FORM P8
(To be lodged in duplicate)

REPUBLIC OF SOUTH AFRICA
PATENTS ACT, 1978

PUBLICATION PARTICULARS AND ABSTRACT
[Section 32 (3) (a) - Regulations 22 (1) (g) and 31]

OFFICIAL APPLICATION NO			LODGING DATE		ACCEPTANCE DATE		
21	01	2007/02733	22	2 Apr 2007	43		

INTERNATIONAL CLASSIFICATION	
51	G06F F16P

Not for publication
Classified by:

FULL NAME(S) OF APPLICANT(S)

71 **MOGOBA, Pearl, Mantsoko; RAUTENBACH, Walter, Ignatius**

FULL NAME(S) OF INVENTOR(S)

72 **MOGOBA, Pearl, Mantsoko; RAUTENBACH, Walter, Ignatius**

TITLE OF INVENTION

54 **PERSON IDENTIFICATION, TRACKING AND SAFEGUARDING SYSTEM**

EARLIEST PRIORITY CLAIMED	COUNTRY		NUMBER		DATE	
NB - Use International abbreviation for country (See Schedule 4)	33	ZA	31	2006/00781	32	27 Jan 2006

57	Abstract (not more than 150 words) and figure of the drawings to which the abstract refers, are attached.

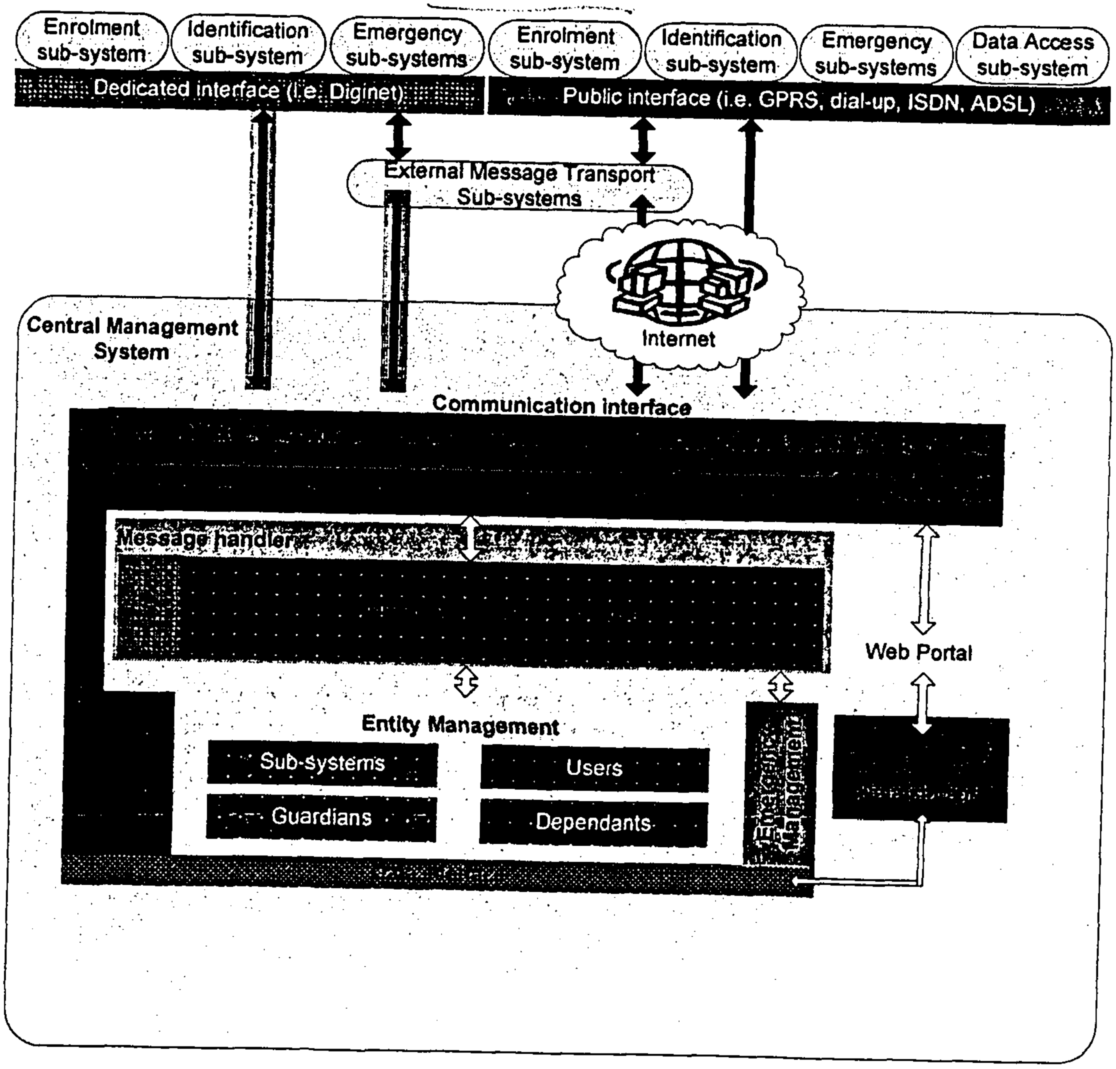
Number of sheets	

57	Abstract (not more than 150 words) and figure of the drawings to which the abstract refers, are attached.

Number of sheets	

FIGURE FOR PUBLICATION

FIG. 1



FIELD OF INVENTION

The invention described in this document is a method and system, offering guardians and dependants' services and functionality that will assist in proactively preventing harm, assist with emergency situations as well assist with escalating of declared emergencies. The invention has a primary application to children but can also be applied to other persons, such for example as other dependants, prisoners or persons on parole, occupants of old age homes and foreign visitors.

BACKGROUND

Certain proposals have been made in the literature around chills locating and tracking, identification and loss prevention; reference may be made to US patents that each describe some but not all features of the invention : -
7,114,619, 6,338,529, 6,7704,806, 6,278,370, 6,266,592, 6,168,495, 6,061,571 and 5,934,492.
The absence of a comprehensive system that is highly co-ordinated and accesses available technology solutions in a unified way reduces the effectiveness of dealing with preventing harm, dealing with emergency situations and assisting with escalating declared emergency situations.

THE INVENTION

The invention provides a method that will securely transfer data electronically between systems. The data to be transferred electronically relates to data of a personal and or critical nature that could be applied to locate and or identify children and others who may or may not find themselves in a possible vulnerable or dangerous situation. In addition the invention will enable the identification of the enrolled child's guardian or other contact. Signals are securely transmitted from a transmitter device to a central server which will intelligently process the data. Depending on the nature of the data transmitted to the central server, appropriate decisions will be made (either artificially or by human intervention) to take appropriate action. The action can include interfacing with other systems in order to locate and or identify the child or person whose transmitter sent the received signal.

This invention extends to the implementation of the system, including the enrolment of children and their guardians or others.

The system consist of a secure central system that provides an open interface that allows for integration of various technologies as well as several tightly integrated decentralised components or sub-systems to provide assistance and safeguarding for persons on the system, in a unique way.

The invention further provides apparatus that manages identification and tracking data of guardians and the dependants under their protection. The identification data captured is configurable and adaptable to allow for incorporation of new identification characteristics and methods as well as tracking technologies as they become available.

The identification and tracking units technologies are integrated into a system that provide the protection, safeguarding and emergency escalation services and functionality as briefly described above.

The invention includes the following individual components:

Personal and or critical data

The invention relates to a method where data of a personal and or critical nature can be transferred electronically across electronic mediums between secure systems in order to assist in the locating and or identification of children that may or may not find themselves in possible vulnerable or dangerous situations.

The nature of the data includes:

- In order to successfully locate a child electronically, global positioning coordinates (GPC) that are acquired from the Global Positioning System (GPS) are required.

- A child's vital bodily signals such as monitoring the child's heart rate and respiratory functions. The vital signals can be used to establish whether a child finds himself/herself in a possible vulnerable or dangerous situation

- Biometric data includes a child's fingerprints, retinal scan, voice recognition, facial recognition. The biometric data is extended to the child's guardian as it is to be used to successfully identify a child's guardian when required.

- Other personal information will include information that will assist in uniquely identifying a child when required. This can include but is not limited to an Identification Number, name, surname, birth date etc.

- The invention will allocate a unique identification number to uniquely identify the child on the system

An enrolment station or service centre

The service centre could be a temporary, mobile, or fixed location where guardians of children who wish to register their children and themselves on the child locating and identification system. The service centre will comprise out of at least one enrolment station (Personal Computer) which will have various peripherals attached to it in order to successfully enrol a child and their guardians.

The enrolment station will enable communication with the transmitter and receiver device that is uniquely assigned to a child. The enrolment station will securely write required data to the child's assigned transmitter/receiver in order to enable accurate identification of the child.

The enrolment station will securely connect to a central server where required data is stored in order to allow for effective and immediate action when required.

The enrolment station will run specialized enrolment software that will be used to securely enrol children and their guardians and to transmit and receive electronic data from authorised systems.

A personal computer that will be suitable for this invention is the Acer Power F6 Desktop PC.

Registration or enrolment involves adding a new entity to the system described in this invention. The main entities in this invention are:

- ➢ Sub-systems
- ➢ Users
- ➢ Guardians
- ➢ Dependants

These entities are described further below. Any of these entities need to be registered on the system before obtaining access to the system. During the registration of a new entity on the system the system assigns a unique identifier and certification to the entity which is used in the lifecycle of the system to ensure system integrity and ability to be audited. This process is described in detail under the *Security Module* section.

Sub-systems in the apparatus are systems or platforms that are registered and link to the core system. Sub-systems consist of hardware whose functionality is defined by software components. Sub-systems are normally enrolment or identification systems that collect and transmit identification data to the core system. Sub-systems can include third-party or external systems

Users include a person registered on the system to perform system functions. Examples of these functions are registration and enrolment of guardians and dependants on the system as well as system configuration. These functions require knowledge of how the system works in order to maintain the integrity of the system data and cannot be done by a guardian or dependant.

Guardians include parents or anyone that will potentially take care of anyone dependant on them at any point in time. The system relation between guardians and dependants are defined as a many to many relation. This allows various guardians to be assigned to a dependant like parents, school teachers and care takers. The relations are clearly identified on the system and configurable rules can be implemented when the dependant is under the protection of a particular guardian at a particular time. Many dependants can be assigned to a particular guardian.

A potential guardian can also be enrolled on the system even if there is no current dependant under its protection. This is allowed to enable familiarisation of the system before becoming a guardian as well as readiness for when a dependant needed to be added to onto the system.

Dependants include persons that are dependant on someone else or that needs to be taken care of. The most common dependant, but not limited to, is a child depending on its parents, as guardians, to ensure his/her safety.

Unlike the guardian, a dependant will always be assigned to at least one guardian. The guardian requesting the dependant to be registered and enrolled on the system is defined as the primary guardian.

Visual identification characteristics

These type of characterises can be used to visually verify a person. Some of these characteristics overlap other identification characteristics but are defined separately since they rely on a human to visually compare them to confirm an identity. The human interaction with this type of biometrics can have a negative impact on the accuracy of this identification method. Examples of these characteristics are portrait images, identification numbers and so on, used typically on identification documents.

- Assigned identification data

  Assigned identification data can consist of an identifier assigned to a person to assist with identification. These identifiers are normally stored on an electronic device like a cell phone, global positioning system, radio frequency tag, card or chip carried by the entity to be identified. Some of these assigned identification data can be linked to a person by attaching it to a person or physical belongings of a person. Examples of this are child protection bracelets and motor vehicle tracking devices.

  Assigned identification data is only as accurate as far as it can be assured that the correct person is carrying or using it. Accuracy can be improved by combining the use of it with biometric or visual identification characteristics to it as well as attaching the device securely to the carrier.

Identification is the function of establishing someone's identity without knowing who the person is. The verification function on the other hand is the process of confirming someone's claimed identity.

Both of these functions make use of identification data previously captured to perform their function. Reference to identification in this document includes verification unless specifically indicated differently in the specific text.

The definition of identification data in this content is data that is associated with a person that will assist at a later point with positively recognising the person or establishing he's/her identity or other attributes belonging or assigned to them.

Identification data is used to:

- Establishing an unknown persons identity
- Confirming the identity of a person that claims to be someone
- Locating a person with the use of previously captured identification data

Identification data can be categorised as follow:

- Common characteristics

  These are characteristics that cannot on their own provide unique identification of a person. A combination of these characteristics can assist with filtering for identification but can still not offer definite unique identification of a person. An example of these types of characteristics is a person's names, eye colour, height and birth date

Biometric devices

- Biometric characteristics

  These characteristics are measurable, physical or personal behavioural traits belonging to a specific person. Many different biometric characteristics exist like voice, fingerprint, palm, facial, vein and DNA to name but a few. What makes some biometric characteristics more usable than others are the conversion of these characteristics into processed binary data that can be used to identify a person, or confirming a person's identity, in a time efficient and convenient fashion, increasing the uniqueness by establishing a bigger biometric pattern.

  Many biometric identification techniques claim to be unique. Unique is a relevant term as there is currently no database and there most probably never will be a database at any single point in time storing everyone's biometric data to proof it the concept of uniqueness. Never the less, certain biometric traits, like fingerprints, are 'unique' enough to be accepted as reliable identification techniques. Using different biometric elements in conjunction, referred to as multifactor biometrics, dramatically increase the uniqueness of the data.

Biometric devices include fingerprint scanners, retinal scanners, voice recorders, camera, and signature pads. that will be used to capture the biometric data of children and their guardians.

Fingerprint scanners are in general use today and suitable devices include the Sagem MSO 300 and the Suprema SFR300. The fingerprint scanner will capture a person's fingerprints and specialised software will create templates for later use in identifying a person.

Retinal scanners are highly specialised and very expensive. A suitable retinal scanner includes the LG IrisAccess 4000. The retinal scanner will capture a person's iris patterns and specialised software will create templates for later use in identifying a person

Cameras are used to capture facial images and specialised software will create templates for later use in identifying a person. A suitable camera for the invention is the Canon PS 540.

Signature pads capture a person's electronic signature. Specialised software will create templates for later use in identifying a person. Signature of guardians will be captured. The Interlink EPad is suitable for this invention.

Tracking data in this context is associated with an entity on the system and which provides information of the entity it is associated with. Samples of tracking data are physical location information, vital signs, information relating to an entity accessing or utilising services of the system.

Tracking data is only as accurate as the source it is received from and the translation of the information received.

Transmitter and receiver devices

Transmitter and receiver devices are those devices that will allow for the locating of children. The transmitter and receiver device will allow for the storage of electronic data that can be used to uniquely identify the carrier thereof. The transmitter and receiver devices can vary in size, functionality, and duration of service. The transmitter can be a small electronic chip that can be implanted underneath the child's skin for a long period of time, or alternatively the transmitter and receiver can be worn as a bracelet around the wrist, neck, or ankle etc. for only a specified period of time.

The transmitter and receiver functionality can vary and could run basic software to only transmit it location or alternatively enable two way voice communications, fingerprint technology by embedding a fingerprint scanner onto the device etc.

Many transmitter and receiver devices exist today which differ in size, robustness, and functionality. The present invention relates to securely transferring data electronically and ensuring personal and critical data on children is available when required. Therefore, the invention is not concerned with the transmitter and receiver as it will cater to allow for communication between the invention and the various transmitter and receivers.

The transmitter and receivers boast different functionality which includes but are not limited to:

- Two-way voice communication
- GPS functionality to track a the carrier thereof
- Sending distress signals
- Monitoring bodily vial signals
- Storing personal information that can be used to identify the carrier thereof

The premise of the transmitter and receiver is that it will be switched on while carried by a child; it will be in working order, that it will uniquely identify the carrier thereof and that it will allow for locating a child.

Although various transmitters and receivers exist, the following includes but is not limited to transmitters and receivers that are suitable for the invention:

- LAIPAC S-911 Personal Locator
- LAIPAC GPS bracelet
- VeriChip

Communication mediums

Communication mediums allow for communication between the various components of the invention. Communication mediums are those mediums that enable the transmitting of electronic data between devices and include but are not limited to Satellites orbiting earth and cellular networks.

Central server

The central server will be used to govern secure communication between systems. The central server will receive and store the personal and critical information of children and their guardians. The central server will process the received data appropriately and where required perform appropriate action. The action can include but is not limited to alarming authorities on a potential dangerous situation that a child may or may not find him/her in.

The central server will also provide for an interface where authorised users can access personal or critical data.

A server that will be suitable for this invention is the Dell PowerEdge 2950.

External systems

The invention will allow for external systems to securely interface with the central server in order to transfer data to and from the central server and or external system. The external system will run specialised applications in order to enable secure communications between the systems.

THE DRAWINGS AND EXAMPLES

The invention is more fully described by way of examples, including the following drawings : -

Figure 1 is a schematic of the apparatus of an embodiment of the invention,

Figure 2 is a flow diagram illustrating the functionality of an embodiment of the invention,

Figure 3 is an illustration of th schematics used,

Figure 4 is a flow chart that illustrates an example of a flow of data within the communication interface,

Figure 5 is a flow diagram that illustrates the authority management and encryption layer,

Figure 6 illustrates an external message transport subsystem.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring to figure1, the functions of the *Central Management System* is to receive, store, process and redistribute sub-system, user, guardian and dependent identification and tracking data in a secure fashion to ensure system integrity and to enable safeguarding of persons on the system.

The *Central Management System* is built around a Service Orientated Architecture (SOA) which allows for expansion of functionality through adding new services to the system to enable the functionality growth as required over an extended period.

The *Central Management System* can be sub-divided into the following main service groups for:

Security Module (SM)

The core function of the Security Module is to ensure the integrity of data on the system. Data integrity is essential as any tampering with data or forbidden access to the system compromises the protection of guardians and dependants on the system.

The *Security* Module is used across the whole system. Each sub-system will describe in detail the implementation of the *Security* Module pertaining to it. This section documents in detail sections which is not described in the individual sections but that is required for understanding the *Security Module.*

Communication Interface Security

The *Security Module* implementation for the *Communication Interface* can be divided into the following:

- General encryption layer
- Authority management encryption layer
- User access layer

The implementation of these security layers is described further in this section as well as in the sections where it is integrated into specific modules.

Authority Management Module

The main function of the *Authority Management Module* is to generate, assign and manage digital certificates associated with entities on the system to ensure integrity of data communicated between sub-systems and the *Central Management System.* The *Authority Management Module* contains Certification Authority (CA) capabilities.

To ensure system integrity the *Authority Management Module* assign a strong digital certificate to any sub-system or person registered on the system. This unique digital certificate is generated on the centralised system and is done in a trusted and secure environment. The certificate is unique to the entity (sub-system or person) it is assigned to and is used to secure all data for storage and transmission.

Referring to figure 2, The flowchart indicates the process followed for assigning a certificate to a person or sub-system:

No sub-system or person can transact on the system without a digital certificate assigned to it. For this reason a certificate is assigned directly after being registered on the system.

All decentralised sub-systems will also be assigned a certificate in the same way as the persons enrolled on the system. This certificate will be used to ensure authenticity of data communicated to and from the centralised system and will leave a footprint to reliable indicate the source of the specific transaction on the system.

This is described in more detail under the *Communication Interface Security* section.

Hardware encryption and communication module

The hardware encryption and communication module is a configuration of different hardware components to ensure secure communication with the *Communication Interface*. This module is implemented on the sub-system side but is described in this section as it works with the *Security Module* to perform its function.

The use of this device on the sub-systems is preferred but data can be processed from sub-systems that do not implement this device. In these cases data will be treated accordingly.

The device is connected to a 'host' utilising the RS232, USB or Bluetooth host interface. A 'host' is defined as any remote platform accessing the *Central Management System*. The host can be a computer, point-of-sale or any other platform with the capability to communicate via USB, RS232 or Bluetooth interface.

Hardware components

The hardware components incorporated into this module are:

Global Positioning System (GPS)

The GPS function is to record positioning information. The coordinate information is retrieved by the processor component and stored on the flash data for retrieval by the host.

This information can be used to establish the location of the unit and to determine if the unit is used within its defined location parameters.

This hardware component is an optional item in the configuration of the hardware encryption module. It can be controlled by the processor or can be electronically switched to enable the host to do direct communication with the device.

General Packet Radio Service (GPRS) and Global System for Mobile (GSM) modem

The GPRS/GSM modems function is to enable the device to communicate with remote systems, specifically the *Central Management System*.

This hardware component is an optional item in the configuration of the hardware encryption module. It can be controlled by the processor or can be electronically switched to enable the host to do direct communication with the device.

Flash data storage

The flash data storage is used to store information for processing by the processor. The data storage is divided into two partitions:

- Secure area

  The secure area is used to store security certificates. Write access to this area is only accessible by the processor through the presentation of a certificate generated by the *Authority Management* module and specifically intended for the purpose of updating this area. The *Authority Management* module form part of by the Central *Management System* and is discussed later on.

  The secure area stores the following information:

  - Unique device serial numbers and identifiers
  - System authorization certificates that allows for certificate retrieval by the processor. These certificates are assigned to specific sub-system implementations and are required to retrieve data protection certificates.
  - Device certificates that is retrieved by the processor for:
    - Encryption of data stored on the *general storage area*
    - Creation of session keys for secure communication
    - Certificates used for external data storage
  - Configuration and device profiles controlled by the host

- General storage area

  The general storage area is used by the device to store information internally with regards to logs retrieved from other hardware components and general transaction information. A sub-system platform can also make use of this storage area if authorized by the *Authority Management* module.

  The data is protected under the certificates stored in the secure area of the flash.

The certificates described above, functions in combination with the unique processor serial number. This serial number is a combination of the manufacturer serial number and manufacturer id to ensure unique identification across processor manufacturers. The serial number is included in all certificates generated by the *Authority Management* module or by local keys created by the device itself.

This hardware component is not optional and will exist on all *Hardware encryption and communication modules*. The size of the flash data storage hardware components can vary according to requirements.

System clock

The system clock is used by the module for the following purposes:

- Time stamping transactions and logs
- Generating random session and local keys
- Managing expiry of profiles

This hardware component is not optional and will exist on all *Hardware encryption and communication modules.*

Host interfaces

The following interfaces can be provided to communicate to the host.

- USB
- RS232 serial
- Bluetooth

All of the mentioned hardware components are optional items, but at least one needs to be incorporated in the configuration of the hardware encryption module at any time.

External interfaces

The external interfaces are implemented to provide interfaces for external devices (excluding the host). These devices can for example be a cell phone, fingerprint reader or any other device with a known interface, communicating via one of the following communication mediums:

- USB
- RS232 serial
- Bluetooth

These hardware components are optional items in the configuration of the hardware encryption module. It is possible to have two USB, RS232 and Bluetooth interfaces, where one is used for host interfacing and the other one for external interfacing. It is also possible to have one of each and be able to switch between if the component is used for host or external interfacing.

These components can be controlled by the processor or can be electronically switched to enable the host to do direct communication with the device.

Integrated fingerprint reader

This optional hardware component can be integrated into the device for added security as well as avoiding adding additional hardware components to a sub-system. This device can be controlled by the processor or can be electronically switched to enable the host to do direct communication with the device.

Processor

The processor is used to integrate all the different devices into the *Hardware encryption and communication module.* The processor logic is spilt into two clearly defined sections. The first is the kernel that will consist of the code controlling the interfaces to all the other hardware components, data storage access and encryption functionality. The other part can contain downloadable programs to perform specific functionality like interfaces to external devices or specialized functionality applying to a specific sub-system type.

This hardware component is not optional and will exist on all *Hardware encryption and communication modules.*

Power

The device will mainly receive its power from the host when connected. The module will contain power regulators and converters to supply and regulate power to the different hardware components.

Battery

The module will contain a battery. In some cases the battery will be in the form of a backup battery that will mainly be used to maintain correct system clock details while not connected to the host and therefore without power. In other cases a more sophisticated battery will be used to perform minor operations while the device is not connected to the host. These operations will typically be recording and storage of GPS coordinates.

Battery charger

The battery charger module will depend on the type of battery used on the system. The charger will be responsible for charging the battery while in contact with the host or external power supply.

Hardware schematics

Referring to figure 3, The module is connected to the sub-system, acting as the device host, using one of the *host interfaces* described above. This device is registered on the *Central Management System* and is then used to secure communications from and to the *Central Management System*. Information from the device, like global positioning information, can also be used by the *Central Management System* to determine if the sub-system is operating in the correct location or tracking of mobile units for operational purposes.

When a guardian or dependant comes in contact with a sub-system using this module, the tracking information will be linked to the specific person. Therefore this unit also provides reliable identification and tracking data that can be used to protect entities on the system

The core function however is to manage certificates supplied by the *Central Management System* when communicating data to the *Central Management System*. Certainty of the source and reliability of data received from a sub-system using this module is the main benefit.

Integration of this into the total system is discussed in many of the sections following.

Referring to figure 4, the flow chart illustrates how a typical flow of data would be within the *Communication Interface*:

The communication interface manages all communication messages between components and systems outside the *Communication Interface* and allows for interaction with the *Central Management System*.

This service group or module serves as the communication bus for data interchange between different services within the *Central Management* System in support of the *Service Orientated Architecture*. It is responsible to validate, process and forward communication within the system, to the different modules for processing.

The communication medium (i.e. GPRS, dial-up, ISDN, ADSL, Diginet line) is not restricted to current communication technology available. It provides access through a public or dedicated interface for more stringent data processing requirements. Both methods allow for interfacing with the same central system functionality.

The *Communication Interface* consists of different modules to ensure the interface remains configurable and flexible. No system that needs to allow for scalability can operate on predefined messaging interfaces. The different sub-systems in this interface allow for fully configurable security and message structure definitions.

The *Communication Interface* consist of the following modules

- Security Module (SM)
- Message Handler (MH)
- Web Portal (WP)

1.1.1.1 Communication Interface security

The *Security Module* expands over the whole system. The implementation of the *Security Module* in the *Communication Interface* consists of the following layers:

1.1.1.1.1 Generic Encryption Layer (GEL)

The *General Encryption Layer* is a standard security layer for encrypting data on protocol level. This encryption is implemented through current technologies like Secure Socket Layer (SSL) or Secure Hyper Text Transfer Protocol (S-HTTP) as implemented for TCP and HTTP communication. Although this layer is documented in this invention it is purely done to illustrate the security principals followed but in it self it is standard technology implemented to enhance the security of the system.

This layer is implemented by installing specific technology servers and hardware to manage the protocol encryption. This layers' decryption is performed before it is processed by the other internal security layers adding additional data protection, ensuring transparency to the *Central Management System.*

SSL and S-HTTP are two examples of this type of encryption. Other 3rd party hardware and software encryption can be implemented to ensure compliance with external systems where required.

1.1.1.1.2 Authority Management Encryption Layer (AMEL)

The main function of the *Authority Management Encryption Layer* is to decrypt messages containing system data before passing it on to the *User Access Layer.* This security layer is only used for messages intended for the *Message Processing Module* and not *Web Portal* communication.

Referring to figure 5, the flowchart indicates the process logic performed by the *Authority Management Encryption Layer.*

The *Authority Management Encryption* layer uses sub-system registration data for encryption purposes. When a new sub-system is registered on the system certain encryption codes are assigned so the particular sub-system platform.

With other words, if a school decides to implement an identification sub-system for child identification, then an identification sub-system will be registered for the particular school and each of the identification points or platforms connected (i.e. computers) will be assigned certificates to operate with. Various ways of assigning these certificates are possible – It could be certificates linked to the particular platforms serial number or the certificates could be linked to a *Hardware encryption and communication module.*

Any data captured by this platform will be encrypted with the certificates assigned to the sub-system platform for storage and communication. The *Authority Management Module* will manage the assignment of certificates to these platforms and the *Authority Management Encryption* layer, which forms part of the *Authority Management Module,* will decrypt data communicated from the sub-systems to ensure the data have not been tampered with.

1.1.1.1.3 User Access Layer (UAL)

The purpose of the *User Access Layer* is to validate users that came in contact with the system. In many cases a user will not necessary be actively involved with a transaction submitted from a sub-system. In this case the transaction is not linked to a particular user and the transaction always assumes that the sub-system to be the user.

For certain transactions user intervention is required. An example of this is enrolment of new persons onto the system. A person cannot enrol himself onto the system due to enrolment quality and identity fraud issues. In cases where user intervention is required the data will be encrypted with the user's certificate, in addition to the general encryption module, so that the system can clearly identify which user was responsible for the capture. This is required for traceability and auditability.

After validating the information received, using the user certificate, data are validated against the system configuration. In the case where no user intervention was required, the sub-system rights are used to validate the transaction. Each user or sub-system has the right to perform certain functions or transactions. If the transaction submitted is not within this list, the system will not load the information into the system but will rather record it into the audit area where it will be escalated for investigation.

1.1.1.2 Message Handler (MH)

After the security validation done by the *Security Module* the data is passed onto the *Message Hander.* It is this module's function to process the message data by communicating with the *Entity Management* system to add, modify and remove data from the *Central Management System.*

The following section describes the method in which the *Message handler* manages communication within the communication interface. The functionality of the message handler interacts with most of the different modules within the communication interface. The module is specifically designed to allow for scalability of the system without changing the system.

Examples of communication structuring and configuration are provided below to assist the reader with understanding the way in which the module operates.

1.1.1.2.1 Communication structuring

Communication data is structured through the use of different message layers. These layers are used within the *Communication Interface* to validate communication and it enables the interface to forward the message data to the right message processing services within the central management system.

The message structuring can be illustrated in the following XML message format structure:

```
<ServiceID>1</ServiceID>  //Authority management encryption layer
<MessageID>2</MessageID>
<Version>23</Version>
<CertificateInfo>
    <1>
        <Owner>1234</Owner>
        <OwnerType>3</OwnerType>
        <PublicKey>45342343</PublicKey>
    </1>
    <2>
        <Owner>54321</Owner>
        <OwnerType>1</OwnerType>
        <PublicKey>43545234</PublicKey>
    </2>
</CertificateInfo>
<EncryptionMethod>3</EncryptionMethod>
<Request> //User access layer content
    <ServiceID>5</ServiceID>
    <MessageID>56</MessageID>
    <Version>1</Version>
    <UserInfo>
        <1>
            <UserID></UserID>
            <UserType>3</UserType>
            <PublicKey>45342343</PublicKey>
        </1>
    </ UserInfo>
    <EncryptionMethod>6</EncryptionMethod>
    <Request> //Message Handler content
        <ServiceID>26</ServiceID>
        <MessageID>76</MessageID>
        <Version>3</Version>
        <Request> //Entity management – Dependant module content
            <ServiceID>55</ServiceID>
            <MessageID>66</MessageID>
            <Version>3</Version>
            <Request> //Processing content
                <GaurdianID>7511165033087</GaurdianID>
                <NewDependantID>200101035022089</NewDependantID>
            </Request> //Processing content
        </Request> //Entity management – Dependant module content end
    </Request> //Message Handler content end
</Request> //User access layer content end
```

This message structure determines the flow of data through the *Central Management System*. Each of the processing layers will perform its function on the data and will use the service ID, Message ID and Message version to determine the flow of the message through the communication bus within the *Central Management System.*

The first level of messaging processing within the *Communication* Interface will generate a unique transaction id. This transaction ID will be entered into the transaction processing database for reference by sub-processes and can be used for auditability.

All the data in this message example is in readable format but in reality it will not be in this format since different layers perform content decryption as required for the message definition and in accordance with the message contents.

In the above example the text in red will be encrypted when received by the *Authority Management Encryption Layer.* This data will then be decrypted and validated using the certificate information received in the message data. Any decryption failure at any level will result in a security audit entry and data communication will be terminated without any response to protect the system against trial an error intrusion.

If the validation performed by the *Authority Management Encryption Layer* is successful the layer required by the *Authority Management Encryption Layer will be removed* and the remainder of the data, now not encrypted, together with additional data added by the *Authority Management Encryption* Layer, according to the requirements defined in the *Message Configuration Module*, will be forwarded to the right service for processing according to the service ID, Message ID and Message version indicated in the next level of message data. Please note that in the *Message Configuration Module* definition a relation will be defined from where a message can be forwarded to and not. This security feature ensure that a particular message follows the communication bus as it should and prevents incorrectly structured messages from being forwarded to services without following the correct route.

In this example the following would be passed onto the next service:

```
<ServiceID>5</ServiceID>
<MessageID>56</MessageID>
<Version>1</Version>
<ServiceAddition>
        <TransactionNumber>454543</TransactionNumber>
</ServiceAddition>
<UserInfo>
        <1>
                <UserID></UserID>
                <UserType>3</UserType>
                <PublicKey>45342343</PublicKey>
        </1>
</ UserInfo>
<EncryptionMethod>6</EncryptionMethod>
<Request> //Message Handler content
        <ServiceID>26</ServiceID>
        <MessageID>76</MessageID>
        <Version>3</Version>
        <Request> //Entity management – Dependant module content
                <ServiceID>55</ServiceID>
                <MessageID>66</MessageID>
                <Version>3</Version>
                <Request> //Processing content
                        <GaurdianID>7511165033087</GaurdianID>
                        <NewDependantID>200101035022089</NewDependantID>
                </Request> //Processing content
        </Request> //Entity management – Dependant module content end
</Request> //Message Handler content end
```

Please take note of the additional field <TransactionNumber> added by the processing service. This is an example of where the service is required to add data for processing by the next service.

The next service, defined as 5 in the example, belongs to the *User Access Layer*. The message ID and content enables this layer to validate the function being performed against the system user that initiated the request.

In this example above the text in red will be encrypted when received by the *User Access Layer*. This multilevel data encryption enables more secure data transport. The number of levels of encryption use is determined by the requirements of the particular sub-system and configured accordingly on the *Central Management System* through the *Message Configuration* Module. This data is then decrypted and validated using the certificate information received in the message data.

The transaction is processed once the *User Access Layer* decrypted the message and validated the action performed by a particular user. A negative response will be send to the requesting system if the user performing the action is not authorised to do so. This response is also controlled by the *Message Configuration Module*.

In this example the following would be passed onto the next service if validation was successful:

```
<ServiceID>26</ServiceID>
<MessageID>76</MessageID>
<Version>3</Version>
<ServiceAddition>
        <TransactionNumber>454543</TransactionNumber>
</ServiceAddition>
<Request> //Entity management – Dependant module content
        <ServiceID>55</ServiceID>
        <MessageID>66</MessageID>
        <Version>3</Version>
        <Request> //Processing content
                <GaurdianID>7511165033087</GaurdianID>
                <NewDependantID>200101035022089</NewDependantID>
        </Request> //Processing content
</Request> //Entity management – Dependant module content end
```

Please take note that once again the additional field <TransactionNumber> added by the processing service.

The next service, defined as 26 in the example, belongs to the *Message Processing Module*. The message ID and content enables this layer to format and root the message to correct module. In certain cases the data received by the *Message Processing Module* needs to be formatted into a particular format for processing by a particular processing module. This as well as load balancing, in the case of multiple servers performing processes, is the function of the *Message Processing Module*.

The *Message Processing Module* will validate the information and pass the following information on to the service that needs to perform the processing:

```
<ServiceID>55</ServiceID>
<MessageID>66</MessageID>
<Version>3</Version>
<Request> //Processing content
        <GaurdianID>7511165033087</GaurdianID>
        <NewDependantID>200101035022089</NewDependantID>
</Request> //Processing content
```

The following is an example of the reply data created by the service that performed the processing:

```
<ServiceID>26</ServiceID>
<MessageID>76</MessageID>
<Version>3</Version>
<ServiceAddition>
        <TransactionNumber>454543</TransactionNumber>
</ServiceAddition>
<Reply>
        <ServiceID>55</ServiceID>
        <MessageID>66</MessageID>
        <Version>3</Version>
        <Reply> //Reply content
                <NewDependantID>200101035022089</NewDependantID>
                <ReplyCode>Dependant Added</ReplyCode>
                <UniqueSystemID>45434534</UniqueSystemID>
        </Reply> // Reply content
</Reply>
```

Please note that the service that performs the process and calculates the reply know where it should be passed back to through the data stored in the *Message Configuration Module*. This enables the system to transfer the response through the message bus to the required services for processing and then back to the requesting sub-system.

This method of data transportation allows for both single and batch processing. The following is an example of how the above request and reply would look in batch processing mode:

Batch request:

```
<ServiceID>55</ServiceID>
<MessageID>66</MessageID>
<Version>3</Version>
<Request> //Processing content
        <1>
                <GaurdianID>7511165033087</GaurdianID>
                <NewDependantID>200101035022089</NewDependantID>
        </1>
        <2>
                <GaurdianID>6812165033087</GaurdianID>
        <NewDependantID>200701035022089</NewDependantID>
    </2>
</Request> //Processing content
```

Batch reply:

```
<ServiceID>26</ServiceID>
<MessageID>76</MessageID>
<Version>3</Version>
<ServiceAddition>
        <TransactionNumber>454543</TransactionNumber>
</ServiceAddition>
<Reply>
        <ServiceID>55</ServiceID>
        <MessageID>66</MessageID>
        <Version>3</Version>
        <Reply> //Reply content
                <1>
                        <NewDependantID>200101035022089</NewDependantID>
                        <ReplyCode>Dependant Added</ReplyCode>
                        <UniqueSystemID>45434534</UniqueSystemID>
                </1>
                <2>
                        <NewDependantID>200701035022089</NewDependantID>
                        <ReplyCode>Dependant Already On System</ReplyCode>
                </2>
        </Reply> // Reply content
</Reply>
```

1.1.1.2.2 Messaging Configuration Module (MCM)

The *Message Configuration Module* allows for configuring different message formats and data flow within the system. This module consist of configuration data stored in the *Central Management System* database as well as program logic to access the configuration data when receiving incoming messages for validation and rooting of messages.

Please note that key fields are indicated in **green**.

The first definition type is service definitions. This identifies a specific program that contains certain logic and functionality to process specific data received. A service is defined as follow:

Service definition:

Field	Description	Data type	Length
Service ID	Unique id created for each service on the system	Numeric	2
Description	Describes the function performed by the service	Alpha	1000

To ensure that messages follow the correct route the following table defines what messages can be received:

The following would be the data entries for service definition in the example provided above under *Communication Structuring:*

Service ID	Description
1	Authority management encryption layer – Dependant additions
5	User access layer – Dependant additions
26	Message handler – Dependant additions
55	Dependant management module – Dependant additions

Any defined messages have to follow pre-defined routes to ensure that the right route is followed in the communication bus. These rules are determined by the *Service route definition* table:

Service route definition:

Field	Description	Data type	Length
Service ID	Unique id created for each service on the system	Numeric	2
Message ID	Unique id created for each possible request on the system	Numeric	2
Message type	Indicates if the root definition entry defines the route for request or reply messages. 0 = Request, 1 = Reply	Numeric	1
Destination Service ID	Unique service id where the message can be routed to	Numeric	2

The following would be the data entries for service route definition in the example provided above under *Communication Structuring:*

Service ID	Message ID	Message type	Destination Service ID
1	2	0	5
5	56	0	26
26	76	0	55
55	76	1	26
26	56	1	5
5	2	1	1

Multiple request routes can be defined for a Service ID and Message ID combination. This allows a different request route to be followed for incoming messages. Any Service ID and Message ID combination can only have one reply definition as this is used to reconstruct the reply message.

This table content is used to ensure validity of 'request' messages and is used to construct 'reply' responses.

For each route definition certain data can be added to the message before forwarded to the next service end-point. The *Service route data addition* table indicates to the service what data needs to be added onto the message before passing the message on:

Service route data addition:

Field	Description	Data type	Length
Service ID	Unique id created for each service on the system	Numeric	2
Message ID	Unique id created for each possible request on the system	Numeric	2
Message type	Indicates if the route definition entry defines the route for request or reply messages. 0 = Request, 1 = Reply	Numeric	1
Destination Service ID	Unique service id where the message can be routed to	Numeric	2
Additional data	Indicates the field name that needs to be added to the message as it is processed by the service	Alpha	100
Source	The source indicates to the service where the data should be retrieved from. In certain cases the logic for retrieval of this data might be hard coded into the particular service	Alpha	1000

The following would be the data entries for service root data addition in the example provided above under *Communication Structuring:*

Route definition key	Additional data	Source
1, 2, 0, 5	<TransactionNumber>	*TransactionTable*
5, 56, 0, 26	<TransactionNumber>	*TransactionTable*
55, 76, 1, 26	<TransactionNumber>	*TransactionTable*

Each message has a specific Message ID and version that defines the structure of the message.

This is defined in the Message definition table:

Message definition:

Field	Description	Data type	Length
Message ID	Unique id created for each message on the system	Numeric	2
Message Version	Version of the message. Different message allowed for system evolution. The combination of *Message ID* and this field is unique and defines the structure of a message.	Numeric	1
Description	Describes the purpose of the message	Alpha	1000

The following would be the data entries for service message definition in the example provided above under *Communication Structuring:*

Message ID	Message Version	Description
2	23	AMEL – Dependant addition
56	1	UAL – Dependant addition
76	3	MH – Dependant addition
66	3	Dependant module - additions

For each combination of Message ID and version there is a definition of fields for the message. This is used by the services to validate that the required fields are present. These field definitions are stored in the Message field definition table:

Message field definition:

Field	Description	Data type	Length
Message ID	As defined above	Numeric	2
Message Version	As defined above	Numeric	1
Field name	The name of the field within the message	Alpha	1000
Message type	Indicates if the root definition entry defines the root for request or reply messages. 0 = Request, 1 = Reply	Numeric	1
Description	Describes the purpose of the message	Alpha	1000

The following would be the data entries for service message definition in the example provided above under *Communication Structuring:*

Message ID	Version	Field name	Message type
2	23	<CertificateInfo><Owner>	0
2	23	<CertificateInfo><OwnerType>	0
2	23	<CerificateInfo><PublicKey>	0
2	23	<EncryptionMethod>	0
56	1	<UserInfo><UserID>	0
56	1	<UserInfo><UserType>	0
56	1	<UserInfo><PublicKey>	0
56	1	<EncryptionMethod>	0
66	3	<GuardianID>	0

66	3	<NewDependantID>	0
66	3	<NewDependantID>	1
66	3	<ReplyCode>	1
66	3	<UniqueSystemID>	1

The function of the web-portal is to provide access to the data stored on the system. The access referred to will typically be information that guardians, dependants and users requires access to. Access to the web portal is controlled through user access codes and where increased security is required the access is controlled by the means of biometric validation protection.

Direct access to the web-portal is not allowed. For security and modularity reasons the access to the portal must be through a data access sub-system. Various data access sub-systems can exist to provide custom data and update capability to vendors that deliver value added functionality to the system.

Entity management

Sub-systems, user, guardians and dependants are managed as separate entities on the system. A guardian or dependant can be registered and enrolled as a user on the system but will be managed as separate entities.

A person can be added onto the system as a user, guardian and/or dependant. Data will not be recaptured during registration and enrolment if the data already exist on the system as a different type of entity. This is done to avoid management of common static and demographic details for one person in several places as well as preventing duplicate enrolment data capture and non-corresponding data in different areas on the system. Certain of the registration and enrolment data captured might however differ between the different types of entities. For this reason the additional data required by the second or third registration will be added as required. Please note that the person will have to be registered separately for each type of entity it represents. This is required since a unique identifier and certificate will have to be authorised and created with the registration information for each entity type. With other words, the person will exist as different system entities on the system but previously captured registration and enrolment data will be re-used to avoid duplication.

Certain users or systems will only have access to the registration and enrolment data pertaining to that particular entity management system. For example: Updating a person's guardian information will not allow for changing the persons user access information.

This section describes the functions of the *Entity Management Module*.

Sub-system management

Sub-systems are systems that provide access to the *Central Management System* in various forms. These systems can be implemented at various locations and add value to the system through:

- Providing input data for the *Central Management System*
- Accessing data on the *Central Management System* for guardian and dependant protection
- Managing interfaces with systems dealing with emergencies
- Managing non-compliant interfaces with systems that can add value to the system by providing identification and tracking information
- Accessing data on the *Central Management System* for reporting and management functionality

One particular sub-system can belong to different sub-system types. The main sub-system types are defined as:

- Enrolment
- Identification
- Emergency
- External message transport
- Data accessThis following section describes how sub-systems are managed on the *Central Management System.*

Registration and management

Before a sub-system can become active on the system it needs to be registered on the *Central Management System.* The registration of a sub-system consist the following:

- Receiving an authorisation request to add the new sub-system to the *Central Management System*
- Capturing owner and demographic information belonging to the sub-system for management purposes
- Requesting and assigning a unique sub-system number from the *Authority Management System* so that it can be recognised accordingly
- Associating unique serial numbers to the sub-system on the *Authority Management System.* This unique serial numbers can be that of the platform hard drive, CPU or the hardware encryption device assigned to it.

- Obtaining sub-system certificate information generated by the *Authority Management System*. This certificate information is generated using a combination of unique serial numbers assigned to the platform the unique sub-system number and type and is used for identifying and encrypting data received from the sub-system.
- The certificate information can either be:
    - issued in the form of an electronic certificate which needs to be present on the system for operation and that needs to correspond to the serial numbers from the sub-system
    - The sub-system owner can be issued with a *Hardware Encryption Module* that needs to be connected to the platform to enable operation. This method is more secure and will enable more secure transacting.

The information captured and associated to the particular sub-system can change. The interface allow for managing the data belonging to the sub-system. If certain key information, like serial numbers used for certificate generation, change then the particular certificate will be hot-listed and use of this will not be permitted any longer.

The operational activities can be controlled from the *Central Management System.* Therefore the operation of any sub-system can be suspended with immediate effect should a security breach of any sort be detected.

Configuration

The configuration of the sub-system entails the assignment of rights of the platform within the system. The sub-system has to operate within these rights. These rights include:

- What functions can be performed. With other words, a platform can for example provide identification functions but not enrolment functions.
- What area the platform can operate in. This is only appropriate for the instances where the platform is connected to a GPS or other positioning system and needs to operate within certain co-ordinates.
- What times the platform can operate in. A particular platform for example may only be used in a particular time period.

These are some examples of configurations. The *Service Orientated Architecture* allows for adding additional services complying with the scope of the system. Each service will contribute to the configurations that are allowed and therefore the configuration of the sub-systems using these services can grow with time.

Another part of the configuration on the *Central Management System* is configuring the data interchange between these different sub-systems and the central system. Certain common data elements will be required for sub-systems of the same type.

For example:

All enrolment platforms will have to be able to communicate enrolment data to the central system. For this they will have to do an enrolment upload request in real-time or in batch format. All of these communication messages will contain the following common information:

- User performing the enrolment
- Enrolment type, indicating if it is a user, guardian or dependant
- Identifier, used to uniquely identify the person being enrolled
- Identifier type, indicating what type of unique identifier is being used for enrolment
- Sub-system ID and security certificates
- Enrolment data type

The central system will know in the case where the enrolment data type indicates a type of biometric enrolment what data to expect. If it is flagged as a fingerprint enrolment it will expect to receive the fingerprint data in the enrolment message. The following is an example of the message:

```
<EnrolmentDataUpload>
        <EntityType>Guardian</ EntityType >
        <Identifier>6711155044087</Identifier>
        <IdentifierType>SAID</IdentifierType>
        <EnrolmentDataType>FlatFingerEnrolment</EnrolmentDataType>
        <EnrolmentDeviceType>Sagem MSO300</EnrolmentDeviceType>
        <EnrolmentDeviceSerialNumber>687798-9879-97</EnrolmentDeviceSerialNumbe>
        <EnrolmentData>
                <FingerData>
                        <FingerNumber>1</FingerNumber>
                        <FingerQuality>56</FingerQuality>
                        <FingerData>#encoded binary data#</FingerData>
                <FingerData>
                <FingerData>
                        <FingerNumber>2</FingerNumber>
                        <FingerQuality>56</FingerQuality>
                        <FingerData>#encoded binary data#</FingerData>
                <FingerData>
```

```
<FingerData>
        <FingerNumber>3</FingerNumber>
        <FingerQuality>56</FingerQuality>
        <FingerData>#encoded binary data#</FingerData>
<FingerData>
<FingerData>
        <FingerNumber>4</FingerNumber>
        <FingerQuality>56</FingerQuality>
        <FingerData>#encoded binary data#</FingerData>
<FingerData>
<FingerData>
        <FingerNumber>5</FingerNumber>
        <FingerQuality>56</FingerQuality>
        <FingerData>#encoded binary data#</FingerData>
<FingerData>
<FingerData>
        <FingerNumber>6</FingerNumber>
        <FingerQuality>56</FingerQuality>
        <FingerData>#encoded binary data#</FingerData>
<FingerData>
<FingerData>
        <FingerNumber>7</FingerNumber>
        <FingerQuality>0</FingerQuality>
        <FingerData>Damaged</FingerData>
<FingerData>
<FingerData>
        <FingerNumber>8</FingerNumber>
        <FingerQuality>0</FingerQuality>
        <FingerData> Amputated</FingerData>
<FingerData>
<FingerData>
        <FingerNumber>9</FingerNumber>
        <FingerQuality>0</FingerQuality>
        <FingerData>#encoded binary data#</FingerData>
<FingerData>
<FingerData>
        <FingerNumber>10</FingerNumber>
        <FingerQuality>0</FingerQuality>
        <FingerData>Amputated</FingerData>
<FingerData>
```

```
        </EnrolmentData>
</EnrolmentDataUpload>
```

One can notice that some of the mandatory data is not present in the message. This is due to the fact that it is presented in the header of the information. With other words, data like user and sub-system ID will only be sent once where many other enrolment data structures can be repeated.

The message configuration, as discussed in the *Communication Structuring*, will be managed by the *Message Configuration Module*. Enabling the type of messages for a particular sub-system will be *Sub-system Entity Management Configuration* interface.

For this reason specific sub-systems will only be able to communicate using specific messages. In the example used above the particular sub-system can also be configured to do linking of child tracking bracelets. In that case the message would look something like this:

```
<IdentificationDataAssignment>
        < EntityType >Dependant</ EntityType >
        <Identifier>6711155044087</Identifier>
        <IdentifierType>SAID</IdentifierType>
        <IdentificationDataType>Child tracking bracelet</ IdentificationDataType >
        <IdentificationDeviceType>ionKids Child Locator</IdentificationDeviceType >
        <IdentificationDeviceSerialNumber>dfs88-32423</IdentificationDeviceSerialNumber>
</ IdentificationDataAssignment >
```

Identification and tracking data storage and management

When a sub-system starts transacting, identification data is provided that can be linked to the sub-system, user, guardian or dependant. This identification data will be used according to the configuration of the sub-system.

For example: If a new enrolment sub-system is registered on the system, it will be assigned a unique number which will serve as its identification data. The platform will be registered as operating from a fixed location or it could be a portable workstation. In the case where it is a fixed location or where a GPS device is connected to the platform it can link the positioning information of persons using the system to its physical location. In the case of fixed location platforms, the *Central Management System* will know that any transactions performed by a user, guardian and dependant were done at that particular co-ordinates. With a portable enrolment platform linked to a GPS the platform would report the change of location as soon as it can to the *Central Management System*. With other words if a user signs on to the system, or if a user access the system to enrol a dependant or if a dependant is enrolled, this specific location information is linked to the particular person as identification and tracking information.

This data will be sent in a similar way as illustrated above, where the message is defined in the *Message Configuration Module* and the different identification and tracking data messages is linked through the Sub-system *Entity Management Module* to the particular sub-system according to its capability.

This data provided from sub-systems and linked to a person serves as identification data that can be used to track and protect persons accessing the system.

The particular sub-system definition and functions are described in more detail later on.

User management

Users are persons that access sub-systems to perform certain user functionality. This user functionality is defined and controlled from the *Central Management System*. Certain functionality on the sub-systems cannot be performed directly by the guardian or dependant and needs user intervention to ensure integrity of data on the system. Examples of this is registering and enrolling new guardians or dependants. To ensure integrity of the data these processes needs to be guided by a user. When a user register or enrol a new guardian on the system, the process will be guided by a user and will be linked to that user. This prevents guardians from adding themselves onto the system as different 'ghost' guardians and also ensures that the enrolment data complies with the standard required by the system.

This also provides for tracing particular transactions to a user in the case where fraudulent information was captured or where the data captured did not comply with the standards required so that correctional steps can be implemented.

Registration and management

Before a user can access the system he/she needs to be registered on the system. . The registration of a user consists out of the following:

- ➢ Receiving an authorisation request to add the new user to the *Central Management System*

- Capturing user particulars for management purposes. The details of the user and sub-system performing the user registration will also be stored with the user details for auditability.
- Requesting and assigning a unique user number from the *Authority Management System* so that the user can be recognised accordingly
- Obtaining user certificate information generated by the *Authority Management System*. This certificate information is unique to the user and is used for identifying and encrypting transactions performed by a particular user. The use of the certificate is protected by user access codes or biometric authentication depending on the specific transaction requirements.

After the registration of a user, certain transaction rights are assigned to him. These rights are used to control what transactions the user can perform or not. Some examples of these rights are:

- Registering sub-systems
- Configuring sub-system information on the *Central Management System*
- Configuring local settings on the sub-system platform
- Sub-system access rights controlling what users can access what platforms
- Registering users
- Enrolling users
- Configuring users
- Registering guardians
- Enrolling guardians
- Managing guardian information
- Registering and linking dependants to guardians
- Enrolling dependants
- Managing dependant information

The user rights will be stored in a user profile that can be downloaded by the sub-systems when a user requires access to a sub-system. User profiles can be used in conjunction with the user certificate in off-line operations. For this reason a particular user profile will be assigned a certain lifetime during which this profile can be used. If a user is suspended on the *Central Management System* but the sub-system does not come in contact with the central system then the user will still be able to perform functions off-line during the lifetime of the profile. When the sub-system comes in contact with the *Central Management System* the transactions performed after suspension of the user will not be entered into the *Entity Management System* for use but would be stored in a separate area for manual authorisation of the transactions.

Enrolment

All users of the system will be enrolled before accessing the system. The enrolment process entails:

- Capturing and linking of identification data. This data can differ depending on the user type and access required but can include:
  - Common characteristics
  - Biometric characteristics to be used for authentication. Where possible the system will enforce the capturing of this type of identification data and where possible use this data for external clearance like background and criminal clearance checks to ensure integrity of the system.
  - Visual identification characteristics
  - Assigned identification data. This assigned identification data can include smart cards, radio frequency tags and so on that must be present when accessing the system as an added security measure.

- Validation of registered user details
- Changing of user access codes

A previously registered and enrolled user needs to perform the enrolment of a new user. For security purposes the system will not allow the same user that performed the registration of a user to perform the enrolment as well.

The enrolment user will be linked to the new user record for audit and investigation purposes.

Identification and tracking data storage and management

Different identification characteristics can be associated or assigned to a user during his/her the lifetime as a user on the system. These identification characteristics are used to identify the user when accessing the system.

Before a user start transacting on the system certain of his/her identification data is used to verify his/her identity. The can for example be biometric identification characteristics, assigned identification information like smartcards or tags or user access codes. The verification of the user by these means unlock the user certificate to be used for transacting on the system. Different levels of authentication are required for different types of transactions. Biometric identification techniques will be used where possible to ensure reliable authentication of a user on the system.

When a user transacts on the system, a collection of data is used to track the user and his/her access on the system. For example: If a user sign onto a specific sub-system the information of the sub-system, like the physical location, will be linked to the user transaction. This data is stored on the *Central Management System* against the user record to track user activity on the system.

Guardian management

Guardians are persons registered on the system to take care of dependants registered or assigned to them. Guardians need to access the system to initiate and authorise system information to ultimately protect their dependants. The functional capabilities of a guardian is defined and controlled from the *Central Management System*. Certain functionality on the sub-systems cannot be performed directly by the dependant and needs guardian intervention to ensure integrity of data on the system.

Examples of this is registering and enrolling new dependants. To ensure integrity of the data these processes needs to be approved by a guardian. When a user register or enrol a new dependant on the system, the process will be approved by a guardian. This prevents users from adding themselves onto the system as different 'ghost' dependants.

This also provides for tracing particular transactions to a guardian in the case where fraudulent information was captured or where the data.

Registration and management

The first step of becoming a guardian on the system is being registered on the system. Registration and enrolment of a guardian only occurs once, although the guardian can be a guardian for several dependants on the system.

The registration of a guardian consists out of the following:

- Capturing guardian particulars for management purposes. The details of the user and sub-system performing the guardian registration will also be stored with the guardian details for auditability.
- Requesting and assigning a unique guardian number from the *Authority Management System* so that the guardian can be recognised accordingly

- Obtaining guardian certificate information generated by the *Authority Management System*. This certificate information is unique to the guardian and is used for identifying and encrypting transactions authorised by a particular guardian, where guardian authorisation is required. The use of the certificate is protected by guardian access codes or biometric authentication depending on the specific transaction requirements.

Two different guardian configurations exist on the system:

- Primary guardian

  A guardian is defined as a primary guardian when he/she is responsible for adding dependants onto the system. Only one primary guardian is allowed per dependant. The primary guardian can authorise the change of data of dependants for whom he/she is the primary guardian. This information can include secondary guardian access to dependant information. This for example is the parent of a child, where the dependant is a child.

- Secondary guardian

  A secondary guardian can be authorised by the primary guardian. In the example provided above a secondary dependant can be a school teacher or caretaker responsible for the child. The primary guardian is responsible for authorising registration of a secondary guardian on the system, for a particular dependant, and also specifies the rights and actions allowed by the secondary guardian

A guardian profile is created defining the rights of the guardian with regards to rights and actions allowed with his/her own data. This profile is very limited since in most cases a guardian is in charge of his/her own data.

The guardian-dependant profile, created according to the type of guardian and the rights and actions allowed for the guardian, is created when a new dependant is added onto the system. The use of this profile is more prominent as this defines the relation between the guardian and his/her dependant.

Enrolment

All guardians will be enrolled before accessing the system. The enrolment process entails:

- Capturing and linking of identification data. This data can differ depending on the guardian and sub-system type.
    - Common characteristics
    - Biometric characteristics to be used for authentication. Where possible the system will enforce the capturing of this type of identification data.
    - Visual identification characteristics
    - Assigned identification data. This assigned identification data adds value to the guardian as it can assist with tracking the guardian in an emergency situation.

- Validation of registered guardian details
- Changing of guardian access codes

A previously registered and enrolled user needs to perform the enrolment of a guardian. The enrolment user will be linked to the new guardian record for audit and investigation purposes.

Identification and tracking data storage and management

Different identification characteristics can be associated or assigned to a guardian during his/her lifetime as a guardian on the system. These identification characteristics are used to identify the guardian when accessing the system.

Before a guardian start transacting on the system certain of his/her identification data is used to verify his/her identity. This can for example be biometric identification characteristics, assigned identification information like smartcards or tags or guardian access codes. The verification of the guardian by these means unlock the guardian certificate to be used for transacting on the system. Different levels of authentication are required for different types of transactions. Biometric identification techniques will be used where possible to ensure reliable authentication of a guardian on the system.

When a guardian transacts on the system a collection of data is used to track the guardian and his/her access on the system. For example: If a guardian signs onto a specific sub-system the information of the sub-system, for example the physical location, will be linked to the guardian transaction. This data is stored on the *Central Management System* against the guardian record to track user activity on the system.

This tracking information can also be used in emergency situations where the guardian has to be located. For example: A guardian can select to assign his/her vehicle tracking device as an assigned identification method to the system. To enable this, the vehicle tracking company will have to be associated to the system and be registered as an *Identification* or *External message transport sub-system* on the *Central Management System* and provide tracking information to the *Central Management System* on an ongoing or demand basis. This is discussed later on under sub-systems.

Dependant management

Dependants are persons registered on the system to be placed under the protection of guardians. The enable the protection of dependants on the system they need to be registered, on request of a guardian. In certain cases dependants need to access the system although most of the dependant functionality is controlled by their guardians. The functional capabilities of a dependant is defined and controlled from the *Central Management System*. Certain functionality on the sub-systems cannot be performed directly by the dependant and needs guardian intervention to ensure integrity of data on the system.

The following section describes the managements of dependants on the system.

Registration and management

The first step of becoming a dependant on the system is being registered on the system. Registration and enrolment of a dependant only occurs once although the dependant can be assigned to many guardians during his/her lifetime on the system.

The registration of a dependant consists of the following:

- Capturing dependant particulars for management purposes. The details of the user, requesting guardian and sub-system performing the dependant registration will also be stored with the dependant's details for auditability.
- The registration of a dependant is initiated by the primary guardian
- If the dependant is already on the system and linked to another guardian (the primary guardian) then the dependant will not be able to be registered again.
- Requesting and assigning a unique dependant number from the *Authority Management System* so that the dependant can be recognised accordingly
- Obtaining dependant certificate information generated by the *Authority Management System*. This certificate information is unique to the dependant and is used for identifying and encrypting transactions performed by a particular dependant, where dependant authorisation is required. The use of the certificate is protected by dependant access codes or biometric authentication depending on the specific transaction requirements.

Registration of a dependant is only performed once and the guardian requesting the registration is defined as the primary guardian. With authorisation of the primary guardian a number of additional guardians can be assigned to a particular dependant during the lifetime of the dependant, as a dependant, on the system. These are referred to as secondary guardians.

A guardian profile is created in relation to a dependant. With other words, when a dependant is added to the system or when a secondary guardian is defined for a current dependant, a Guardian-Dependant profile is created to define the relationship between the two entities. This profile stipulates the rights that a guardian has with regards to a dependant and the actions it can perform.

A dependant profile is also created but with the authority of the primary guardian. This profile dictates the rights and actions that a dependant has with regards to his/her own data. In most cases this profile is limited as most of the dependant data is managed by the guardian under the guardian-dependant profile.

Enrolment

The same as with other entities, all guardians will be enrolled before accessing the system. The enrolment process entails:

- Capturing and linking of identification data. This data can differ depending on the dependant and sub-system type as well as the guardians requirements. Enrolment allows for capturing of the following information:
    - Common characteristics
    - Biometric characteristics to be used for authentication. Where possible the system will enforce the capturing of this type of identification data.
    - Visual identification characteristics
    - Assigned identification data. This assigned identification data adds value to the guardian as it can assist with tracking the dependant in an emergency situation.

- Validation of registered dependant details
- Changing of dependant access codes

A previously registered and enrolled user needs to perform the enrolment of a dependant. The guardian also needs to be present to confirm the enrolment of a dependant. The enrolment user and guardian will be linked to the new dependant record for audit and investigation purposes.

All entities discussed can be re-enrolled on the system or additional enrolment functions can be performed to enrich or better the existing enrolment information. The re-enrolment or enrolment additions are performed using the same strict control measures to ensure integrity of the system.

Re-enrolments or enrolment additions In the case of dependants are more frequent depending on the age of the dependant. In the case of a child dependant certain enrolment data captured is only valid for a certain period. This applies typically for biometric and visual identification characteristics due to the fact that these change during the growth of the child. The period for which these types of identification characteristics are available is configurable on the system. The guardian is notified in time when dependant enrolment data needs to be re-captured to remain valid. These notifications are managed by the *Central Management System* as part of the service delivered to the guardian. All records of previous enrolments are kept to enrich the functionality of the system. Stick measurements are implemented to ensure that the updated enrolment data of dependants still belongs to the same dependant.

Identification and tracking data storage and management

Different identification characteristics can be associated or assigned to a dependant during his/her lifetime as a dependant on the system. The update of these identification characteristics is controlled by his/her guardians on the system according to the guardian-dependant profile. These identification characteristics are used to identify the dependant when accessing the system and provide valuable tracking information to assist the guardian in case of emergencies.

Before a dependant can make use of the system certain of his/her identification data is used to verify his/her identity. This can for example be biometric identification characteristics, assigned identification information like smartcards or tags or guardian access codes. The verification of the dependant by these means unlock the dependant certificate to be used for transacting on the system. Different levels of authentication are required for different types of transactions. Biometric identification techniques will be used where possible to ensure reliable authentication of a dependant on the system.

When a dependant transacts on the system a collection of data is used to track the dependant and his/her access on the system. For example: If a dependant is identified on a specific sub-system the information of the sub-system, for example the physical location and participating user details, will be linked to the dependant identification. This data is stored on the *Central Management System* against the dependant record to track dependant movement on the system.

This tracking information can also be used in emergency situations where the guardian is attempting to locate the dependant.

Emergency management

Emergency management is a core part of protecting guardians and dependants on the system and therefore a core function of the invented system. The emergency management module of the invention provides methods of declaring an emergency when it occurs and manage and distribute identification and tracking data according to system rules for efficient escalation of emergency situations.

Declaring an emergency

Before an emergency can exist it needs to be declared an emergency. Declaring an emergency can be something a person initiate or alternatively certain conditions that are met that indicates an emergency situation.

The following describes these methods:

Automated system emergency declaration

This method is controlled by the *Central Management System*. Different rules are configured on the system to define an emergency. Each identification and tracking method can be configured according to its own properties. The following are samples of different identification technologies and their possible configurations:

- ➢ Required identification

  Dependant or guardian profiles can be configured to report at a specific location for identification at certain times during their day-to-day life. A typical example of this is an identification sub-system implemented at a school where a child needs to be identified to acknowledge that they are there.

  For this type of scenario:

  - o The system administrator will configure the system to indicate that the particular sub-system is in operation during school days and what time the school start and end. Public holidays for will be configured on the system for the particular area.

- The sub-system owner, or school administrator, will configure certain exceptions like field trips and other events where children will not come to school.
- A secondary guardian like the school nurse will be able to indicate on the system when a child was booked out early due to sickness.
- The guardian will have permission to go onto the system and indicate when his/her child will not be able to attend school due to sickness or for any other reason. The guardian will also be able to indicate variances to be allowed for attendance as well as after school activities.

If the child is not identified at the school within the given parameters then the system will activate emergency procedure.

- Positioning information

Different identification devices can be assigned to a guardian or dependant. Samples of this type of identification data is:

- Protection bracelets with GPS or GPRS functionality
- Cell phones
- Vehicle tracking devices belonging to the persons primary form of transport

These devices are connected to central systems, which could be the *Central Management System* or that can be connected through *External Message Transport Sub-Systems* to the *Central Management System*, and provides positioning information.

Another source of positioning information is sub-systems. As described before, sub-systems either operate from a fixed location with fixed co-ordinates or they can be connected to a GPS module that provides location information. When a guardian or dependant transacts on these sub-systems the positioning information of these systems is stored as tracking data against their own records.

The *Central Management System* can implement certain rules with regards to positioning information. These rules can typically:

- Stipulate certain coordinates that are considered dangerous or forbidden areas.

When positioning information is received for a person and if the area is declared as dangerous or forbidden, then the system will raise an emergency when that person moves into or away from that pre-configured area.

- Relate positioning information of a person with certain timeframes

  This can be used as in the example above where certain areas are considered dangerous or forbidden with the difference that these areas are only registered as dangerous or forbidden within a certain timeframe. For example, if a child wears a protection bracelet with GPS functionality any area outside the living area might be declared a dangerous area during the night-time period.

  It could also be used in the opposite way where the positioning information should be within certain parameters during certain timeframes. A typical example is a child that needs to be within the school premises or if at a participating resort then the child should not leave certain perimeters of the resort.

Front-end

Various interfaces to the *Central Management System* exist. These are commonly referred to as the 'Front-end' as the persons registered on the system come in contact with these platforms or devices. A front-end in most cases is one of the possible sub-systems but can also be external devices linked to the *Central Management System* through *External Message Transport Sub-systems* to enable integration of these devices with the *Central Management System*.

In all the different methods provided, certain key information will have to be provided to link the emergency to a guardian or dependant.

The following section describes different ways in which an emergency can be declared by persons registered on the system through the front-end platforms.

1.1.1.2.2.1.1 User emergency declaration

A user can declare an emergency on the *Central Management System* on the instruction of a guardian or dependant. This is typically done through one of the *Emergency Sub-systems.*

An example of this is if a guardian calls a call centre to report a missing child. In this case the call centre operator will have access to an *Emergency Sub-system* and will enter the related data on the system for escalation.

1.1.1.2.2.1.2 Guardian emergency declaration

A guardian can declare an emergency on the *Central Management System* through various front-end interfaces. It works the same as the *User emergency declaration* but in this instance the guardian himself will authenticate himself through one of the sub-systems and record the information related to the incident.

An example of this is the guardian accessing the *Central Management System* through the internet or a particular sub-system designed for reporting emergencies.

1.1.1.2.2.1.3 Dependant emergency declaration

A dependant can also declare an emergency. This can be done in the same fashion as the above examples. In this scenario it is more likely that the emergency is activated silently by the dependant through the use of emergency functionality on for example a child tracking bracelet or by presenting a finger to a biometric identification sub-system which is registered as a duress finger and which is used only in these scenarios. This enables the dependant to activate an emergency without the knowledge of the persons which are potentially putting the dependant in an emergency situation.

Emergency rules, process execution and data distribution

The *Central Management System* manages different rules for different emergency situations based on the way that the emergency was declared as well as the information provided. These rules are configured on the system as new emergency types are defined on the system.

With the use of these rules different emergency escalation procedures are followed. For example:

If a teacher, declared as a secondary guardian, notices that a child is not present; he/she can declare an emergency through calling the call centre or by accessing one of the sub-systems to report the information. The *Central Management System* will have a particular execution sequence or rule configured for this type of emergency. Typically the following will happen:

- The primary guardian will receive a SMS reporting the incident. If the guardian responds favourably to the SMS the emergency event will be cleared and the reporting party will be notified accordingly. The guardian can respond by calling the call centre or accessing the *Central Management System* directly by logging onto a sub-system with an appropriate interface or by replying with a pre-determined response indicating that no emergency exist.

- If a favourable response is not received within a specified period, for example 5 minutes, then the process will be escalated to a call centre operator. The operator will attempt to get into contact with the primary guardian or guardians according to the dependant setup, to receive this type of emergency resolution functionality. If the guardian responds favourably then the emergency event is cleared and the reporting party will be notified accordingly.

- If the emergency is not resolved then the emergency will be escalated a further level. Typically historical and current tracking techniques would be activated. This information will be used generate a report indicating the last movements of the person on the system. If the information is current it will be forwarded to the guardian and/or external *Emergency Sub-systems* (like the police and emergency response companies) to assist with resolving the emergency. The operators of these systems can also provide information into the system to assist the *Central Management System* to resolve the emergency and to avoid duplication.

  Available tracking and identification devices will be activated and monitored actively. If the dependant is wearing a passive tracking device the device will be activated to receive tracking information. All related positioning systems, like GPS, vehicle and cell phone devices and any other sub-systems will be monitored actively for any activity. Any activity detection will be forwarded to *Emergency Sub-systems* to assist with resolving the emergency.

- The *Central Management System* will even further escalate the emergency should the dependant not be located within a certain time-frame. Examples of further escalation are:

  - Distribution of dependant profile information, like biometric and visual characteristic information to the police missing child system
  - This information can also be sent to other *Emergency Sub-systems* like marketing companies with television or self-help kiosk marketing in shopping centres which can display the visual identification data to make the public aware of the missing dependant.

- The identification data can also be distributed to the authorities dealing with un-identified bodies and can be used for positive identification

The process discussed above is an illustration of personal identification captured and tracking data linked to persons on the system assist with resolving information through management and distribution of data to linked sub-systems for resolving emergencies in the most efficient way.

Sub-systems

The previous section described the function of the *Central Management System* and the different modules. It also in several instances mentioned sub-systems. The importance of both sub-systems and the *Central Management System* are equal. They have no value if both are not present. The *Central Management System* implements the rules of the system and serves as a central repository of information which is used to assist persons using the system. The sub-systems on the other hand is the physical platforms implemented in the field with which persons will come in contact with.

Various functions can be performed on these sub-systems. They are divided into five different types to clearly define the function of each type. Although they are divided like indicated below, all five of these sub-system types can exist on a single platform and can provide all the functionality as described.

Sub-systems can be systems developed by the inventor or it could be systems developed by external companies that comply with the interface specifications as provided when integration is planned and performed.

Enrolment sub-system

The purpose of the enrolment sub-system is to capture user, guardian and dependant identification data and to securely store and upload the captured information to the C*entral Management System.*

Please keep in mind that an enrolment sub-system consists of certain core functionality. The core functionality is dependant on the functionality required. In certain instances the enrolment sub-system will be configured to perform biometric enrolment and in others it might be required to only link a person to certain assigned identification data like a child protection bracelet or to link a person's cell phone to him on the system for identification and tracking purposes.

The enrolment sub-system can be sub-divided into the following functionality:

Enrolment sub-system management

- Registration

  Before an enrolment platform can be utilised it needs to be registered through the *Sub-system Entity Management Module*. The registration assigns a unique identifier and certificates to the sub-system which would be used for communication.

  The sub-system cannot become operational without being registered on the system. Please refer to the *Sub-system Management* section.

- Configuration

  Each enrolment sub-system contains its own configuration. For example: If the enrolment sub-system support fingerprint enrolment then the configuration of the particular enrolment sub-system will be configured on the *Central Management System* using the *Enrolment Sub-system Configuration Interface*. This will allow the particular sub-system to communicate with the *Central Management System*.

  Configuration of the sub-system can only be done after sub-system registration and configuration of the sub-system needs to be performed before the sub-system become operational.

Please refer to the *Sub-system Management* section for further information.

Functionality

Any user, guardian or dependant that wants to access the system needs to be registered and enrolled before they can access the system. The *Enrolment sub-system* platform allows for this. The following describes the functionality pertaining to this:

Registration and management

The registration process involves adding the user to the *Central Management System*. This is a very secure process because of the fact that the system then assigns unique identity data to the person being enrolled.

The *Enrolment sub-system* provides an interface to register new users, guardians and dependants on the system. This functionality is always guided by a previously registered and enrolled user with the rights to access the particular sub-system. For security reasons this processes is normally performed online to allow the *Central Management System* to communicate online with the sub-system for issuing of registration id's and certificates.

In most cases the registration of a new person is done through a dual authorisation method. In cases where this is the case the new person will have to be registered on two different enrolment sub-system types and users. This enables double verification of data provided and makes it far more difficult for an entity to be registered incorrect or fraudulently. This is however configurable on the *Central Management System.*

The registration and management interface allows for registration data to be captured. The data needed for registration is controlled by the *Central Management System* depending on the type of registration. This corresponds with the messaging configuration done on the *Message Configuration Module* as well as the *Entity Management Module.* This information is stored on the enrolment sub-system in a profile to allow for off-line registration where permitted by the *Central Management System.*

Enrolment

Enrolment is the process of linking identification data to a person registered on the system. This data can be one or more of the following:

- Common characteristics
- Biometric characteristics
- Visual identification characteristics
- Assigned identification data

Please refer to the earlier definitions for more clarity.

Each enrolment sub-system can be configured to do different types of enrolments. Not all enrolment types are supported by all enrolment sub-systems and certain enrolment types takes priority or is required before another can be performed. This configuration is configured on the *Central Management System*. For example: A guardian might be required to first perform a biometric enrolment before the assignment of identification data. This might be required to enable biometric authentication of the guardian before assigning further identification characteristics to the guardian.

All enrolment data is stored against the person's record and is used throughout the system as required from time to time. It might be that enrolment performed on one sub-system is used on other sub-systems to avoid duplication. For example: If a child is enrolled at school for attendance purposes then there is no need to re-enrol the child for purposes of identification at the gym or for access to their home. This enrolment data performed at the school will then be used by other sub-systems to authenticate the child.

Data storage and communication

Operational modes

Different configurations exist for the way an enrolment sub-system operates. These operational modes are configured on the *Central Management System.*

The two main operational modes are online and offline. The configuration of the platform will dictate what operations can be performed by an enrolment sub-system in online and offline mode. Certain operations, like registration, will be configured to only be able to operate in online mode for security reasons.

Offline operation allow for capturing of data on portable platforms where online communications are not available. These transactions will be uploaded to the *Central Management System* in batch format.

Data storage and communication

Most data captured on the enrolment sub-system is stored in an encrypted format. Due to the sensitivity of the data, data is immediately encrypted, using the user and/or guardian certificate, and stored accordingly. This is required to ensure that there is no tampering with the data and is implemented to ultimately protect persons on the system.

In offline mode the data is stored on the system so that upload can be performed as soon as the system enters online operations.

The data stored on the system is divided into two different types. This first is data needed for synchronisation with the host and the other data is data that will remain on the system for local use. The *Central Management System* will always receive all the data captured on the enrolment sub-system. Certain sub-systems might provide additional functionality that requires that the data is captured for use on the sub-system group.

For example: A school might capture enrolment data for pupils of the school. This data can be used for identification for attendance purposes. Where several sub-systems exist within a sub-system group, like a school, the data would be captured for upload to the *Central Management System.* In most cases the data captured on a local sub-system in offline mode will not be usable until uploaded. Once the data is uploaded to the *Central Management System* it will be flagged for download to other sub-systems belonging to the same group and the local profile will be available on the sub-system that performed the enrolment. The reason for this data upload and download methodology is to ensure that a sub-system group can operate in an offline environment. All profiles stored on a local sub-system, like the profile stored on the sub-system performing the enrolment as well as profiles downloaded, will only be valid for a certain period. Once the profile expires it will have to be refreshed by communicating with the host. If the profile is not valid, due to updates or the fact that the person is removed from the system, then the local profile will be removed from the sub-system platform.

This methodology allows for offline operation and ensures regular communication with the host for synchronisation purposes.

Identification sub-systems

The purpose of identification sub-systems are to allow for transacting with previously captured identification data and to provide tracking information to a centralised system which in turn process and store the information according to pre-configured rules. This tracking data and the interpretation thereof provide the information used to assist and safeguard guardians and dependants registered on the system.

Identification types

Confirming claimed identity (Verification)

When it is known who the dependant or guardian is, the systems identification data can be used to confirm the claimed identity of the person. This can be done by entering claimed identity data and authenticating it against unique identity data like biometrics on one of the decentralised sub-systems or online with the centralised system.

Assigned electronic identification devices will also in some instances store unique biometric data that can be used for authenticating the bearer of the device. An example of this is radio frequency tags warn by a dependant used in conjunction with a pupil fingerprint authentication station to record school attendance or securely transacting with a biometric and radio frequency enabled ATM.

Locating a person who's identity is known

When a person who's identity is known needs to be located any, or a combination of identification data, can be used to locate the person.

For example, in the case where a dependant is separated from one of their guardians the guardian can raise an emergency declaring the dependant missing. The system can provide:

- Tracking information, consisting of information of where the dependant was last in contact with the system, such as GPS tracking, radio frequency tag or system transacting activity can be utilised to establish the location of the dependant.
- Visual identification data can instantly be transmitted to sub-systems to enable visual recognition of the dependant. Some examples of this is transmission of portrait, name and other visual identity information to sub-systems like shopping centre television advertising systems who can display the missing child or dependant information. It can also be integrated with police authority systems or conventional posters can be printed.

Actively monitoring a persons location who's identity is known

The system can be configured to actively monitor a person though assigned electronic identification device and automatically raise an emergency to notify the guardian once certain perimeter rules are violated.

A child can for example be the bearer of a GPS, radio frequency bracelet or cell phone which is configured by the guardian to raise an exception when the child leaves a certain perimeter, like a house, school or resort. A combination of rules, like perimeter definition, specified times and dates as well as notification method can be configured by the guardian to customise the system service.

Establishing an unknown persons identity

When the identity of a person is not known, a combination of all identification data is used to uniquely identify the person. This data is distributed to the authorities to assist for example with identification of unknown diseased persons.

The identification sub-system can be sub-divided into the following functionality:

Identification sub-system management

- Registration

  Before an identification platform can be utilised it needs to be registered through the *Sub-system Entity Management Module*. The registration assigns a unique identifier and certificates to the sub-system which would be used for communication.

  The sub-system cannot become operational without being registered on the system. Please refer to the *Sub-system Management* section.

- Configuration

  Each identification sub-system contains its own configuration. For example: If the identification sub-system support fingerprint identification then the configuration of the particular identification sub-system will be configured on the *Central Management System* using the *Identification Sub-system Configuration Interface*. This will allow the particular sub-system to communicate with the *Central Management System*.

  Configuration of the sub-system can only be done after sub-system registration and configuration of the sub-system needs to be performed before the sub-system become operational.

Please refer to the *Sub-system Management* section for further information.

Functionality

Any user, guardian or dependant that wants to access the system needs to be registered and enrolled before they can access the system. The *Enrolment sub-system* platform allows for this. The following describes the functionality pertaining to this:

Identification

Identification is the process of establishing or confirming a person's identity who is registered and enrolled on the system. Various different identification data can be linked to a person. The linking of identification data against a person is done through one or many enrolment sub-systems. Please refer to the earlier definitions of identification data for more clarity.

Each identification sub-system can be configured to do different types of identification. Not all identification types are supported by all identification sub-systems.

An example of an identification system is a platform located at a school. This platform can be used to identify a child by means of fingerprint to record attendance of the child. This same platform might be used to identify a parent collecting his/her child from the school. Another example of an identification sub-system is a radio frequency enabled identification sub-system that recognises radio frequency tags that comes in the vicinity of the platform. The particular radio frequency tags will be assigned to a person through an enrolment sub-system platform. When the identification platform detects a tag it will match it to the carrier of the tag.

Data storage and communication

As mentioned before – the purpose of an identification sub-system is to first of all identify a person by comparing enrolled and linked identification to data captured or detected by the identification sub-system. Secondly this information is stored and forwarded to the *Central Management System* which uses it as tracking data and protect the persons on the system by applying rules to the data received in order to ensure that the person is save or to detect if an emergency should be raised.

Operational modes

Different configurations exist for the way an identification sub-system operates. These operational modes are configured on the *Central Management System* in the same fashion as an enrolment sub-system.

The two main operational modes are online and offline. The configuration of the platform will dictate what operations can be performed by an enrolment sub-system in online and offline mode. Certain operations will be configured to only be able to operate in online mode. Performing online identification would be practical in certain scenarios as the sub-system is not required to store data locally as it is directly connected to the *Central Management System* who will link the enrolled identification data against the data captured by the identification sub-system.

Offline operation allow for performing identification without being connected to the *Central Management System.* This might be more practical and cost effective in certain scenarios as it does not require a permanent connection to *Central Management System.* In these cases the identification sub-system will store the applicable sub-set of identification data locally of persons that can be identified on it. An offline identification sub-system will be required to connect to the *Central Management System* on regular intervals to ensure that it is up to date with the latest identification data on the central system. Data stored on the sub-system will only be valid for a certain period before it will be required to be refreshed by the *Central Management System* before use of the identification data can continue.

Data storage and communication

In the case of offline operation the data stored on the identification sub-system will be in an encrypted format. This is required to ensure that there is no tampering with the data and is implemented to ultimately protect persons on the system.

In offline mode the tracking data generated from performing identification is stored on the system so that upload can be performed as soon as the system enters online operations.

The data stored on the system is divided into two different types. This first is data needed for synchronisation with the host and the other data is data that will remain on the system for local use. The data stored for synchronisation with the host is the tracking data that is stored to record an identification that happened at a specific time by a specific person.

For example: A school might capture identification data for pupil of the school. This data can is recorded for attendance purposes. In this case the sub-system group, belonging to the school, will store identification data of pupils and parents that need to be identified. The identification sub-system will perform identification of pupils and parents in offline mode but would store packets of encrypted data that indicates when a person was identified. When the system goes online it will send this data to the *Central Management System* that will store the data centrally for processing and access.

Emergency sub-systems

The purposes of an emergency sub-system can be to report an emergency or it could exist to deal with an emergency. These types of sub-systems can co-exist with another sub-system but is defined separately to describe its particular functionality.

These types of sub-systems normally operate in online mode due to the nature of its functionality.

Herewith a description of the functionality:

Reporting emergencies

When an emergency occur it can either be triggered by certain data defining an emergency on the *Central Management System* or it can be initiated by a user, guardian or dependant.

Emergency sub-systems allow one of these entities to declare an emergency as discussed under the section *Emergency Management*.

The following are different samples of Emergency sub-systems:

- A software package used by a call or contact centre operator that accept calls to assist persons on the system. If a guardian or dependant contacts the call centre then the operator will be able to record or update emergency data on the *Central Management System* using this type of sub-system.
- A guardian or dependant can be the carrier of a device that triggers an emergency. This could be linked to an emergency sub-system linking directly to the *Central Management System* or if it is an externally managed system it could be linked through an *External message transport system* which would serve as the link between the external system and the *Central Management System.* When the guardian or dependant triggers the emergency button the emergency sub-system will receive a distress signal and the data would be communicated to the *Central Management System.* These types of devices can also possibly measure vital signs and automatically trigger an emergency without the bearer's intervention.
- A guardian or dependant can have access to an emergency sub-system which will allow them to sign onto the system and declare an emergency. These types of systems can be accessible through the internet or could be supplied by co-operating businesses like shopping centres, resorts and many more.

Dealing with emergencies

These types of systems focus on management and resolving emergency situations. There are many sophisticated currently implemented to deal with emergency situation. Some of them include:

- Policing systems dealing with missing persons
- Police emergency response units and their related systems
- Emergency response companies dealing with various categories like accident and medical emergencies and fire brigade response units.
- Interpol
- National disaster management systems

Certain companies are obligated to have their own emergency management systems to ensure the safety of their employees. Mining companies is a good example of this.

These current systems can be linked to the *Central Management System* through *External message transport sub-systems* which will leave them functioning as they are currently but will provide a bi-directional interface to the *Central Management System* that will allow for sharing of data between the different systems to ultimately add value to the protection services provided currently to persons on these systems.
In addition to these existing emergency systems platforms a whole new array of platforms can be integrated to form part of the emergency sub-system solution. The following are some of examples:

- Online distribution of missing child information to shopping centre kiosks and electronic marketing media to immediately alert al shoppers of a child who is missing
- Distribution of a full personal profile to the police services that can include fingerprint and visual verification characteristics
- Temporary bracelets provided for child protection when visiting a resort or shopping centre to ensure the child remains within a certain perimeter and can be monitored by the parent with ease

In all the above mentioned scenarios the *Central Management System* orchestrates emergency information provided by emergency sub-systems to assist management of emergency situations in the most efficient way.

External message transport sub-system

This interface provides an open interface for integration of external enrolment, identification and emergency sub-systems to be integrated into the *Central Management System*. This enables current technology solutions to add value to the system and to provide a holistic guardian and dependant identification and tracking view. Through this platform this can be achieved without compromising or changing the current system.

Developers of this type of sub-systems normally develop this platform to integrate seamlessly with external systems that can benefit from integration with the *Central Management System* or which can add value or data to the central system.

Although the integration interface is an open system, new integrators have to fulfil certain security and cryptography requirements for integration and certification to ensure the integrity of the system.

Referring to figure 6, the diagram illustrates how this platform will operate:

As illustrated above, the *External Message Transport Sub-system* will consist of two clearly defined sections. The one section communicates with the *Central Management System* through the interface discussed above and the purpose of the other is to communicate with the external system. Therefore this platform serves as a bridge between the two systems and might even store data on the platform for distribution to the recipient system.

- Standardised Central Management System Message Interface

  This part of the *External Message Transport Sub-system* is designed to interface with the *Central Management System* in the standard way through messages defined and configured on the system.

  This can be done through use of interface specification provided from the *Central Management System* defining the messages that can be used.

- Customised External Interface Code

  This code is developed in accordance with the interface provided from the external sub-systems.

Data access sub-systems

The purpose of data access sub-systems is to access the data stored on the *Central Management System.* This is typically used by persons on the system for reporting purposes or to check the status of any of the processes within the system.

This type of sub-system normally connects through the internet and web portal. This is not a core part of the invention as it is mainly used for reporting and not for core functions of the system. For this reason this is not documented in this document.

Example of implementation of invention

The invention relates to a system that will securely transfer data electronically between systems. The data to be transferred electronically relates to data of a personal and or critical nature that could be applied to locate and or identify children who may or may not find themselves in a possible vulnerable or dangerous situation. In addition the invention will enable the identification of the enrolled child's guardian. Signals are securely transmitted from a transmitter device to a central server which will intelligently process the data. Depending on the nature of the data transmitted to the central server, appropriate decisions will be made (either artificially or by human intervention) to take appropriate action. The action can include interfacing with other systems in order to locate and or identify the child whose transmitter sent the received signal.

2.1. Enrolment process

Refer to diagram 1 as part of the description below.

A guardian takes their child or children to an enrolment station or service station (1). The service station can be at a participating shopping centre like a Pick 'n Pay or a school, community centre or the like.

The enrolment operator (2) will capture the guardian's (3) personal information including biometrics details. The guardian will be enrolled by capturing his/her fingerprints, facial portrait, a verification voice sentence, iris patterns, and electronic signature using the biometric devices (4, 5, 6, 7, and 8). In addition to the guardian's biometrics data, required demographic data like name, surname, identification number, and contact details are captured.

Before successfully completing the guardian enrolment process, the invention caters for the enrolment station to establish a secure connection (9) with the central server in order to communicate with the central server in order to authorise the enrolment. The enrolment station will send an encrypted message to the central server in order to establish a secure connection to the central server. After receiving the encrypted message and the central server will decode the message and verify that the message is legitimate. If the message is found as legitimate, the central server will process it accordingly. (10) That is, the message will contain a message type that will indicate the type of message the enrolment station sent. The central server will create a unique identification number that will be valid for the period of communication between the central server and enrolment station for the present communication process only. The central server will send an appropriate encrypted reply back to the enrolment station indicating whether communication can continue or not.

(11) After receiving and decoding the received message, the enrolment station will compile an encrypted message containing the person's enrolment data and send it to the central server. After receiving the encrypted message, the central server will process the message accordingly and process the message appropriately. The central server will check whether the person has already been enrolled. If not, the enrolment will continue and a unique reference number will be created that will link the person to the system. An appropriate message will be compiled by the central server, encrypted and send to the enrolment station.

(12) After receiving the encrypted message the enrolment station will perform the appropriate actions. If the guardian enrolment was successful, the next step (13) in the enrolment process can follow.

The guardian's child (15) or children is enrolled onto the system. The child's personal information including biometric details is captured onto the system. The child will be enrolled by capturing his/her fingerprints, facial portrait, a verification voice sentence, and iris patterns. In addition to the child's biometrics data using biometrics devices (4, 5, 6, and 7), required demographic data like name, surname, identification number are captured. The system will now follow step (11) again to perform child enrolment. In addition, the enrolment data will contain data on the transmitter and receiver (14) that the child will carry to uniquely locate and or identify him/her. A child will be linked to one or more enrolled guardian.

If the child enrolment is successful the next process can take place.

2.2. *Activating the child transmitter and receiver*

Refer to diagram 2 as part of the description below.

The transmitter and receiver (1) has to link uniquely to the enrolled child (2). In order to transfer required data to the transmitter and receiver the enrolment station will securely connect to the central server (3) by sending an encrypted message to the central server. After receiving the encrypted message, the central server will process the message appropriately. After establishing that the message is legitimate the central server will send back an encrypted message to the enrolment station to indicate whether communication can continue or not. The central server will create a unique identification number that will be valid for the period of communication between the central server and enrolment station for the present communication process only. The enrolment station will process the reply message accordingly. Depending on the reply from the central server the enrolment station will send an encrypted message (4) to central server indicating that the child's data has got to be send to the child's transmitter and receiver device in order to activate and uniquely link it to the child. The message will contain the unique identification number of the transmitter and receiver that will be assigned to the child as well as the unique details of the enrolled child that have to be send to the transmitter and receiver device. The central server will process the message appropriately. If the message is a legitimate request the central server will establish a secure connection (5) with the child's transmitter and receiver using the available communication mediums (e.g. satellite, GPRS, cellular networks)

The transmitter and receiver will accept the encrypted message from the central server and process it accordingly. After the transmitter and receiver devices has processed the message an encrypted reply message (9) will be send to the central server in order to indicate the status of the transmitter and receiver device. The central server will process the encrypted message accordingly and send an appropriate encrypted reply message (10) back to the enrolment station. The enrolment station will process the encrypted reply message accordingly and provide feedback to the enrolment operator (6), guardian (7) and child (2).

Part of the data (e.g. perimeter coordinates that a child can move within) that is send to the child's transmitter and receiver can be modified by the guardian or other authorised system user by using a personal computer (8) to use the Web interface provided by the central server. A secure message will be send to the child's transmitter and receiver by the central server. The transmitter and receiver will process the encrypted message (11) appropriately and update the perimeter coordinates, and send back an encrypted reply message indicating the result of the request.

2.3. Locating and or identifying a child

Refer to diagram 3 as part of the description below.

The child's (1) transmitter and receiver (2) allows for transmitting its current location. This functionality enables the service provider (3) of the child tracking and identification system to locate a child at any point in time at any place using the GPS (4).

Should a child go missing, or find him/her in another potential vulnerable or dangerous situation the child can send a distress signal using the transmitter and receiver to the central server (5). Alternatively, if the child moves outside of the set perimeter, an automatic alarm signal can be send to the central server. The central server will process the message accordingly and inform the required service provider operator (6) who will act accordingly. The service provider operator will act appropriately and if required inform authorities (7) and the child's guardian (8).

The service provider operator can immediately locate the child by requesting the GPS coordinates of the child's transmitter and receiver. Furthermore, the child's personal and critical information is available from the central server which can be used to compile an identification kit (9) to be used by authorities in locating the child.

The identification kit can also be shared with communication media such as television broadcasting station, internet sites, and radio broadcasting stations to assist in locating the child.

Alternatively, the invention can be used to accurately identify a child. Should authorities like to establish the identity of a child, the invention caters for the interrogation of the central server by passing unique data of the child. The service station (12) will establish a secure connection to the central server by sending an encrypted message (11) to the central server. The central server processes the encrypted message accordingly. If the message is a legitimate message a encrypted reply message is send to the service station. The central server will create a unique identification number that will be valid for the period of communication between the central server and service station for the present communication process only. The child's biometric data (10) is passed to the central server via an encrypted message. The central server processes the encrypted message accordingly and performs identification or verification (13) processes on the received data. When the identification/verification process is complete, the central server compiles an appropriate encrypted reply message and sends it back to the service station. Depending on the reply message, the authorities take the appropriate action.

2.4. Interfacing with external parties (systems)

External parties such as Interpol or the local police service could find information stored on the central server very helpful in locating and or identifying a missing child. The central server can allow the sharing of data with authorised external systems.

The invention is adapted to be applied in a number of applications, for example, missing person (ages 2 years to adult). An example of an existing problem is that a parent takes along a son to a shopping mall. While in the mall he gets into a shop, he gets distracted, leaving the child to wander in the shop. Five minutes or so later he realizes the child is no longer in the shop. While he's looking out for the child he sees the guards and explains what happened and they start all looking within the mall and 30 minutes later it's all history. They then resort to call the police and the search continues and a docket of missing child is then opened.

1750 children go missing from South Africa every year and only 10% of them are found. Would South Africa not be a beautiful country if 98% of these children are found? South Africa's kidnapping stats have increased by 6% from the previous year.

The present invention provides a technology to track humankind, and the control centre of the technology is in a position to pick up the child's vital signs of fright/fear/screaming or any other sense of emotional reaction that a child might use in a situation of being abducted. The control centre after noticing those signs then contacts both parents/relatives/partners/siblings or those put on the system in case of emergency , and the process continues that the contact people on the system in order of priority are first contacted on their mobiles and if this fails to elicit response after being tried for the second time, a task team will be sent, following GPS co-ordinates pin pointing the exact location, reducing searching time and retrieving the child to safety within a short period of time.

Another example of an application of the invention is in overcrowded jails. A man is accused of minor crime and is then a suspect and he's put in an over crowded cell. A jail cell in South Africa is meant to accommodate 3 inmates, where now it accommodates 15 to 28 prisoners at a time. Awaiting prisoners are raped, infected by HIV/ AIDS, taught new ways of committing crime while waiting for the Justice System to clear them. Would tagging this man and monitoring of him from home not be a relief to the tax payers, while at the same time it would reducing the over crowding in jails and also destroying the criminal schooling happening in jails. The invention provides to Correctional Services in South Africa technology it can use to tag these awaiting trial criminals and use to monitor and trace while awaiting trial from their homes, until such time for the court hearing. This would help the correctional Services reduce the number captives in jail, saving running costs and also saving the country from petty criminals who after being arrested learn a lot more from their inmates.

Another example arises with parents, after wanting a child for a long time, a mother gives birth to a beautiful baby boy, a child she and the father had long been waiting for. While the mother is still in hospital she is told the baby is missing. Most Hospital tags only work within a certain set radius of the hospital area and about 12% of these babies still get missing because of the inefficiency of systems outside the hospital premises. According to the invention if the child is tagged, and goes missing, the technology control centre picks up the child the minutes the baby goes beyond the set boundaries, there would be an alerting message immediately to the people responsible for security and still be in a position to trace and reflect the exact location of the missing child.

Illegal immigrants who have been deported and still persist to come back into the country. Technology according to the invention can be a position to trigger and alert the responsible authorities of the person trying to come back into the country and check his/her legitimacy of being back in the country.

A person is hijacked, then panics and tries to defend himself and he's murdered and put in the boot to be dumped somewhere. Integration of technology according to the invention can come handy here, where in a situation of a hijack you can freely allow the hijacker to take the car and everything they want and use a tag/technology to alert the likes of Netstar*, Tracker* etc of the vehicle being stolen and this should reduce number of deaths immediately recover stolen cars within minutes. (*trademark).

Deep under ground in the mining side of one of South Africans biggest gold producers, an explosion has buried many men alive. They have very little air to live from but as their rescue team keeps digging at the wrong sides, they run out of air and die. During the explosion, which happens beyond everybody's control, all under mine people could be affected by the explosion and at the time of rescuing it becomes difficult cause of failing to trace the bodies affected, technology of the invention can be used with specialised radio equipment to do a quick search and quick response to increase chances of people, as they would have been tagged and thus preventing more disaster.

Bank identification of people is becoming urgent with the current way of using personal information of things like signatures and ID's which are not enough to verify the people's identity. The banks are currently using a FISCA method, which has its own limitations. With the biometric technology of the invention it would be easier and secure to give a 100% identity check.

Peace keeping soldiers who can never be traced, when sent out on a mission for whatever reason, a lot of times are not recovered should anything happen at them. With a technology tracking device according to the invention this situation can be avoided and thus having a lot of soldiers being recovered, when sent out on a mission also being able to assess the health condition while out there.

Patients with heart problem and strokes can be helped with the invention. 18% of South Africans diabetic patients die from unforeseen heart attacks ever year. With technology according to the invention that can read vital signs the patients with heart ailment could be rescued within a reasonable time during the heart attack and also tell his exact location.

CLAIMS

1. A method that will securely transfer data electronically between systems, the data to be transferred electronically relating to data of a personal and or critical nature that could be applied to locate and or identify children and others who may or may not find themselves in a possible vulnerable or dangerous situation, with enablement of the identification of the child's guardian or other contact, in which the signals are securely transmitted from a transmitter device to a central server which will intelligently process the data and depending on the nature of the data transmitted to the central server, appropriate decisions will be made (either artificially or by human intervention) to take appropriate action, which can include interfacing with other systems in order to locate and or identify the child or person whose transmitter sent the received signal.

2. A method as claimed in claim 1, which includes the steps of enrolment of children and their guardians or others.

3. A method as claimed in either one of claims 1 or 2, which includes acquiring and loading on the database one or more selected from global positioning coordinates (GPC) that are acquired from the Global Positioning System (GPS), a child's or person's vital bodily signals including monitoring the heart rate and respiratory functions, biometric data including fingerprints, retinal scan, voice recognition or facial recognition and other personal information which includes information that will assist in uniquely identifying a child or person when required, including but not limited to an Identification Number, name, surname or birth date.

4. A method as claimed in any one of claims 1 to 3, in which the biometric data is extended to the child's or person's guardian to be used to be identified when required.

5. A method as claimed in any one of claims 1 to 4, in which the method includes allocating a unique identification number to uniquely identify the child or person on the system.

6. A method as claimed in any one of claims 1 to 5, in which the step is added of registration or enrolment involving adding a new entity to the system, including sub-systems, users, guardians and/or dependants.

7. A method as claimed in claim 6, in which these entities are registered on the system before obtaining access to the system, including the assignment of a unique identifier and certification to the entity which is used in the lifecycle of the system to ensure system integrity and ability to be audited.

8. A method as claimed in either one of claims 6 or 7, in which users include a person registered on the system to perform system functions, including registration and enrolment of guardians and dependants on the system as well as system configuration.

9. A method as claimed in any one of claims 6 to 8, in which the system relation between guardians and dependants is defined as a many to many relation, which allows various guardians to be assigned to a dependant like parents, school teachers and care takers, the relations being clearly identified on the system and configurable rules implemented when the dependant is under the protection of a particular guardian at a particular time, so that many dependants can be assigned to a particular guardian.

10. A method as claimed in claim 9, in which a potential guardian is also enrolled on the system even if there is no current dependant under its protection.

11. A method as claimed in any one of claims 6 to 10, in which the guardian requesting the dependant to be registered and enrolled on the system is defined as the primary guardian.

12. A method as claimed in any one of claims 1 to 11, in which visual identification characteristics are added to the database and are used to visually verify a person and rely on a human to visually compare them to confirm an identity.

13. A method as claimed in any one of claims 1 to 12, in which assigned identification data consisting of an identifier assigned to a person to assist with identification are stored on an electronic device selected from one or more of a cell phone, global positioning system, radio frequency tag, card or chip carried by the entity to be identified.

14. A method as claimed in claim 9, in which assigned identification data is combined with biometric and/or visual identification characteristics and the device securely attached to the carrier.

15. A method as claimed in any one of claims 1 to 14, in which establishing an unknown persons identity, confirming the identity of a person that claims to be someone and/or locating a person with the use of previously captured identification data is performed by the steps of filtering a combination of common characteristics that cannot on their own provide unique identification of a person, including a person's names, eye colour, height and birth date.

16. A method as claimed in claim 15, in which are added steps of identifying biometric characteristics, which are measurable, physical or personal behavioural traits belonging to a specific person, including voice, fingerprint, palm, facial, vein and DNA, processed into binary data.

17. A method as herein described.

18. Apparatus that will securely transfer data electronically between systems, the data to be transferred electronically relating to data of a personal and or critical nature that could be applied to locate and or identify children and others who may or may not find themselves in a possible vulnerable or dangerous situation, with enablement of the identification of the child's guardian or other contact, in which the signals are securely transmitted from a transmitter device to a central server which will intelligently process the data and depending on the nature of the data transmitted to the central server, appropriate decisions will be made (either artificially or by human intervention) to take appropriate action, which can include interfacing with other systems in order to locate and or identify the child or person whose transmitter sent the received signal.

19. Apparatus as claimed in claim 18, in which the transmitter and receiver devices are those devices that will allow for the locating of children, for the storage of electronic data that can be used to uniquely identify the carrier thereof.

20. Apparatus as claimed in either one of claims 18 or 19, in which the transmitter and receiver device is a small electronic chip that can be implanted underneath a child's or person's skin for a long period of time, or alternatively can be worn as a bracelet around the wrist, neck, or ankle etc. for only a specified period of time.

21. Apparatus as claimed in any one of claims 18 to 20, in which the transmitter and receiver functionality includes the ability to run basic software to only transmit its location or alternatively enable two way voice communications, fingerprint technology by embedding a fingerprint scanner onto the device, GPS functionality

to track the carrier thereof, sending distress signals, monitoring bodily vital signals and/or storing personal information that can be used to identify the carrier thereof.

22. Apparatus as claimed in any one of claims 18 to 21, in which communication mediums allow for communication between the various components of the invention and enable the transmitting of electronic data between devices and include satellites orbiting earth and cellular networks.

23. Apparatus as claimed in any one of claims 18 to 22, which includes a central server used to govern secure communication between systems, the central server receiving and storing the personal and critical information of children and their guardians or persons, programmed to relay critical information to authorities.

24. Apparatus as claimed in claim 23, in which the central server will also provide for an interface where authorised users can access personal or critical data.

25. Apparatus as claimed in any one of claims 18 to 24, which allows for external systems to securely interface with the central server in order to transfer data to and from the central server and or external system, the external system running specialised applications in order to enable secure communications between the systems.

26. Apparatus as claimed in any one of claims 18 to 26, in which the system consists of a secure central system that provides an open interface that allows for integration of various technologies as well as several tightly integrated decentralised components or sub-systems to provide assistance and safeguarding for persons on the system, in a unique way.

27. Apparatus as claimed in any one of claims 18 to 26, which further provides apparatus that manages identification and tracking data of guardians and the dependants or persons under their protection, the identification data captured being configurable and adaptable to allow for incorporation of new identification characteristics and methods as well as tracking technologies as they become available.

28. Apparatus as claimed in any one of claims 18 to 27, which includes an enrolment service centre that could be a temporary, mobile, or fixed location where guardians of children who wish to register their children and themselves on the child or person locating and identification system, the enrolment station able to

securely connect to a central server where required data is stored in order to allow for effective and immediate action when required.

29. Apparatus as claimed in claim 28, in which the enrolment station enables communication with the transmitter and receiver device that is uniquely assigned to a child, the enrolment station able to securely write required data to the child's or person's assigned transmitter/receiver in order to enable accurate identification of the child.

30. Apparatus as claimed in any one of claims 18 to 29, which includes sub-systems or platforms that are registered and link to a core system and consist of hardware whose functionality is defined by software components, the sub-systems including enrolment or identification systems that collect and transmit identification data to the core system and third-party or external systems.

31. Apparatus as claimed in any one of claims 18 to 30, which includes biometric devices including fingerprint scanners, retinal scanners, voice recorders, camera, and signature pads that will be used to capture the biometric data of children and their guardians or persons.

32. Apparatus that will securely transfer data electronically between systems as herein described and as illustrated in the drawings.

DATED THIS 2ND DAY OF APRIL 2007

Berndt

-----------000-----------

FIG. 1

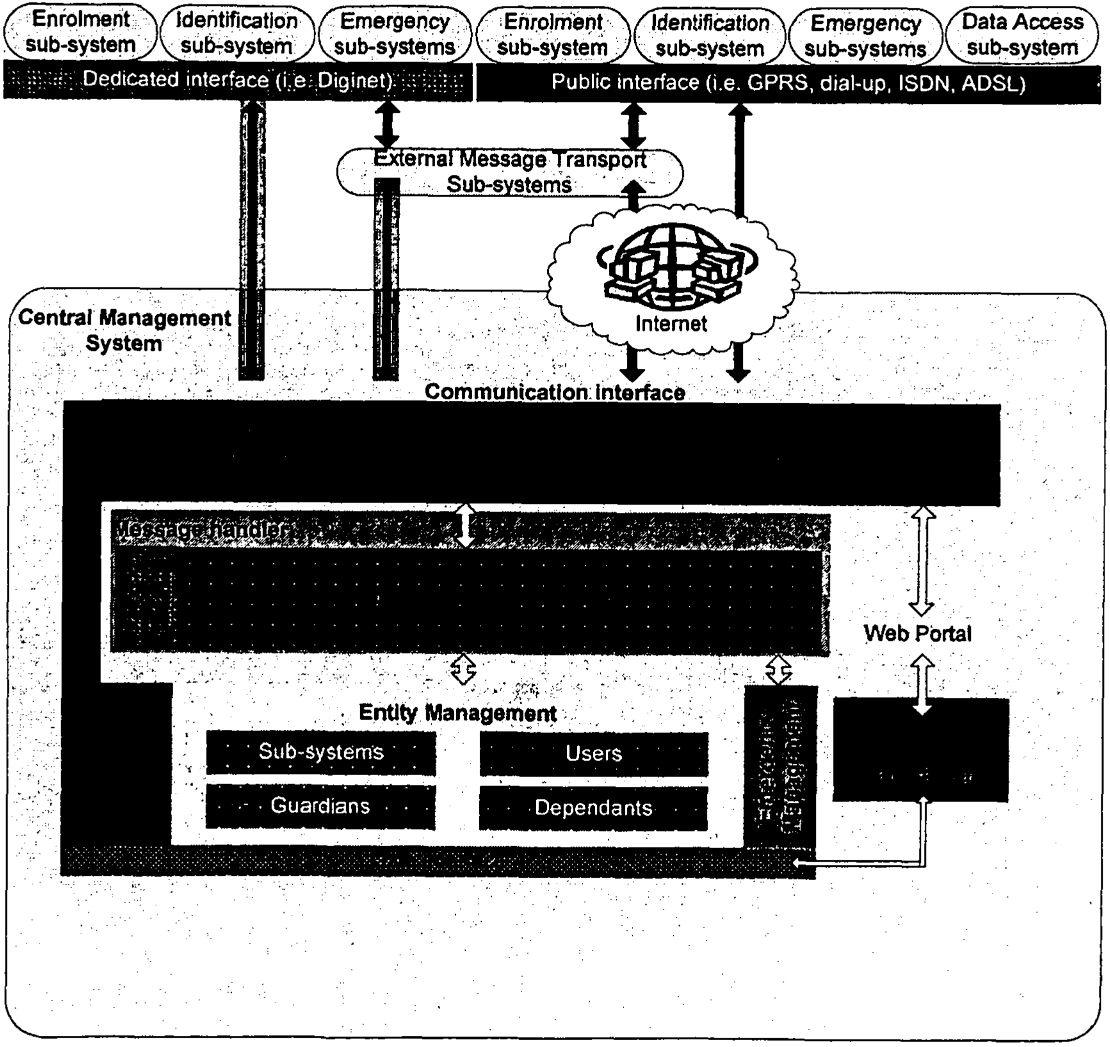
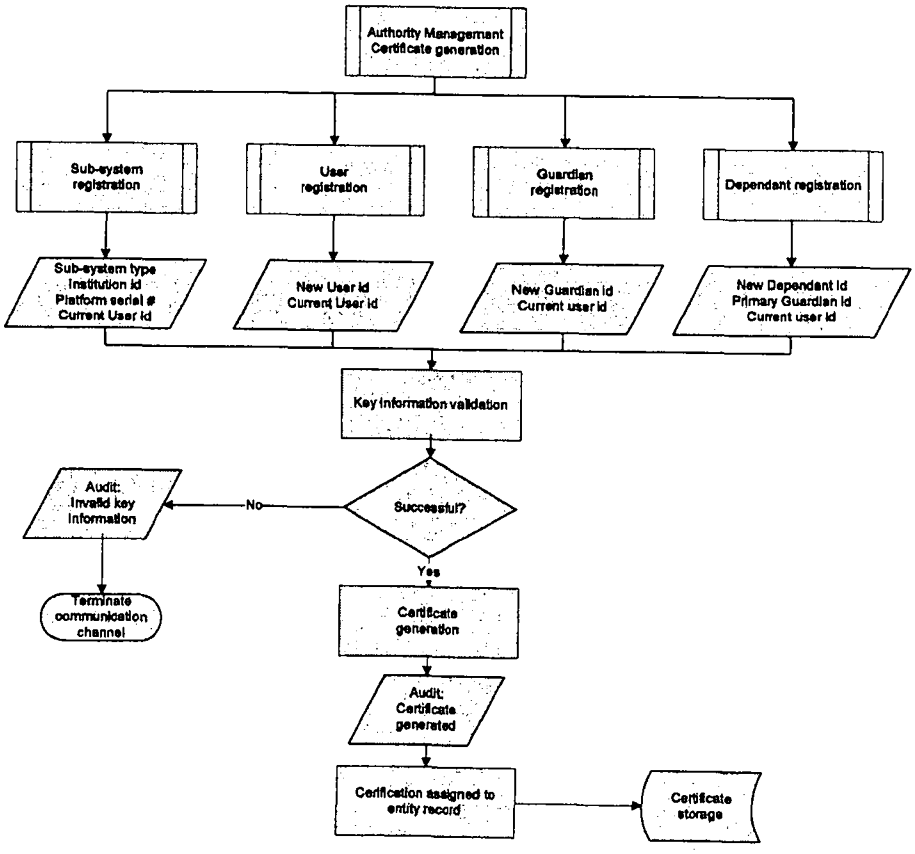
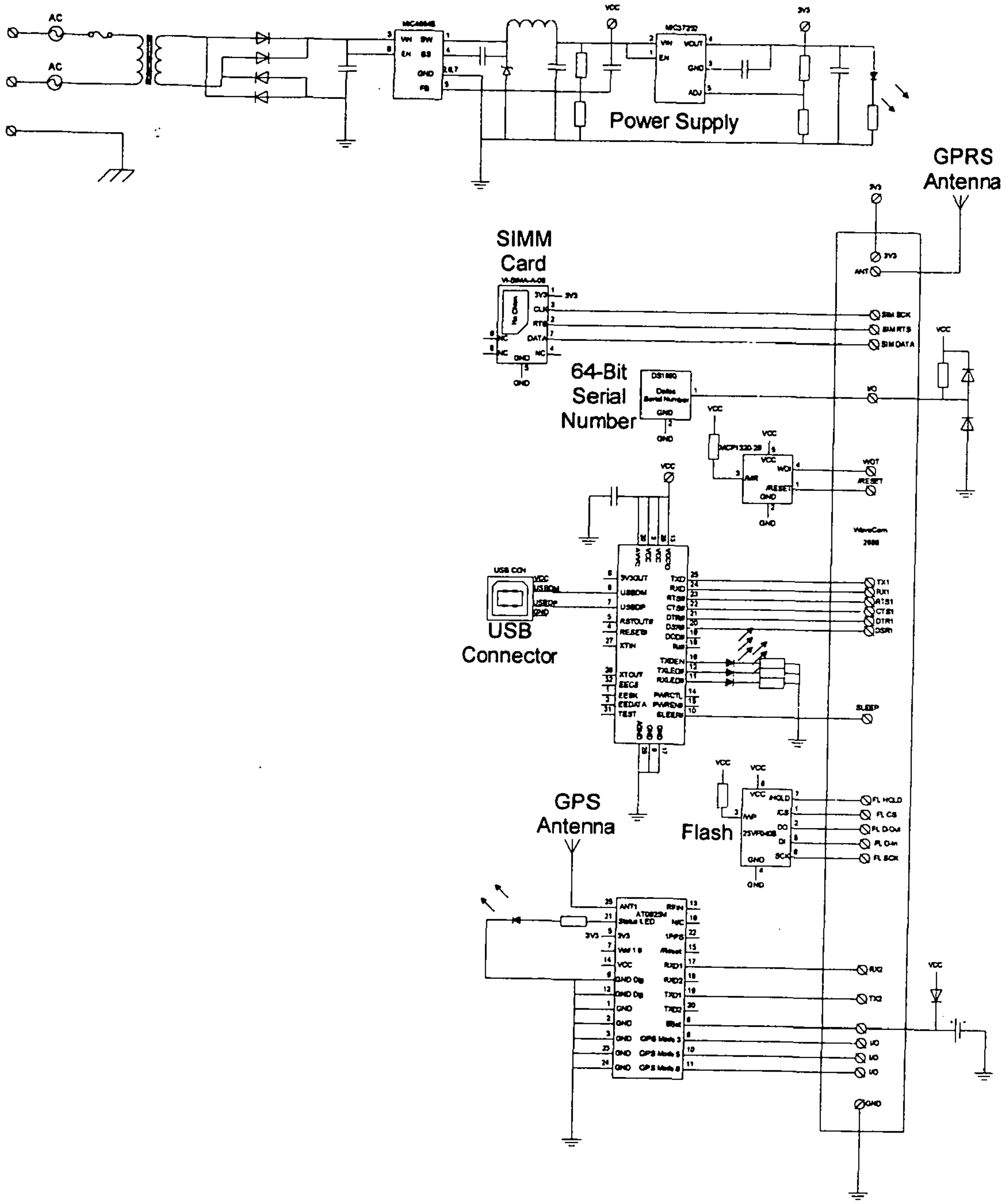

Enrolment sub-system
Identification sub-system
Emergency sub-systems
Enrolment sub-system
Identification sub-system
Emergency sub-systems
Data Access sub-system
Dedicated interface (i.e. Diginet)
Public interface (i.e. GPRS, dial-up, ISDN, ADSL)
External Message Transport Sub-systems
Internet
Central Management System
Communication Interface
Message handler
Web Portal
Entity Management
Sub-systems
Users
Guardians
Dependants

FIG 2


Authority Management Certificate generation
Sub-system registration
User registration
Guardian registration
Dependant registration
Sub-system type Institution Id Platform serial # Current User Id
New User Id Current User Id
New Guardian Id Current user Id
New Dependant Id Primary Guardian Id Current user Id
Key information validation
Successful?
No
Audit: Invalid key information
Terminate communication channel
Yes
Certificate generation
Audit: Certificate generated
Certification assigned to entity record
Certificate storage

Berndt

FIG 3



Bennett

FIG 4

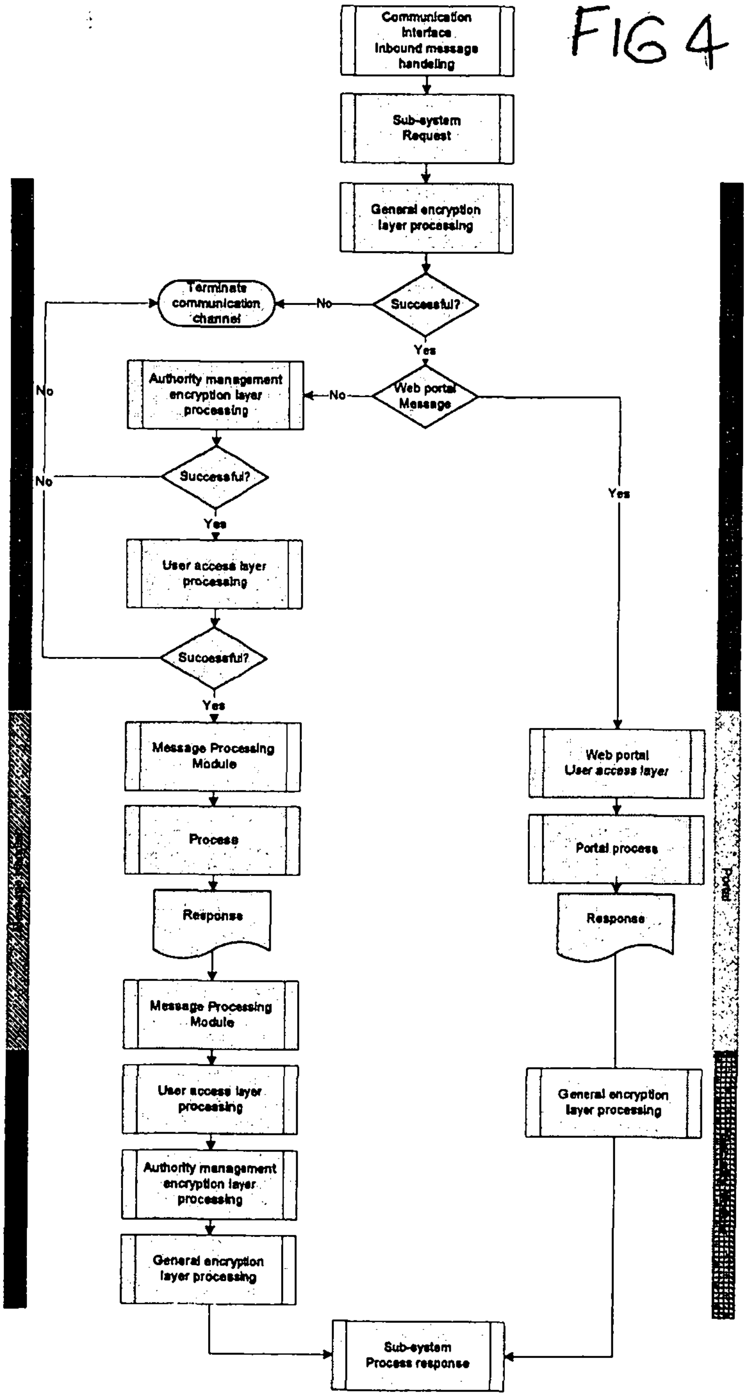
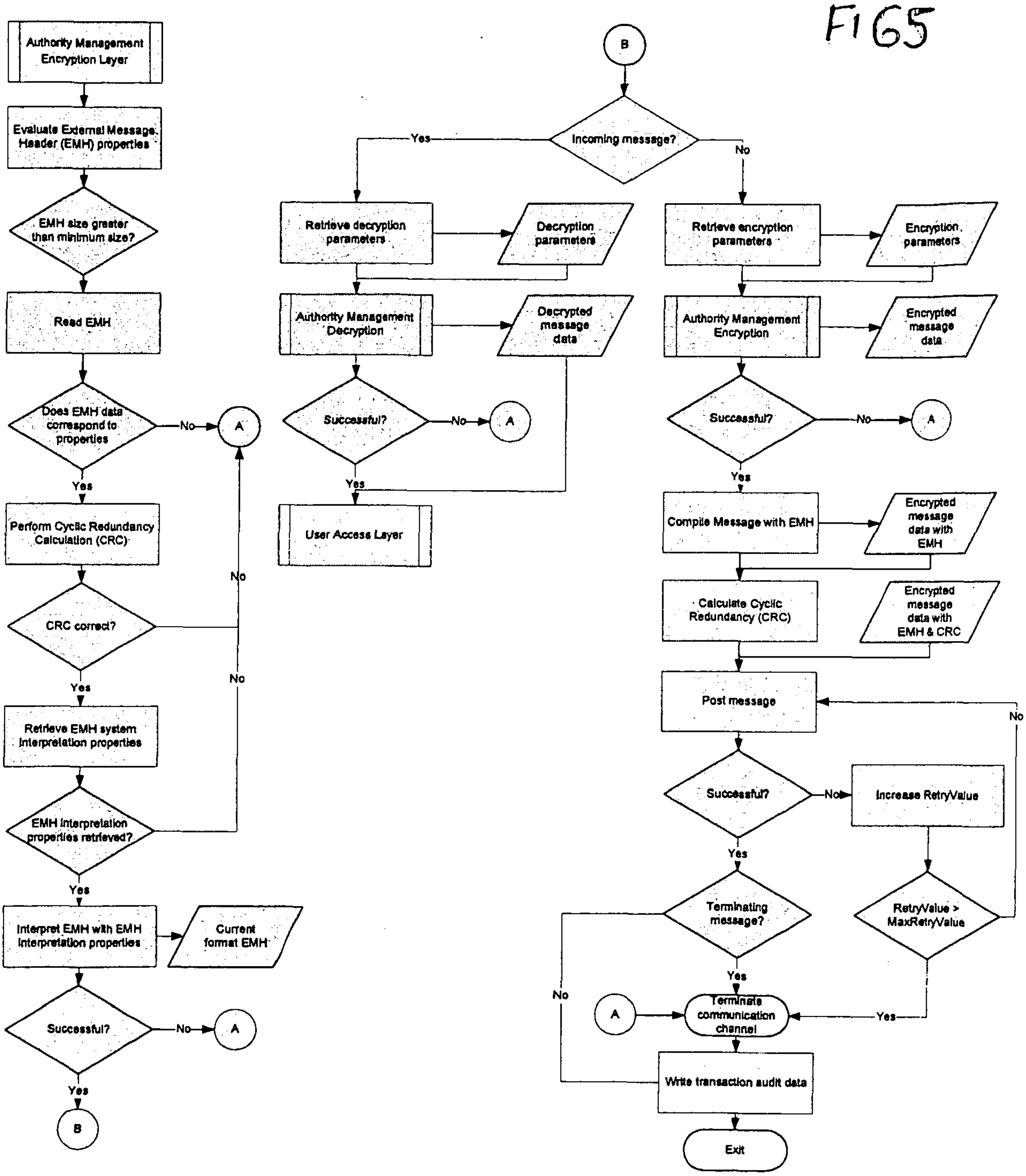
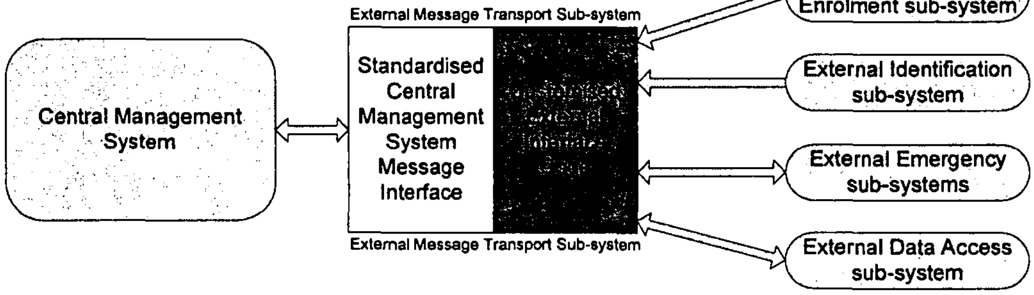

Communication Interface Inbound message handeling
Sub-system Request
General encryption layer processing
Successful?
No
Terminate communication channel
Yes
Web portal Message
No
Authority management encryption layer processing
No
Successful?
No
Yes
User access layer processing
Successful?
Yes
Message Processing Module
Process
Response
Message Processing Module
User access layer processing
Authority management encryption layer processing
General encryption layer processing
Yes
Web portal User access layer
Portal process
Response
General encryption layer processing
Sub-system Process response
Portal

FIG5


Authority Management Encryption Layer
Evaluate External Message Header (EMH) properties
EMH size greater than minimum size?
Read EMH
Does EMH data correspond to properties
No
A
Yes
Perform Cyclic Redundancy Calculation (CRC)
No
CRC correct?
Yes
No
Retrieve EMH system interpretation properties
EMH interpretation properties retrieved?
Yes
Interpret EMH with EMH interpretation properties
Current format EMH
Successful?
No
A
Yes
B
B
Incoming message?
Yes
No
Retrieve decryption parameters
Decryption parameters
Authority Management Decryption
Decrypted message data
Successful?
No
A
Yes
User Access Layer
Retrieve encryption parameters
Encryption parameters
Authority Management Encryption
Encrypted message data
Successful?
No
A
Yes
Compile Message with EMH
Encrypted message data with EMH
Calculate Cyclic Redundancy (CRC)
Encrypted message data with EMH & CRC
Post message
No
Successful?
No
Increase RetryValue
Yes
Terminating message?
RetryValue > MaxRetryValue
No
Yes
A
Terminate communication channel
Yes
Write transaction audit data
Exit

UBerndt

FIG 6


External Message Transport Sub-system
Central Management System
Standardised Central Management System Message Interface
Customised External Interface Layer
External Enrolment sub-system
External Identification sub-system
External Emergency sub-systems
External Data Access sub-system
External Message Transport Sub-system

Berndt