access to the personal data may be denied and the token may "completely" shut down (see original claim 2).

Article 11 RPBA, Rule 103(1)(a) EPC,
alleged substantial procedural violations

2. The appellant requests that the appeal fee be reimbursed because two substantial procedural violations occurred during examination.

2.1 It argues that its right to be heard under Article 113(1) EPC was violated because it could not comment on documents D6-D8, which were mentioned first in the reasoned decision (see the grounds of appeal, page 3, paragraph 2; page 4, paragraphs 1-2).

2.2 It also takes the view that the decision was insufficiently reasoned (Rule 111(2) EPC), because

i) the examining division justified an Article 123(2) EPC objection to a feature merely with the statement that "the applicant did not provide, and the examining division could not identify in the application as filed", disclosure of that feature (see page 6, last paragraph, to page 7, paragraph 1),

ii) it did not provide evidence for its statement that "the use of encryption for data protection is a well known technique" (see the grounds of appeal, page 9, point 2.3.1), and

iii) it did not use, as would have been required, the problem-solution-approach to show why the skilled person would have combined D1 and D2 (see page 10, point 4) or these two with any of D6-D8 (see page 10, point 2.4).

3. As regards the alleged violation of the appellant's right to be heard, the board's opinion is as follows.

3.1 The board agrees with the appellant that the mention of new documents only with the reasoned decision may affect the its right to be heard, but also where it does not may cause avoidable misunderstandings.

3.2 That said, the board notes that point 2.4 of the reasons, to which documents D6-D8 relate, discusses a feature which the examining division considered to contravene Article 123(2) EPC (see reasons 1.1). Ignoring this feature, the examining division concluded in point 2.3 of the reasons (last sentence) that claim 1 lacked inventive step.

3.3 The board has no objection to the examining division ignoring, in an inventive-step assessment, a feature that it found to contravene Article 123(2) EPC. More specifically, the board considers that the examining division is not obliged to anticipate the replacement of such a feature with a similar one that might be originally disclosed and provide a speculative inventive step assessment of a so-amended claim.

3.4 The board thus considers that point 2.4 of the reasons contains - and is easily recognisable as containing - an *obiter dictum* itself and not to form part of the reasons for the inventive-step objection. Thus, a potential deficiency of the argument in point 2.4 cannot be a fundamental one within the meaning of Article 11 RPBA or a substantial procedural violation according to Rule 103(1)(a) EPC. This applies in particular to the citation of documents D6-D8 "in support of the statement in section 2.4" (see further remarks 1 in the decision and point 3.1 above).

3.5 The board also notes that the argument put forward in point 2.4 of the reasons was already given in the

communication of 30 March 2016 (point 2.1) without reference to any written evidence. The appellant not having responded to this communication, the examining division was entitled to maintain its opinion without having to produce evidence for it. And that the examining division has indeed maintained its opinion appears to follow from the fact that the newly cited documents were introduced merely "[f]or completeness" in a section clearly separate from the reasons for the decision.

3.6 Finally, while the appellant stresses that it should have been given an opportunity to study D6-D8, it does not, in its grounds of appeal, contradict the substantive assumption about the common knowledge in the art which D6-D8 were cited to support (reasons 2.4 and further remarks 1). Hence, the substantive assumption *per se* seems to be uncontroversial irrespective of the disclosure of D6-D8.

4. With regard to the allegedly insufficient reasoning, the board takes the following view.

4.1 The examining division found (see the decision, reasons 1.1) that it was not derivable from the passage in the description cited by the appellant - and which had been identified by the examining division in the annex to its summons to oral proceedings (see point 1.1) - and the last passage of page 39 "that the apparatus [was] operable to inter[face] with any other external device" as claimed. It was added ("Furthermore") that "the applicant did not provide, and the examining division could not identify in the application as filed, the support for the amendment" in question (see reasons 1.2). The examining division had

already raised the same objection in its communication dated 30 March 2016 (see point 1.2), to which the appellant chose not to respond.

4.2 The board considers that the reasons provided by the examining division are sufficient to justify the Article 123(2) objection. It is not relevant in this regard whether the board agrees with it. Moreover, the examining division had no occasion to assume that the appellant considered this reasoning to be insufficient or in what respect.

5. Also as regards points ii) and iii), the board does not agree that the decision is deficient. Regarding point ii), the board notes that the appellant does not challenge the examining division's assumption in substance, and regarding point iii), the board notes that the examining division has formulated an objective technical problem and then stated that it was solved in D2 (see reasons 2.3.2). The board takes the view that this scenario would have provided sufficient prompt for the skilled person to combine D1 with D2 and sees no lack of compliance with the problem-solution approach.

6. When the board drafted its preliminary opinion, and for the reasons reproduced above, the board did not see any fundamental deficiency in the first instance proceedings that would have required an immediate remittal of this case to the first instance under Article 11 RPBA.

7. A reconsideration of this issue, and a decision as to whether a substantial procedural violation had occurred that could make reimbursement of the appeal fee equi-

table, is not necessary because the board does not find the appeal to be allowable (see Rule 103(1)(a) EPC).

8. The appellant further argued that "the present application was unfairly prejudiced against as a result of the Unity Objection which was raised in the Search Opinion" (see the letter received on 4 October 2018, paragraph 2).

8.1 It is true that the search division raised a nine-fold non-unity objection against the set of claims 1-15 that were filed before the supplementary European search report. More specifically, based on the finding that independent claims 1, 6 and 12 were not allowable due to lack of novelty or inventive step over D1, it argued that the dependent claims made different and non-unitary contributions over D1. It is also true that the examining division maintained its non-unity objection - and the appellant objected to it - throughout the examination proceedings.

8.2 However, the application was refused *inter alia* for lack of inventive step and not for lack of unity. The non-unity objection against the dependent claims was kept only as an *obiter dictum* that expressly depended on the finding that the independent claims 1 and 5 lacked inventive step (see the decision, further remarks 2).

8.3 Thus, the non-unity objection is secondary (*a posteriori*) to the question whether the independent claims are allowable or not. If the independent claims had been found to be allowable, the non-unity objection would have fallen, too, and any objection to the dependent claims is immaterial for the application as a

whole if the independent claims are found to lack inventive step.

8.4 The appellant states that he had to delete a substantial part of the claimed subject-matter in response to the non-unity objection. It also suggests that remittal for further prosecution by the examining division is required for the applicant to have the deleted subject-matter "fully examined" (see the letter received on 4 October 2018, page 3, paragraph 2).

8.5 The appellant does not, however, specify which subject-matter it had to delete or what kept it from reintroducing it during examination or appeal. At no point did the examining division - or this board - object to an amendment because it related to "deleted" subject-matter. Any subject-matter that the appellant might want to have "fully examined" by the examining division after remittal could have been filed during the appeal proceedings. That this has not happened renders unclear what purpose the requested remittal could serve.

8.6 Consequently, and irrespective of whether and to what extent the board agrees with the non-unity objection in substance, the board cannot allow this request.

Claim construction

9. The board notes that the term "interphase" does not exist in the relevant art and takes it that "interface" is meant instead.

10. The independent claims of all requests specify that the claimed "apparatus [is] operable to [interface] with an external device for various operations" without specifying the kind of operations or whether or how

they interact with the security mechanism specified in the remainder of the claims.

11. The independent claims state that "access to the stored 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". Due to the "and", this phrase is ambiguous between saying that access is denied "by way of" shutting down the device or access is denied independently of the shutdown.

12. The independent claims specify that "access [...] is only enabled" after successful authentication of the user. The board notes that this phrase refers to any access, not just access by the external device.

13. The independent claims specify continuous biometric authentication and the detection of a "change" in the biometric parameters. Illustrating the notion of change, the appellant refers to a device that detects a change in the user's heart rate, takes this to indicate that the user is under duress and shuts down the device to protect the data (see the grounds of appeal, page 10, paragraph 2). However, the claim wording is much broader than that: Specifically, if the apparatus was handed over to a different user after the first authentication, a "change" in the measured biometric parameters would also be detected.

The prior art

14. D1 discloses an electronic device, preferably a mobile phone (see figures 6 and 7), with several biometric and liveness sensors for controlling access to its data (see paragraph 25, 28, 41, 57, 75 and 76).

15. D2 discloses a protected system that requires continuous biometric authentication for a user to get and keep access to the system (see column 2, lines 41-66, and column 3, lines 21-26) and that may shut down when the user "fails more than a prescribed number of [biometric] comparison tests" (see column 5, lines 4-6, and column 7, lines 24-28).

Inventive step

16. In a nutshell, the invention is a mobile data storage for sensitive data which can be attached to all kinds of "external devices" to provide them with access to the sensitive data. Access is controlled by biometric and liveness sensors and further protected by encryption. A central idea is that the mobile device keeps data storage separate from the applications running on the external devices (see the grounds of appeal, page 7, paragraph 4 from the bottom).

16.1 D1 discloses a smartphone storing sensitive data, access to which is controlled by biometric and liveness sensors, i.e. providing the claimed data storage functionality and the biometric access protection. The data access being controlled is "local", i.e. originates from a user manipulating the smartphone rather than from any "external device".

16.2 However, the board considers it to be commonly known that smartphone data can be accessed from an "external device", via its display and keyboard, for example from a PC in order to backup the smartphone memory or to transfer pictures. It is also commonly known that the data on the phone can only be accessed from the PC when the user has logged in at the phone. In its preliminary opinion, the board did not provide any written evidence

for this assumed common general knowledge, and the appellant did not challenge it.

16.3 The board therefore takes it to be common practice in the art - and thus at least obvious in the context of D1 - that the access control mechanisms provided on the phone may also control access to the data from an external device such as a PC.

16.4 Beyond that, the board agrees with the assessment in the decision under appeal (see reasons 2.2), that the claimed invention differs from D1 by

(a) an encryption module for the storage of user's data,
(b) continuous biometric (re-)authentication, and
(c) shutdown of the apparatus should biometric re-authentication fail.

16.5 The appellant stresses that the "working relationship" between the "processing module", the "memory module", the "encryption module" and the biometric sensors is very specific and provides a link between the above differences (see the grounds of appeal, page 11, point 5). On this account the board notes that it is obvious that a "processing module" be "in communication" with all the other components. The board does not accept that any further interaction between the difference features can be derived from the claimed subject-matter.

16.6 As regards feature (a), the board agrees with the decision under appeal (reasons 2.3.1) that "the use of encryption for data protection" in computer memory is well-known in the art. Also the appellant has not

challenged this assumption in substance (see the grounds of appeal, point 2.3.1).

16.7 As regards features (b) and (c), the board notes that there is no clear difference between "repeated" and "continuous" re-authentication, and reiterates (see point 13 above) that the notion of "change" is very vague and subsumes the situation that biometric data has changed because the apparatus was handed to a different user. From this perspective, the board agrees with the decision (see reasons 2.3.2) that D2 provides a solution to the problem given by the examining division, namely to avoid an unauthorized change of users.

16.8 The board therefore concludes that none of features (a) to (c) establishes an inventive step of the claimed invention over D1, Article 56 EPC.

Auxiliary requests 1-6

17. The auxiliary requests differ from the main request in referring to the external device's display or keyboard (auxiliary request 1), in limiting the "external device" to, respectively, "a mobile communication device or a personal computer" or simply "a mobile communication device" (auxiliary requests 3, 4, 5, 6), and in the deletion of dependent claims (auxiliary requests 2, 5 and 6).

17.1 The deletion of dependent claims is immaterial to the deficiencies of the independent claims. Also, in considering the main request the board has assumed the external device to be a personal computer. Therefore,

the assessment of the main request applies directly to auxiliary requests 1-3 and 5.

17.2 The fact that the independent claims of auxiliary requests 4 and 6 are limited to external access by a "mobile communication device" does not have any impact on the accessed apparatus itself. Moreover, it was an obvious trend in the art well before the priority date in 2010 of the present application that "mobile communication devices" were carrying out more and more functions which used to be limited to desktop computers. Thus the board concludes that this difference cannot render the claimed invention non-obvious either.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated

Sendungsnummer / No de l'envoi / Item number

Art der Sendung /Nature de l'envoi / Type

☐ Brief / Lettre / Letter - Einschreiben / Recommandé / Registered

☐ Paket / Colis / Par[illegible] Vertragskunden)

RH 22 768 969 0DE

RÜCKSCHEIN

Avis de réception

Advice of delivery

Aufkleber auf der Vorderseite der Sendung anbringen.

FRKelly
27 Clyde Road
Dublin D04 F838
IRLANDE

I2287/16

de l'envoi / Addressee

117529362

Am Bestimmungsort auszufüllen / A remplir par le bureau de destination / To completed by office of destination

O.g. Sendung wurde ordnungsgemäß ausgeliefert / L'envoi mentionné ci-dessus a été dûment livré / The article mentioned above was duly delivered

Datum und Unterschrift* / Date et signature* / date and signature*

R Wells 19.11.18

Name in Großbuchstaben (oder andere eindeutige Identifikation)
Nom du destinataire en lettres majuscules (ou autre moyen clair d'identification)
Name of recipient in capital letters (or other clear identification)

* Dieser Rückschein kann vom Empfänger oder wenn die Vorschriften des Bestimmungslandes dies vorsehen, von einem Beauftragten oder Mitarbeiter des Postunternehmens im Bestimmungsland unterschrieben werden.

* Cet avis pourra être signé par le destinataire ou, si les règlements du pays de destination le prévoient, par une autre personne autorisée au par l'agent du bureau de destination.

* This receipt must be signed by the adressee or a person authorized to sign under the regulations of the country of destination or if those regulations so provide, by the employee of the office of destination.

CN 07 | UPU - RL 137.2.2

Deutsche Post AG

Entreprise des Postes allemandes S.A.

RÜCKSCHEIN / Avis de réception / Advice of delivery

Postsache
Service des Postes
Postal service



10.10

915-005-000

PRIORITAIRE
By Airmail
Par avion

Stempel der Post, die den Schein zurücksendet.
Timbre di bureau renvoyant l'avis.
Postmark of the office returning the receipt.

TO

Zurücksenden an / Renvoyer à / return to

Europäisches Patentamt
80298 MÜNCHEN
DEUTSCHLAND / ALLEMAGNE / GERMANY

Europäisches Patentamt
European Patent Office
Office européen des brevets

Closure of the procedure in respect of application No. 11752936.2 - 1217 12.12.18

1. **The procedure in respect of the above application is closed for the following reason:**

REFU 2/24.05.16 The time limit under Art.108 EPC has expired.
No notice of appeal under Article 108 and Rule 99 EPC has been filed. No request for a decision under Rule 112(2), or for further processing under Article 121 EPC or for re-establishment of rights under Article 122 EPC has been filed.

2. **The EPASYS situation has been verified in respect of item 1:**

DFIL: 10.03.11

NOAP: REFUAPPR/21.07.16/26.09.16/21.07.16/

RDEC: ////

RFPR: //

REES: ///

REFU 3/ADWI 3 and DEAD 1 coded. Date of legal effect 09.10.2018

3. **Position regarding fees:**

FEFS01	002	00995586	12.10.12	EUR	975,00
DEST03	005	00995586	12.10.12	EUR	555,00
EXAM02	006	00995586	12.10.12	EUR	1 555,00
NOAP04	011	01027220	21.07.16	EUR	1 880,00
FFEE01	020	00995586	12.10.12	EUR	115,00
RFEE 03	033	00646205	26.03.13	EUR	445,00
RFEE 04	034	00691279	25.03.14	EUR	555,00
RFEE 05	035	00785872	27.04.15	EUR	810,00
RFEE 06	036	00707491	23.03.16	EUR	1 040,00
RFEE 07	037	01228126	28.09.17	EUR	1 165,00
RFEE 08	038	00749529	27.03.18	EUR	1 280,00
PFEE 05	095	00785872	27.04.15	EUR	405,00
PFEE 07	097	01228126	28.09.17	EUR	582,50
NUPF04	520	00995586	12.10.12	EUR	686,00

☒ Examination started on 19.12.14 (EXDS51).

☐ Refund(s) ordered:

☐ 100% EXAM fee** ☐ 75% EXAM fee** ☐ 50% EXAM fee**

☐ DEST fee* ☐ RFEE(s): _____ ☐ Other fees: _____

Note: Attention is to be paid to potential automated refund proposal(s).

* Refund of DEST fee if date of legal effect is before/on SEPU or PACT6 date.

** PLEASE REVIEW REFUND OF EXAMINATION FEE (100% or 75% or 50%)

4. **Mark "DEAD" on the paper file and:**

☒ Check whether a divisional application is pending and if so attach the DEAD file to it.

☐ Any **models** still in the Office's possession were returned on _____
(for dealing with models, please refer to Fil d'Ariane).

☒ Keep paper file in file store (separate place) until next action for file destruction.

12.12.2018
Date

Stuckart, Christoph
Formalities Officer

CS03868

EPO Form 2058 11.16