Connected Mobile Health Devices: A Reference Architecture

Version 1.0
January 2011

Security Classification – NON CONFIDENTIAL WHITE PAPER

Copyright Notice

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction

Governments and Healthcare providers are facing rising demand for services at a time when spending on healthcare is under pressure and there are limited resources to provide care. The way that healthcare systems are being implemented is having to be rethought and steered back onto a sustainable path. One of the approaches that are being advocated is the use of mobile devices for the remote monitoring of chronic diseases including diabetes and COPD.

Within this report the implementation options for remote monitoring solutions are discussed and the key requirements for these types of solutions are identified. From these requirements a reference architecture for mobile health connected devices is developed, along with an attempt to draw out the key assets from a mobile operator network that can be leveraged to provide enhanced mHealth solutions. It also demonstrates the enhanced features introduced when these solutions are developed in partnership with mobile operators compared to without. This report describes a number of use cases for mobile health solutions using embedded and connected mobile health devices, from which a generic set of requirements are generated for a mobile health solution. These requirements then form the basis on which an architecture for connected mobile health device is developed. Particular focus is placed on security and machine-to-machine communications as they are viewed as high priority in the future of mobile health.

The use cases developed within this report focus on solutions that can be used for the management of chronic diseases such as diabetes and COPD. The complexity of the examples will increase from a simple mobile health solution provided in isolation by a mobile operator through to a solution that integrate directly into Healthcare systems, and provides lifestyle coaching. The use cases also attempt to address a number of developing world requirements for these types of devices such as devices that need to be used securely by multiple patients.

The use cases investigated in this report are:

1. Consumer purchases mobile health service
2. Healthcare Provider prescribes mobile health service
    a. Prescribed mobile health service with a mobile health Gateway Device
    b. mobile health service connected to Healthcare IT system
3. Prescribed mobile health service for Disease Management

Emergency services or life critical services are out of scope of this paper.

Although this report stops short of describing the full detailed specification of each architecture element, it does describe the key functions and interfaces required within a mobile health solution. It is viewed that the detailed specification of functionality is an implementation question for each separate mobile health deployment and provides the ability for mobile health service providers to differentiate the products and services that they launch.

The aim of this reference architecture is to support mobile operators in the development of mobile health products and services, identifying areas where they can reuse tried and tested capabilities within their networks to provide differentiated service with enhanced features.

The report will also be used to identify areas where further standardisation is required.

1.1 Mobile health eco-system

In order to prevent different interpretations, the mobile health eco-system is described below. The names of components and roles in this eco-system will be used in the rest of this report. It also defines the scope of mobile health considered in this report.

The mobile health eco-system revolves around a **Patient**. A Patient is a person with some kind of health problem. The health problems considered in this report and the use cases in the next chapter are all low risk. Emergency or life threatening situations are not considered in this reference architecture.

A **Clinician** is a healthcare professional that is treating or helping the Patient with the health problem. A Clinician could be a nurse, a General Practitioner, or a specialised physician. The Clinician is working at an organisation that is called the HealthCare Provider (HCP).

The **HealthCare Provider** is utilizing a mobile health Service in the monitoring, diagnosis and treatment of the Patient. The mobile health **Service** is the service that connects the Patient to the Clinician; it measures, transports and delivers the data generated by the Patient and probably provides additional added value.

The mobile health **Service Provider** is the entity providing the mobile health Service through a mobile health Platform. The mobile health **Platform** is the IT system connected to the mobile network to provide all necessary functionality.

The mobile health **Device** is a device needed to use the mobile health Service and to connect to the mobile health Platform. There are three main types of mobile health Devices that are considered in the report:

I. The mobile health Device is a mobile health sensor with embedded GSM connectivity

II. The mobile health Device consists of one or more mobile health sensors that connect to a mobile health Gateway with GSM connectivity

III. The mobile health Device consists of one or more mobile health sensors that connect to a Smartphone (or tablet or laptop) with GSM connectivity

The mobile health **Application** is embedded in the mobile health Sensor or runs on the mobile health Gateway or the Smart Phone.

The mobile health **Clinician Device** (mHCD) is the device that runs the mobile health Clinician Application and is usually a smart phone or another mobile connected device.

The mobile health **Clinician Application** provides an overview of data of all patients of that Clinician and provides specific functionality that a Clinician needs.

The Patient is the user of the mobile health Service but will not always be the subscriber. In healthcare it is also possible that the Healthcare Provider or even the Healthcare insurance could be the subscriber. A subscriber is the one that is taking the role of ordering, paying and ending the mobile health Service.

2 Use cases for Mobile Health

Within this section, three realistic mobile health use cases are described from the perspective of the Patient and the Healthcare Provider. The first of these use cases is a consumer service without the involvement of a Healthcare Provider, but the subsequent use cases describe mobile health services that are prescribed to the Patient by a Healthcare Provider. In these use cases the solution becomes part of the treatment and will have to comply with the quality and safety standards required in healthcare services.

From these three use cases the set of requirements in section 3 of this paper have been defined.

Note that emergency services or life critical services are out of scope of these use cases.

2.1 Use case 1 - Consumer purchases mobile health Service

This Use Case involves the following actors:

Patient – Graham
Subscriber – Nigel
mobile health Service Provider – Blue Mobile Health
Healthcare Provider – Graham's GP

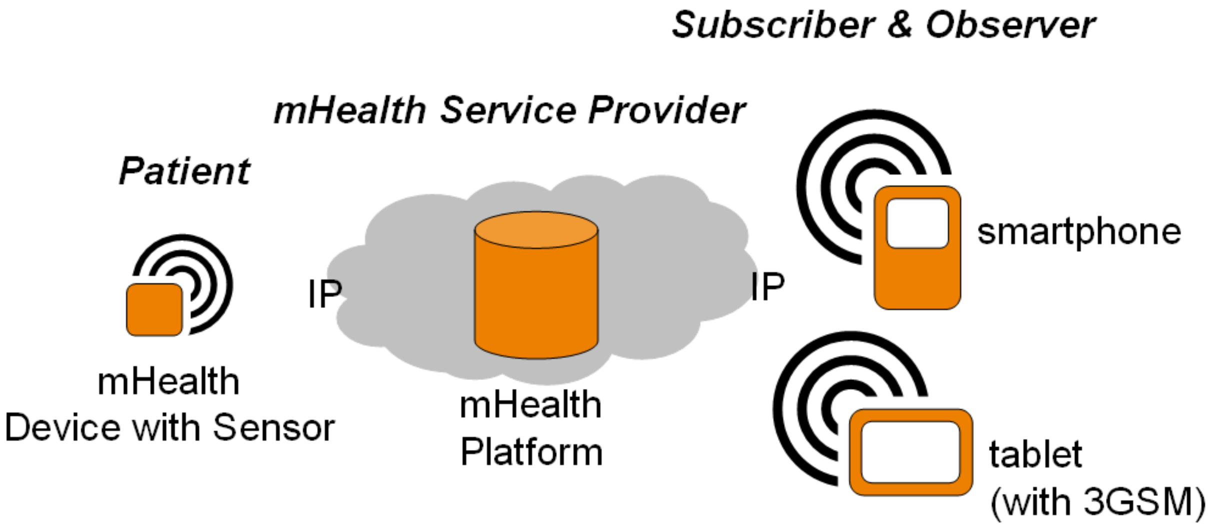

Figure 1 - Consumer purchased mobile health service

Nigel decides that he wants his elderly father Graham to start monitoring his blood pressure because his last visit to the GP showed a tendency to have low blood pressure and he wants to keep track of this in case it gets worse. He doesn't want his father's low blood pressure to end up in an emergency situation without warning as he lives over 100 miles away, he also doesn't want to move his family closer unless it is absolutely essential and Graham has refused to move out of his current house. Nigel wants to be able to respond to or detect a possible crisis situation by monitoring his father's condition more regularly.

Nigel goes to the Blue mobile phone store as he recalls seeing an advert about a service that monitors health conditions.

Once he gets there he speaks to a consultant at the store about his requirements. The consultant asks a few questions about what equipment Graham already has available which is simply a fixed line telephone and Digital broadcast TV. In addition, Graham has an aversion to mobile phones but Nigel suspects that is simply because he doesn't know how to use them but won't admit it. He also tells the consultant that he wants a simple out of the box solution with no bills to be paid by or setup required by his dad Graham.

The consultant suggests a remote monitoring solution that will provide a daily graph of blood pressure and other vital signs with minimal complexity. Nigel signs up for the service and the device are provisioned in the store for Graham.

That weekend Nigel drives over to visit Graham and shows him how to put the cuff on correctly and then to press the Start button – and 'that's it' he tells him, no more buttons, no setup and most importantly no bills to worry about as the whole service is paid for as a subscription that Nigel pays directly to Blue Mobile. There is also no PIN requirement as the expectation is that only Graham will use the sensor and if he lends it to a friend once it will not cause an alarm.

Nigel receives a monthly bill from Blue Mobile for the blood pressure cuff in the same letter as his mobile phone bill.

It could be possible for Nigel to give Graham's GP access to the web service that stores the records created by the Blue Mobile health service. This would then allow him to review Graham's progress during their next appointment.

Nigel tells Graham that if he has any problems using the cuff he should ring the Blue Mobile help desk for advice, but if he has any medical questions he should arrange an appointment with his GP.

2.2 Use Case 2 - Healthcare Provider Prescribes mobile health Service

This Use Case involves the following actors:
Patient – Angus
Healthcare Provider – the primary healthcare provider, also referred to as Clinician

Mobile health Service Provider – In this instance it is assumed that this is the (Mobile Network Operator

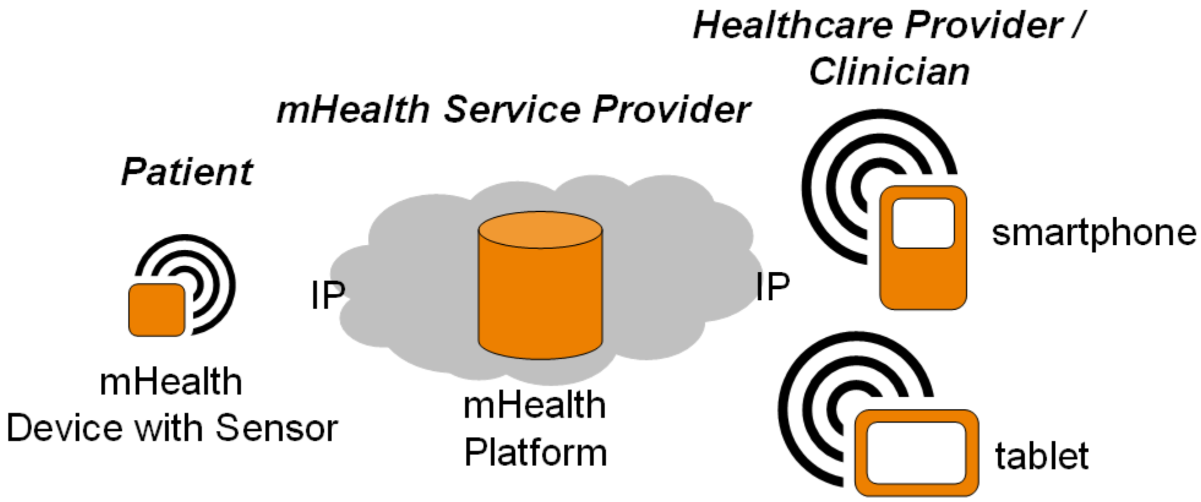

Figure 2 - Healthcare Provider prescribes mobile health service

Angus is diagnosed with a chronic disease (diabetes). He is provided with a dedicated sensor that he uses to monitor his blood sugar level. The physiological data he collects can then be reviewed by the clinician at their next consultation. In this instance the dedicated sensor he is provided with has embedded connectivity in the form of a cellular modem (M2M module). The mobile health device is provided on prescription and it includes the cost of the sensor and all traffic generated by taking readings as well as the web service where they are stored.

The clinician prescribes Angus with the sensor and tells him that he just needs to go to the local pharmacy to pick up the sensor.

At the point of prescription the clinic registers the MSISDN of the sensor to Angus on the Health IT system that the clinic uses and provides him with his User ID. This creates a secure element on the device that is under the direct control of the clinic to store Angus's patient information. They ask Angus to enter a 4 digit PIN (or other identification) which he must use each time he takes a reading to verify it is him using the sensor. Together with the secure element of the UICC, this creates a two–factor authentication of the user for the device ensuring a secure system. It also ensures that all readings from the sensor go directly to his personal medical diary online under his account.

Angus takes the sensor home and the following day takes a reading which involves the following steps:

- Power up the sensor which asks for a 4 digit PIN which he enters
  [a customer call centre function should be provided for remote resetting of PINs OR Angus must take the device back to the clinic]
- Once the PIN is verified Angus takes a reading which is sent to the mobile health application provider with no further interaction required
- For future reading Angus's identity will be authenticated by entering a PIN before each reading is taken.
  [This would be a configurable capability by the mobile health application provider, during the provisioning process]

As this service is being prescribed by his Healthcare Provider Angus will not receive a bill for the service. The mobile health application provider provides an itemized wholesale bill for all sensors that are prescribed by the Healthcare Provider to them on a monthly basis.

At his next visit to the clinic Angus and his clinician access his readings through an online portal. Within this portal Angus and his clinician are also able to manage who else has access to his data.

After 3 weeks the sensor unexpectedly stops sending readings. Angus calls the helpdesk of the mobile health application provider for help. The helpdesk asks Angus for his user ID. From this information they are able to identify the device that he is using. They tell him that some of the settings on the sensor have changed, and they will remotely reconfigure them for him. While speaking to them he says that his last 3 reading were high, but he is informed that this is a technical desk. They tell him that he will need to speak to his Healthcare Provider for help and clinical advice and that they will transfer him automatically to the Healthcare Provider after the call.

At the end of his treatment Angus returns his sensor to the Clinic. The Clinic accesses a web portal and de-provisions the sensor from the service. During this process an aggregated version of Angus' data is sent to his Healthcare provider.

2.3 Use Case 2a - Prescribed mobile health Service with an mobile health Gateway Device

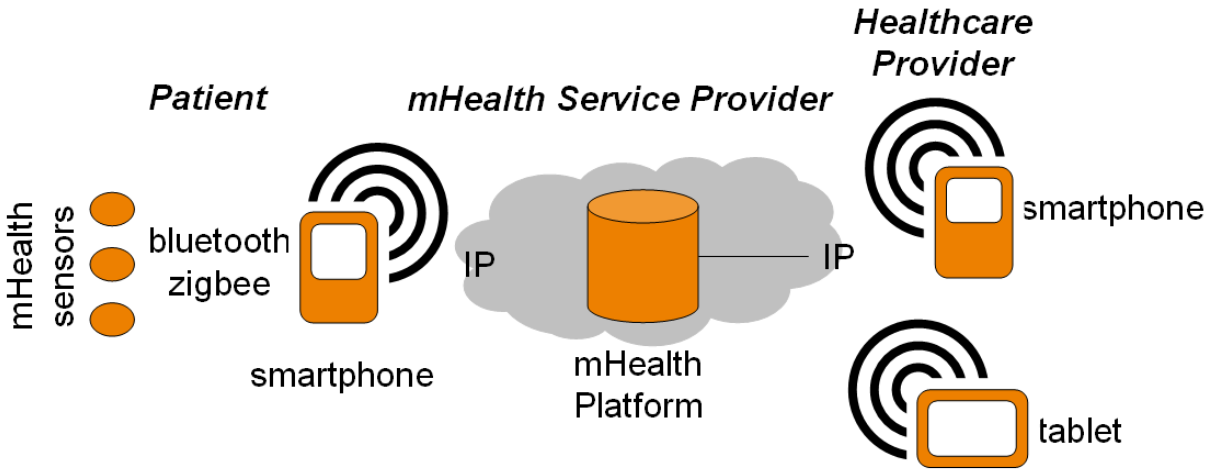

Figure 3- Prescribed mobile health service with a mobile health gateway device

This use case is the same as Use Case II, only the patient gets a more advanced system. Instead of one embedded mobile health sensor, the patient is provided with a (Continua compliant) mobile health gateway device.

The mobile health gateway is provisioned in the same way as the mobile health sensor in use case II. The gateway MAY have a more advanced user interface that provides more interaction option with the patient, for instance in case of identification. The mobile health gateway could also provide feedback about the mobile health service, sensors and data, enabling two way communication between mobile health gateway and mobile health server. In addition, the connection between the mobile health sensor and the mobile health gateway MUST be secure end-to-end.

2.4 Use Case 2b – Mobile Health Service Connected to Healthcare IT system

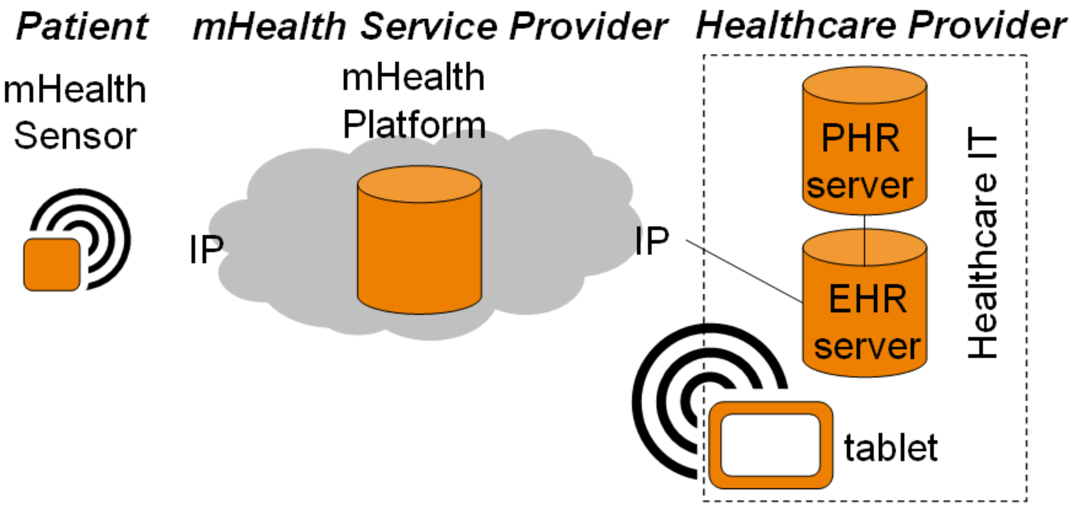

Figure 4 - Mobile health service connected to healthcare IT system

In this use case the Healthcare IT system is connected to the mobile health service. The Healthcare IT system includes an Electronic Health Record (EHR) where a complete record is kept for every patient. The Healthcare provider also provides a Personal Health Record (PHR) where each patient can view his own relevant health information. It may be possible that the PHR is provided by a third party. In that case, the mobile health service provider might need to synchronise to both the EHR and PHR.

The mobile health service is still provisioned through a web portal that the Healthcare provider can access through a mobile device (using a secure UICC).

The Healthcare provider receives notifications from the mobile health service provider if for instance a threshold level is reached. The mobile health service provider synchronises the patient data regularly with the EHR so the Healthcare provider can review all patient data in one application.

2.5 Use Case 3 - Prescribed mobile health Service for Disease Management

This Use Case involves the following actors:

Patient – Lars
Subscriber – Lars and the health insurance entity
Healthcare provider – Lars's GP
mobile health service provider – MNO in partnership with an application provider

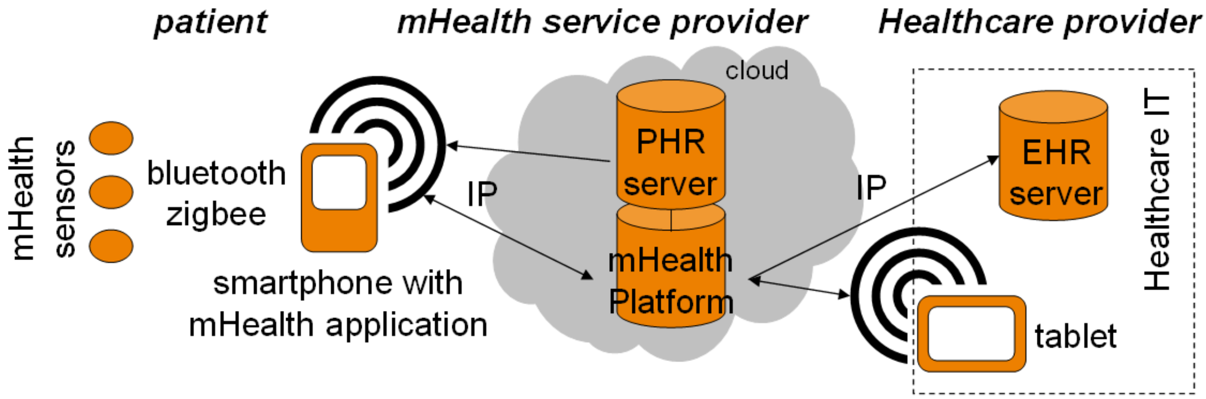

Figure 5 - Prescribed mobile health service for disease management

Lars is diagnosed with diabetes. He does not want the disease to affect his daily life, family and work too much so he has asked his GP for a self-management program. In this program Lars learns to better manage his life with the disease, while also learning to calculate the amount of insulin he needs and adjusting his lifestyle accordingly. The program comes with a blood glucose sensor and a weight scale that both connect to his Smartphone. The Smartphone is running an app that collects and displays the glucose and weight measurements, helps to calculate the level of his insulin, provides educational information about diabetes (short movies), provides questionnaires to test his knowledge about diabetes and living a healthy life as well as providing a communication mechanism with the GP.

The GP receives daily notifications of Lars' measurements (on or off target) on his Smartphone and the results from the questionnaires. Based on that input the GP can send personal notes or point out relevant information to Lars.

To get in the program, the GP provided Lars with a short assessment online to see if his Smartphone and subscription could handle the self-management program. He then created an account to register and connect his self-management program to the information system of the GP. He could download the app and the glucose sensor and scale were ordered. Pairing the blood glucose sensor and scale to the Smartphone and the app was just a matter of turning them on.

The GP continually adjusts the aspects of the remote monitoring program to the level of self-management that Lars has reached. The educational part of the program is less important after the first month but coaching Lars to keep up the good work becomes more important.

Since a chronic disease is not actually cured Lars uses the self-management program for many years. During that time he receives several updates of the app, another phone with a subscription with another mobile operator and he moves to another location and also changes his GP. Amendments to account access and setting need to be done during those changes but he can keep on using the self-management program that he has come to rely on. The best update was when the app incorporated the insulin stock and supply management as well.

Lars is paying for the Smartphone and the operator subscription but the glucose sensor, scale, app and the GP's work are covered by his health insurance.

2.6 Use cases in developing countries

Since the reference architecture should be applicable worldwide and the use cases presented above seem to be situated in developed countries we took a look at what would be different if use cases were situated in developing countries.

Use case 1 and 2 can be situated in developing countries if the necessary infrastructure is in place. Use case 3 might be too complex and demanding at this moment.

However, with simpler means like text messaging, coaching and feedback about measurements, mobile healthcare can be delivered to patients at a distance. Another feature might be "incentive programs" to capture the attention of people for mobile health applications.

What can be seen in developing countries is that mobile health is not always a personal service but a community service. A community healthcare worker has the mobile health tools and helps a group of people with it. That means different requirements on identification of patients because several patients will use the same device and data of patients should not be mixed.

3 Requirements

The use cases from the previous chapter were used to generate a complete set of requirements for a mobile health service. The requirements have been organised and presented below in logical groups. These requirements will then be used as the basis for the development of an architecture in section 4 onwards.

3.1 Functionality of mobile health Device

The mobile health Device MAY have one of the following configurations:

I. The mobile health Device is an mobile health sensor with embedded GSM connectivity

II. The mobile health Device consists of one or more mobile health sensors that connect to an mobile health Gateway with GSM connectivity

III. The mobile health Device consists of one or more mobile health sensors that connect to a Smartphone with GSM connectivity

Requirements:

1. The mobile health Device MUST be easy to use suiting the capabilities of the target group of patients.
2. The mobile health Device must have a unique identifier
3. The mobile health Device MUST have GSM connectivity that complies with the licence condition of the market it is being sold in.
4. The mobile health Device MUST be secure as described below:
    a. The mobile health Device MUST provide data confidentiality while Patient data is processed or stored on the mobile health Device
    b. The mobile health Device MUST provide data integrity while Patient data is processed or stored on the mobile health Device
5. The mobile health Device MUST have an end to end secure connection to the mobile health Platform as described below:
    a. An mobile health Sensor of an mobile health Gateway (Use Cases I or 2) MAY have the ability to do dual factor authentication (depends on user interface capabilities of the device and security risk assessment)
    b. An mobile health Device with a Smartphone (Use Case 3) MUST have the ability to do dual factor authentication
6. The mobile health Device MAY send the measured data at fixed intervals, as soon as possible or at a user initiated
7. The mobile health Device MUST temporarily store Patient data until it can be sent successfully to the mobile health Service Provider
        i. In case of an mobile health Gateway or a Smartphone (Use Case 2 or 3) the mobile health Sensor MUST temporarily securely store Patient data until it can be sent successfully to the mobile health Gateway or Smartphone

8. Use of the (embedded) UICC in an mobile health Sensor or mobile health Gateway MAY be restricted to the specific services provisioned by the mobile health Service Provider only (to prevent misuse or fraud)
9. In case of configuration 2 or 3 of the mobile health Device; the mobile health application MUST NOT interfere with any other application and vice-versa on the Smartphone or mobile health Gateway
10. The mobile health Device MUST send the measured data to the mobile health service provider as soon as possible after service authentication has been completed.

3.2 Functionality of the mobile health Service

11. If notifications are part of the mobile health Service, the Subscriber, Clinician or Patient MUST be able to configure notifications
12. The Patient, Subscriber and Clinician MUST be supported by a technical Helpdesk
13. The technical Helpdesk MUST be able to remotely manage provisioning, network configuration and user authentication
14. The Clinician and the Patient MUST be able to access the Patient data through a secure web portal
15. The Clinician MUST be able to set parameters (for instance threshold values) of the mobile health Service to match therapy goals and/or specific characteristics of the Patient
16. The mobile health Service Provider MUST send notification to the Clinician and the Patient if the set parameters are not met by the data from the Patient
17. The Clinician MUST be able to configure the type of notification sent to himself and MAY be able to configure the notification delivery structure to the rest of the care team
18. The Patient MUST be able to configure type of notification to himself and MAY be able to configure delivery (tree) of notifications
19. In addition to providing Patient Data to the Clinician the mobile health Service MAY also provide secure communication from the Clinician to the Patient or two way communication

3.3 Security

20. The mobile health Service Provider MUST provide end-to-end security by using a unique asset of the MNO (possibly the UICC) as described below:
    a. The mobile health Service Provider MUST provide end-to-end security between the mobile health Device and the mobile health Platform
    b. The mobile health Service Provider MUST provide end-to-end security between the mobile health Clinician Device and the mobile health Platform
    c. The mobile health Service Provider MUST provide end-to-end security between the mobile health Platform and the Healthcare IT system (EHR)
    d. The mobile health Service Provider MUST provide end-to-end security between the mobile health Platform and web portal (for service and review of data)
21. The Subscriber, Patient or Clinician MUST authenticate to the mobile health service provider using appropriate measures in relation to the risk assessment as described below:
    a. Authentication MAY be needed only at first use
    b. Authentication MAY be needed per session
    c. Authentication MAY be needed at every interaction
22. The mobile health Device MUST be registered to the Healthcare provider that provides it to a Patient (for billing)

23. The Patient MUST register for an account at the mobile health service provider to access a web portal with his personal data
24. The Patient MAY authenticate to the mobile health Device using a suitable authentication method (suitable means fitting the capabilities of the Patient and fitting with the required level of security. For instance PIN code, biometric or through NFC)
25. The Patient MUST authenticate to the mobile health server before a measurement can be sent. The Patient MAY also authenticate to the mobile health Device before a measurement can be sent. (to make store and forward functionality possible)
26. The mobile health service provider MUST have the possibility to configure the UICC to give access to the GSM network only for data transfer by the mobile health Device. (might demand authentication of the mobile health Device to the UICC or only provisioned to connect to an mobile health Access Point Name (APN))
27. The mobile health service provider MUST provide end to end security either compliant with Continua Guidelines or based on equivalently secure industry standards.
28. The Patient MAY authenticate to the mobile health application on the Smartphone (or mobile health gateway) of the Patient. If functionality is available the Patient MAY authenticate to the mobile health application on an embedded mobile health sensor
29. The Clinician MUST authenticate to the mobile health application on the Smartphone of the Clinician
30. The mobile health application on the mobile health device MUST authenticate to the mobile health service provider before data can be sent
31. The mobile health Service Provider MUST be able to block the mobile health Device in case of reported misuse
32. The Healthcare IT system MUST authenticate to the mobile health Platform to receive Patient data
33. The mobile health Service continuity levels MUST match the level of medical risk associated with the mobile health Service
34. It must be possible, based on the unique identifier of each mobile health device, to disable lost/device devices on networks that are capable of blocking devices
35. The mobile health Service MUST provide a time-stamped audit trail to independently record the date and time of operator entries and actions that create, modify or delete electronic records. The audit trail will not only be used to gauge who has logged into patient records but could also be used for billing purposes or data gathering for public health reporting and medical research.

3.4 Authorisation requirements

36. The Subscriber or Clinician, with consent of the Patient, MAY provide access, on the web portal or through the mobile health (Clinician) Application, to a third party Observers to view the Patient data
37. Observers MUST have an account on the mobile health Service to gain access to Patient data

3.5 Provisioning

Provisioning of the mobile health Service will depend on the business model. In these requirements all provisioning is done by the mobile health Service Provider. Part of the process could be transferred to other roles (MNO, Healthcare Provider, Subscriber) but all will take place under control of the mobile health Service Provider.

38. The mobile health Service Provider registers the mobile health Device and Subscriber to an account accessible via the internet (web portal)
39. The mobile health Service Provider MUST be able to provide one itemized bill to the Subscriber
40. The Healthcare provider MUST be able to assign (register) the mobile health service to an individual Patient
41. The Healthcare provider MAY need to be able to assign multiple Patients to an mobile health Device, Application or Service
42. The Subscriber MUST be able to cancel an account
43. When de-provisioned the mobile health Service Provider MUST send the aggregated data of the Patient to the Healthcare Provider
44. The Smartphone of the Patient MUST be tested to assess if it can support the mobile health Application and mobile health Sensors

3.6 MNO functionality (mobile health Service Provider)

45. The mobile health Service Provider MUST be able to remotely check status, configure, update or managed the mobile health Device
46. The mobile health Service Provider MUST be able to provide remote configuration of the mobile health application but only with consent of the Patient or Subscriber
47. The mobile health Service Provider MUST be able to provide remote configuration of the Smartphone of the Patient (or an mobile health Gateway) but only with consent of the Patient
48. The mobile health Service Provider MUST log usage of the mobile health service by both Patient and Clinician for billing purposes

3.7 Interoperability

49. The aggregated data MUST be in a format the Healthcare provider IT system can manage and preferably in the format of a widely used industry standard
50. The mobile health application MUST be able to communicate with the Healthcare IT System of the Healthcare provider and the PHR of the Patient to exchange Patient data
51. The mobile health Sensor connects to the Smartphone of the Patient (or mobile health Gateway) through either Bluetooth (v2.1) or Zigbee or a wired USB connection
52. The mobile health Service MAY be able to exchange Patient data with a PHR of the Patient or EHR of the Healthcare provider using industry standards (HL7 and IHE PCD profiles) for Patient data exchange
53. Mobile health Sensors MUST use IEEE 11073 data semantics (or other Healthcare Semantics data standard) and comply with IHE PCD profiles to communicate with the mobile health application on the Smartphone of the Patient (or mobile health Gateway). The embedded mobile health Application or the mobile health Application on the Smartphone (or mobile health Gateway) of the Patient MUST use IEEE 11073 data semantics (or other standard) and comply with IHE PCD profiles to communicate with the mobile health Platform.

4 Architecture

Within this section the key functions of a mobile health solution are discussed and a high-level reference architecture for connected devices is visualised in the figure below. The yellow block represents the mobile health Device of the Patient and the blue block represents the mobile health Device of the Clinician. Between these devices the GSM network highlighting some of the main assets of the MNO are depicted in the grey cloud. The larger light blue box represents the mobile health Platform. On the far right of the mobile health Platform are two key elements of the Healthcare IT system (HIT), the Personal Health Record (PHR) and the Electronic Health Record (EHR) application or system of, for instance, a hospital.

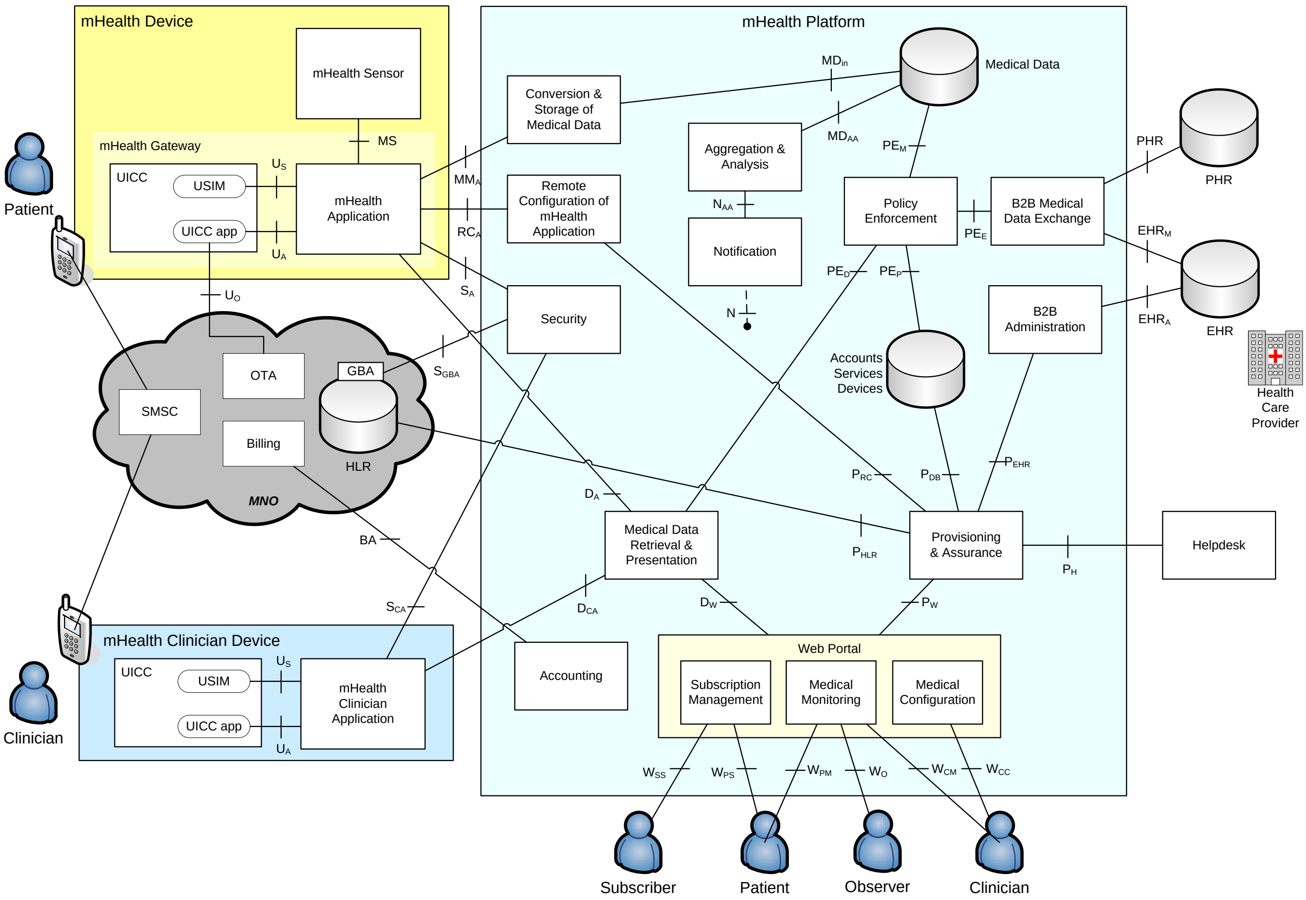

Figure 6 The main building blocks and interfaces of the mobile health reference architecture

Figure 6 shows the main building blocks and interfaces of the architecture. Not all interfaces (lines between the blocks) are drawn as that would make the figure unreadable. Each of the big coloured boxes with its main elements will be discussed briefly below. It should be noted that this is only a representative reference architecture that demonstrates all the key capabilities of a mobile network that can support a mobile health solution.

4.1 Mobile health Device of the Patient

There are a number of form factors that are considered as a mobile health connected device; the type of device will be heavily dependent of the use case for the product or service. The types of devices considered within this paper are:

- An Embedded sensor is a medical device that contains a cellular module that conforms to 3GPP & 3GPP2 standard radio interface
- Gateway device: a medical monitoring device that connects via a short-range technology to a router which then transmits out the information
- Smartphone with application: a device designed to connect via a short-range technology(e.g. Bluetooth) to a mobile phone and those that plug directly into a mobile phone

One of the key enablers of the mobile network is the SIM card that is installed in all mobile devices. The SIM card has been at the heart of the mobile industry for over 20 years, helping to make the GSM family of technologies the most secure, ubiquitous, and successful communications system in the world. The SIM card will remain at the heart of the system for the foreseeable future. The SIM card is secure and it is the custodian of the subscriber's identity. It ensures that trust is maintained between the customer and the mobile telecommunications network. The SIM card will be installed within both the patients and Clinicians device within this architecture.

For enhanced security the mobile health application could use the UICC with the SIM application and/or a mobile health application on the UICC to enable end to end security. The UICC is the unique element provided by the mobile operator inside a mobile health device.

There are a number of different interfaces that could be used by the device to communicate with the mobile health platform. The GSMA recommends that an interface is used that conforms to an international recognised Healthcare messaging standard, for example IEEE 11073, IHE PCD-01, or DICOM.

A possible design for the interface could be the Continua certified WAN interface that encapsulates the IHE PCD-01 and IEEE 11073 data semantics.

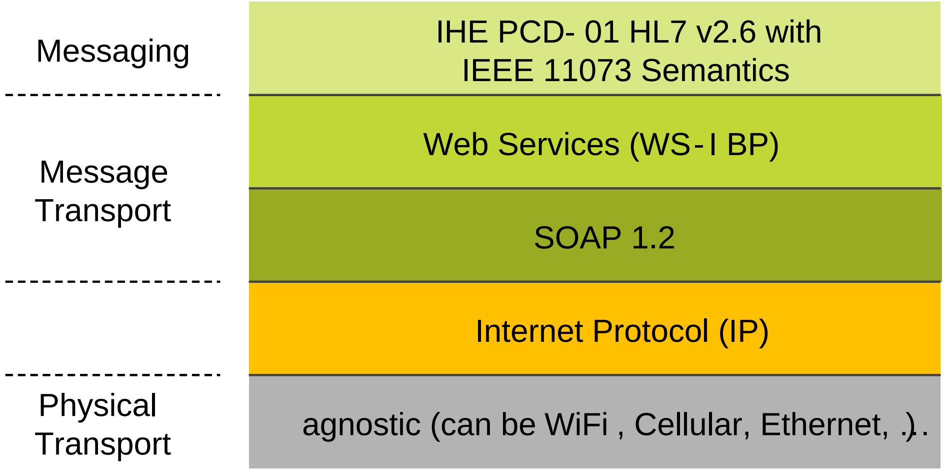

Figure 7 - Continua WAN interface

4.2 Mobile health Clinician Device

The mobile health Clinician Device would enable a clinician to view the data that is being generated by a mobile health device and it is assumed that this will likely be a Smartphone or a tablet based on current market trends. Due to the nature and sensitivity of medical data there will be the need for a significant level of security on the device. Using the capabilities of the mobile network in the same ways as for the patient device it will be possible to meet this need.

4.3 The Mobile Network and its assets

The Mobile Network is represented by the grey cloud between the mobile health devices. This network is used to connect devices and transport data which makes it possible to use mobile health Services largely independent of location.

Other assets are:

- The Home Location Register (HLR) is used to identify a User/Patient's device through the UICC by the International Mobile Subscriber Identity (IMSI). The HLR allows access to the network based on the IMSI of the subscriber and the access profiles that are contained in the HLR.

- Mobile networks have a number of unique identifiers that can be used with the design of a mobile health solution. The most widely implemented of these are the IMSI and IMEI:

    - An International Mobile Subscriber Identity or IMSI is a unique identification associated with all GSM and UMTS network mobile phone users. It is stored as a 64 bit field in the SIM inside the phone and is sent by the phone to the network. It is also used for acquiring other details of the mobile in the Home Location Register (HLR). To prevent eavesdroppers identifying and tracking the subscriber on the radio interface, the IMSI is sent as rarely as possible and a randomly-generated TMSI is sent.

    - The International Mobile Equipment Identity or IMEI is a number, usually unique to identify GSM, WCDMA, and iDEN mobile phones, as well as some satellite phones. It is usually found printed inside the battery compartment of the phone. The IMEI number is used by the GSM network to identify valid devices and therefore can be used for stopping a stolen phone from accessing the network in that country. For example, if a mobile phone is stolen, the owner can call his or her network provider and instruct them to "blacklist" the phone using its IMEI number. This renders the phone useless on that network and sometimes other networks too, whether or not the phone's SIM is replaced. The IMEI is only used for identifying the device and has no permanent or semi-permanent relation to the subscriber. Instead, the subscriber is identified by transmission of an IMSI number, which is stored on a SIM card that can (in theory) be transferred to any handset. However, many network and security features are enabled by knowing the current device being used by a subscriber.

- Subscription Management: The mobile operator has a responsibility to manage its customers' subscriptions correctly, so that the customer receives all services that they are entitled to and equally does not receive (and as a result, is not charged) for services that they do not subscribe to. The management of the subscription for an individual customer requires technical integration between Customer Care systems, Billing Systems, Provisioning systems and the Subscription management elements within the mobile operator network, these being the Home Location Register (HLR). Within the subscription management function it is possible to control the access of a device to the network e.g. it would be possible to limit the access of a device to data services only or even to specific Access point (APN).

- Billing is the functionality that makes it possible to track and invoice revenues generated by the use of mobile health Services. MNO's have flexible billing systems that can work with time, volume, subscription and prepaid models and are also capable of revenue sharing between all involved stakeholders. Information about what and how much to bill is obtained from the accounting functionality from the mobile network or the mobile health platform depending on the charging mechanism that has been implemented. Equally, operator Billing systems can be used to manage other forms of contract that may be required by different sets of their customers. Wholesale agreements with corporates or enterprises can be facilitated to provide a single bill for a large number of individual devices, even when those devices may not be tied to an individual person. This makes the operator capable of providing bills to customers with large numbers of 'non-traditional' devices as a consolidated bill, on the basis of any form of charging model from a flat rate monthly service charge to a highly granular bill with detail of each individual occasion of device-network interaction. No change in network technology is required to enable this, only an understanding of the contract and suitable software changes to reflect the billing model on the customer bill itself.

- Customer Management - Operators have an established commitment to support their customers that is not typical in other telecommunications, internet or computing sectors. This has been traditionally done via call centres, but is increasingly moving to online support as a cheaper, more efficient option. The expertise that mobile operators have in being able to provide end users and corporate customers with advice and support on matters relating to both their services and the devices in the hands of the customers has considerable value which can be extended to include support for services that are in the embedded mobile sphere. Operators often support large corporate clients with dedicated customer support teams, and so for mobile health services operators could provide a customer support offering which is tailored to the specific requirements of the organisation operating those devices.

- Mobile networks have the capability to detect the location of the devices on its network via the Gateway mobile Location Centre (GMLC) and use it in the services that are being provided. This capability would enable the mobile health platform to identify the location of a Patient or Clinician using the service and be a major asset in providing safe mobile health solutions and a differentiator from the current telehealth services.

- Over The Air (OTA) management is another way of providing device configuration, software updates and provisioning of an application on the UICC. As the name implies it provides the capability to do several device and application management tasks at a distance and using the cellular network of a Mobile Operator.

- The Generic Bootstrapping Architecture (GBA) is an element that is used to provide secure authentication and encryption of Patient data and will be further discussed in the next chapter about security. The GBA functionality is well known and standardised and has been implemented by a number of Mobile Operators; however it is has not yet been fully adopted by all Operators as it requires an upgrade to the network.

- The SMS Centre (SMSC) of an operator is an important piece of functionality that could be used for both textual communication between patient and clinician, as well as binary M2M communication between mobile health Platform and mobile health Device. Textual communication could be used to provide feedback to the Patient or for allowing a Patient to send text messages to the Clinician. Binary SMS could be used to configure the mobile health

Device or mobile health Application during provisioning or updates, or as a trigger to the device to set up a connection to the mobile health Platform (see M2M Section). SMS could also be used as an alternative data bearer for transmitting measurement data to the mobile health Platform, but the uses of SMS will mean that complex security and encryption requirements cannot be met.

These are the important assets of a Mobile Operator in both the network and on the device that can provide added value in mobile health provision to Patients and Healthcare Providers. All of these key assets are built on robust and mature standards that ensure the functionality is available globally in over 200 countries and within 800 MNOs at massive scale, and are the reuse of common technologies that have already been fully standardised.

4.4 The mobile health Platform

Many of the building blocks inside the mobile health Platform show the basic functionality that a generic mobile health Service will need. Apart from the true healthcare elements, all of this functionality is either a reuse of common telecoms capabilities or is generated from data sources within the mobile network. However, the exact details of the functionality and its architecture will be determined by the detailed requirements of the mobile health provider developing the platform. In essence, the mobile health Platform is an IT platform that uses the data generated by the mobile network to provide an enhanced healthcare service over traditional telehealth offerings.

In the next section we discuss several of the key building blocks of a mobile health platform, along with focusing on the interfaces that connect the platform to the mobile health Device, the Mobile Network and assets or the Healthcare IT.

The main building blocks:

- Security (will be discussed in next chapter)

- Conversion and Storage of Medical Data
  This capability receives data from the mobile health devices, converts this data when necessary (for instance to and from IEEE 11073 and HL7) and stores the data in the medical data database for further analysis and processing. Data storage and processing should also be secure to be able to ensure privacy. There needs to be access control on the storage of patient data (firewalls) and the data could also be stored in an encrypted format.
  Patient data storage and processing should comply with the relevant healthcare privacy and security standards as for instance formulated in the US Health Insurance Portability and Accountability Act (HIPAA). The HITECH part of this act extends the complete Privacy and Security Provisions of HIPAA to business associates of covered entities.
  HIPAA has been the reference for privacy and security regulations in Healthcare in Europe as detailed in for instance the ISO/IEC 17799 international information security standard. Moreover, in some member nations of Europe the access and control of the patient data is more strictly regulated.

  Interfaces:
  - MM_A: receiving raw data from mobile health application (IEEE 11073 and HL7)
  - MD_{in}: storing medical data converted to database format

- B2B Medical data exchange
  This capability takes care of the automated information exchange between the mobile health platform and the databases of the healthcare providers. It could for instance synchronise data at regular intervals based on data exchange policies. This entity has the capability to expand the systems from a standalone mobile health service to a fully integrated healthcare solution by enabling connectivity with Healthcare ICT systems. It has to apply to the same security and privacy requirements as the data conversion and storage functionality.

  Interfaces:

  - PE_E: access to authorized medical data for B2B exchange with Health Care Provider's IT systems
  - PHR: interface to exchange information with the Personal Health Record database
  - EHR_M: interface to exchange information with the Electronic Health Record database of the Health Care Provider. For example this interface could be designed like the Continua HRN (Health Reporting Network) interface. It can be designed as described in the Continua HRN Interface Design Guidelines based on the HL7 CDA R2 standard (Personal Healthcare Monitoring Implementation Guide)

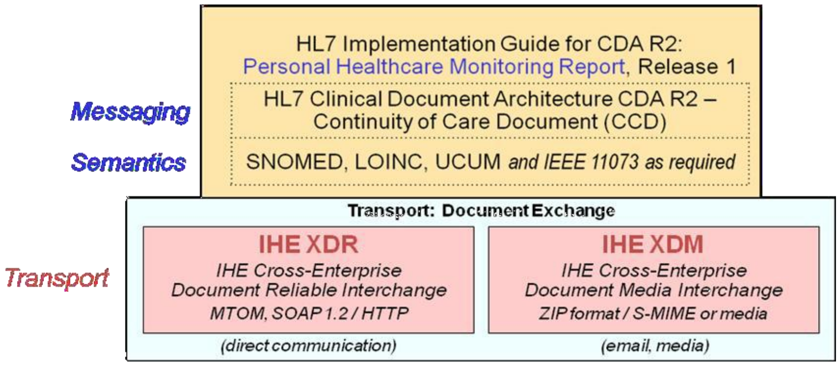
HL7 Implementation Guide for CDA R2:
Personal Healthcare Monitoring Report, Release 1
HL7 Clinical Document Architecture CDA R2 – Continuity of Care Document (CCD)
SNOMED, LOINC, UCUM and IEEE 11073 as required
Messaging
Semantics
Transport: Document Exchange
Transport
IHE XDR
IHE Cross-Enterprise Document Reliable Interchange
MTOM, SOAP 1.2 / HTTP
(direct communication)
IHE XDM
IHE Cross-Enterprise Document Media Interchange
ZIP format / S-MIME or media
(email, media)

Figure 8 - Continua HRN interface

- B2B Administration
  The B2B Administration provides administration functionality to the Healthcare provider. For instance, it can provide accounting information about all patients and clinicians to a hospital for reporting and administration purposes. Or the hospital could provide the access rights for all the staff to the mobile health Platform. The configuration capabilities of the web portal could be compared to the B2B administration, but the B2B administrator provides that capability to configure whole groups. The functionality could also act as the gateway into the mobile health platform from the Healthcare environment to enable provision and management of the mobile health service. Along with these administrative capabilities, this element can provide audit controls to meet the regulatory requirements in several nations for patient control of their data: whether it will be stored and for how long, who has access and identification of who had access and what the data is used for.

- Interfaces:

  - EHR_A: administrative interface for a Health Care Provider to manage accounts and services through its own EHR system
  - P_{EHR}: internal wholesale provisioning interface through adaptation in B2B Administration component

- Provisioning and Assurance

  This capability takes care of all provisioning and assurance functions (comply with the service level agreements (SLA's)) available via the Web Portal or helpdesk in order to perform network configuration, remote application configuration, management of services, accounts and devices and B2B interface management. It enables the set-up of the mobile health service on the mobile health platform and mobile health device provisioning, along with integration into the telecoms provisioning functions . It should also be possible to provision the mobile health service to connect as a data only service or only to a specific mobile health Access Point Name (APN).

  Interfaces:

  - P_W: interface for the Web Portal to the provisioning and assurance capability
  - P_H: interface for the helpdesk to the provisioning and assurance capability
  - P_{HLR}: interface to the HLR of the Mobile Network Operator, set restrictions to services and access to private/secure Packed Data Network (PDN)
  - P_{RC}: interface for remote configuration of mobile health devices, applications and sensors
  - P_{DB}: interface to the database with information about user accounts, mobile health services and devices
  - P_{EHR}: interface for B2B administration

- Web portal

  This capability provides the web portal interface to the Subscriber, Patient, Observer and Clinician.

  - The Subscriber is the entity paying for the service
  - The Patient is the person that is actually using the mobile health Service
  - The Clinician is the healthcare professional that prescribed and monitors the mobile health Service
  - An Observer is a healthcare professional or for instance a relative of the patient that is allowed to review the monitoring data as well

  Each of these roles has a different profile and gets access to a different set of functionality through the web portal.

  The web portal exposes all service management functionalities, like subscription management (set-up, ongoing management and ending of the mobile health service), medical monitoring, and medical configuration.

Interfaces:

- P_W: interface for the web portal to the provisioning and assurance capability D_W: interface for the web portal to the presentation capability
- W_{SS}: Interface for the subscriber to the subscription management functionality
- W_{PS}: Interface for the patient to the subscription management functionality
- W_{PM}: Interface for the patient to the medical monitoring functionality
- W_O: Interface for the observer to the medical monitoring functionality
- W_{CM}: Interface for the observer to the medical monitoring functionality
- W_{CC}: Interface for the clinician to the medical configuration functionality

- Accounting
  This capability performs all accounting functionalities in order to bill the mobile health service to the subscriber and to get service management information. The accounting functionality gathers data about usage of the mobile health service and of functionality used within the mobile health platform. For example it may measure the number of times the service is used, the amount of time it is used or the volume of data use. This information can be used for billing, an audit trail, as management information or within the mobile health service. Input data for accounting can be received from any other element of the mobile health platform, based on the mobile health service pricing model. Accounting data is sent to the Mobile Operator for billing and to the Healthcare Provider for administration and reporting as well as to the mobile health Service Provider for service management information.

  Interfaces:
  BA: Call Data Records (CDR) interface to billing system(s) of Mobile Network Operator

- Notification
  This capability sends notifications to Patients, Observers or Clinicians whenever preset thresholds or other rules are met. The aggregation and analysis functionality provides the input for notification. The type of notifications can be configured through the web portal or the B2B administration interface. The notification engine is connected to the SMS centre of the Mobile Operator as SMS is a good way to notify both individual users and groups of users (for instance about the availability of an mobile health application update).

5 Security

Security is an important element in mobile health. Many of the requirements from chapter 3 are security related. In this chapter solutions are presented that match the security requirements and make use of unique Mobile Operator assets within the scope of a high level reference architecture. It should be stated that many other solutions are possible to meet the security requirements and that any design or implementation of a mobile health Service should include a security risk and regulation analysis. Based on such a specific analysis it is possible to make choices that differ from the options presented below.

The focus in this chapter is on the connection between the mobile health Device and the mobile health Platform because that connection is unique to any mobile health Service. Access control and data storage will also be discussed.

5.1 Summary of requirements

Security is an important aspect of mobile health and because it provides unique opportunities for MNOs to provide added value based on their existing assets. The security requirements that apply to the communication between the Patient and Clinician mobile health Device (mHD) and the mobile health Platform (mHP) could be summarized to:

- Device and data security:
  - Protection of data while in storage on devices
  - Protection of data when processed on devices
  - Protection of data when transmitted to/from the devices
- Integrity and Confidentiality of information exchanged

The following requirements were identified to enable end to end security.

Confidentiality requirement

R1) Confidentiality protection of the Patient data during transport between mobile health (Clinician) Device and mobile health Platform

Integrity requirements

R2) Authentication of the mobile health Platform
R3) Authentication of the (R3a) mobile health Device or (R3b) mobile health Clinician Device
R4) Data Integrity protection of the communication
R5) Data integrity protection of the Patient data
R6) Non-repudiation protection of the Patient data
R7) Authentication of the user: (R7a) Patient, (R7b) Clinician

5.2 Solutions

When looking at solutions that meet the requirements the focus is on solutions that use a unique asset of the Mobile Operator to provide the security. Three general solutions will be discussed:

1. Standard data encryption of 3G, 2.5G and 2G radio
2. Transport layer Security (TLS) with GBA (Generic Bootstrapping Architecture)

3. mobile health application on the UICC / SIM

5.2.1 Standard 3GSM radio encryption

The encryption of data over the radio connection as presently applied in practice shows variations in implementations. The end points of data encryption in 2G, 2.5G and 3G are different and some parts of the standards are optional. Not all operators apply encryption as local regulations may not permit the use of encryption in some jurisdictions. This means the strongest 3G security connection will not always be available to a mobile health Service and other solutions are needed to ensure the end 2 end security between mobile health Device and mobile health Platform.

5.2.2 TLS with GBA

Using GBA (Generic Bootstrapping Architecture) for key exchange would ensure the confidentiality of the mHD to mHP connection by using a unique Mobile Operator asset: the GBA. In standardization this solution is called TLS-PSK (Pre-Shared Key) with GBA. Pre-sharing keys could have some advantages over public key sharing especially if there is a bootstrapping function like GBA available.

How does GBA work?[1]
In mobile phones, Generic Bootstrapping Architecture (GBA) is a technology enabling the authentication of a user. This authentication is possible if the user owns a valid identity on a Home Location Register (HLR) or a Home Subscriber Server (HSS). In fact the UICC is identified and it is assumed to be in the possession of the user. GBA is standardized in 3GPP[2].

The user authentication is instantiated by a shared secret, one on the operator’s smartcard (UICC) inside the mobile phone and the other on the HLR/HSS.
GBA authenticates by making a network component challenge the (U)SIM application on the UICC and verify that the answer is similar to the one predicted by the HLR/HSS.
Instead of asking the service provider to trust the Bootstrapping Server Function (BSF) and relying on it for every authentication request, the BSF establishes a shared secret between the UICC and the service provider. This shared secret is limited in time and for a specific domain.

[1] See: http://en.wikipedia.org/wiki/Generic_Bootstrapping_Architecture

[2] http://www.3gpp.org/ftp/Specs/html-info/33220.htm

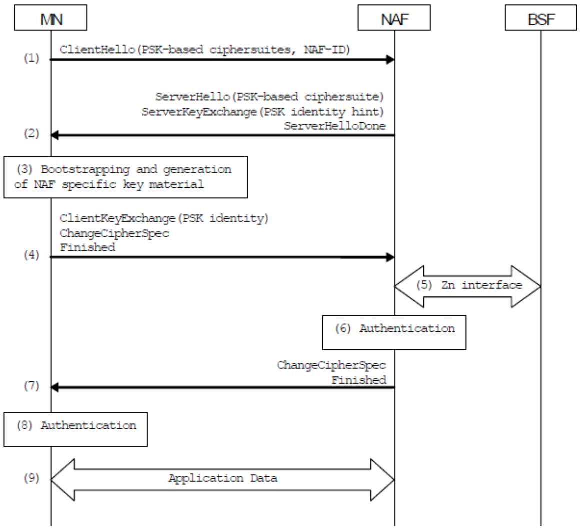
MN
NAF
BSF
(1)
ClientHello(PSK-based ciphersuites, NAF-ID)
ServerHello(PSK-based ciphersuite)
ServerKeyExchange(PSK identity hint)
ServerHelloDone
(2)
(3) Bootstrapping and generation of NAF specific key material
ClientKeyExchange(PSK identity)
ChangeCipherSpec
Finished
(4)
(5) Zn interface
(6) Authentication
ChangeCipherSpec
Finished
(7)
(8) Authentication
(9)
Application Data

Figure 9 - Security Mechanisms Using GBA[3]

(MN = Mobile Network, NAF = Network Application Function, BSF = Bootstrapping Server Function)

5.2.3 mobile health application on the UICC

By using the UICC as a generic MNO asset, and providing a dedicated mobile health application to it rather than the (U)SIM application that is used for 3GSM network authentication (see solution 2), the security requirements can be met as well. The UICC is the smart card used in mobile terminals in GSM and Universal Mobile Telecommunications System (UMTS) networks. The UICC ensures the integrity and security of all kinds of personal data, and it typically holds a few hundred kilobytes for applications or data. With the advent of more services, the storage space will need to be larger. In a GSM network, the UICC contains a SIM (Subscriber Identity Module) application and in a UMTS network it is the USIM (Universal Subscriber Identity Module) application. The UICC can also be used for specific applications that provide access to specific services. For instance, for mobile payments the UICC contains an mPayment application. For mobile health a similar solution is proposed that implies provisioning of a mobile health application on the UICC in the mobile health Device to provide security mechanisms under the control of the Mobile Operator.

5.2.4 Solutions for confidentiality

A possible solution using the UICC could be:

- The mobile health application on the UICC is used to establish a secure channel (i.e. TLS) between the UICC and the mobile health Platform
- The mobile health application on the UICC is used to encrypt the Patient Data before transmission to the mobile health Platform. There are many possibilities to do encryption. A well-known and standardized option is using XML-Encryption. XML itself is a popular technology for structuring data, and therefore XML-based encryption is the natural way to handle requirements for security in structured data interchange applications. Other options for encryption could be:

    - Cryptographic Message Syntax Standard: PKCS#7/CMS [4]

[3] 3GPP2 S.S0114-0, Version 2.0, Version Date: February 2008, Security Mechanisms Using GBA

[4] http://en.wikipedia.org/wiki/PKCS

- Secure/Multipurpose Internet Mail Extension: S/MIME[5]
- Open Pretty Good Privacy: OpenPGP[6]

5.2.5 Solutions for data integrity

The mobile health application on the UICC is used to generate a Message Authentication Code (MAC) over the Patient data before transmission. The mobile health application on the UICC with PKI (Public Key Infrastructure) functionality is used to digitally sign the Patient data before transmission. Many options to do this are available but well known and standardized options include: XML Signature (defines an XML syntax for digital signatures and is defined in the W3C recommendation XML Signature Syntax and Processing) or Cryptographic Message Syntax (CMS is the IETF's standard for cryptographically protected messages. It can be used to digitally sign, digest, authenticate or encrypt any form of digital data).

In general a mobile health application on the UICC can be developed to have many features and security mechanisms.

The document from EPC (European Payment Council) and GSMA entitled: Mobile Contactless Payments (MCP) Service Management Roles, Requirements and Specifications, (EPC 220-08, Version 2.0) of October 2010[7], provides a good example of using an application on a UICC in a mobile service (mPayment) that requires high levels of security and trust. Similar work needs to be done for the mobile health solutions using a mobile health application on a UICC.

ETSI standard TS 102 484 describes a secure channel solution between an application on a UICC and an application on a terminal. The same secure channel could be used between a mobile health application on a UICC and a mobile health platform.

TS 102 569 describes a UICC Security Service Module (USSM) that can be used by UICC mobile health Application developer for crypto & key management. Figure 1010 from ETSI TS 102 569 shows how different applications on a UICC could use the same or different USSMs.

[5] http://en.wikipedia.org/wiki/S/MIME

[6] http://en.wikipedia.org/wiki/Openpgp#OpenPGP

[7] http://www.gsma.com/documents/epc-gsma-trusted-service-manager-service-management-requirements-and-specifications-january-2010/21133

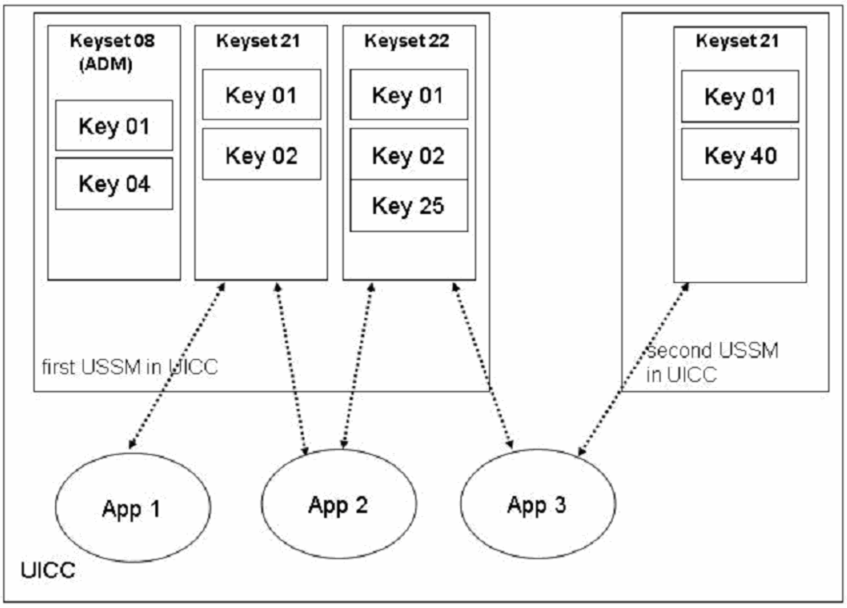

Figure 10 Example of a UICC with two USSMs and how different applications can use these

The use of smartcards in banking is common practice while in Healthcare this is still in development. The MCP services comply with the SEPA (Single Euro Payment Area) standard that is developed for the monetary union of the Euro.

For further information on smartcard standards that are developed for other e-services or specifically for Healthcare, the common smartcard specification IAS-ECC (*Identification Authentication Signature – European Citizen Card*) is a good reference and is also used for Healthcare applications in France.

5.2.6 How to get the mobile health Application on the UICC:

There are three ways to provision a mobile health application on the UICC:

- The mobile health application can be preloaded on the UICC
- The mobile health application can be loaded on the UICC at a Point of Interaction
- The mobile health application can be loaded on the UICC through Over the Air (OTA) provisioning

5.2.7 Discussion of GBA versus UICC

5.2.7.1 Meeting the requirements

By using GBA to secure the confidentiality and integrity of the patient data it is possible to meet all security requirements except for the non-repudiation requirement. Non-repudiation security will only be necessary on mobile health Clinician Devices if they are going to provide feedback to the patient from that device and if that feedback could have direct effects on the health of the patient (for instance, increase medication). In all cases where those kinds of messages are not used the GBA solution provides suitable security protections for mobile health services.

An application on the UICC that is used to provide security is capable of meeting all requirements, even the non-repudiation requirement. The application on the UICC is a flexible solution because the application can perform many different functions. Both GBA and an application on a UICC meet the user authentication requirement once the device containing the UICC is in the possession of the user, which can be verified by PIN entry.

5.2.7.2 Advantages of GBA

GBA has some strong merit over some solutions that use certificates and shared secrets without having some of their weaknesses:

- There is no need for a user enrollment phase or secure deployment of keys, thereby delivering a low cost but effective solution when compared to PKI.
- Another advantage is the ease with which the authentication methods may be integrated into terminals and service providers, as it is based on HTTP's well known "Digest access authentication". Every Web server already implements HTTP digest authentication and the effort to implement GBA on top of digest authentication is minimal.

On the device side the following is needed:

- A Web browser (in fact an HTTP client) implementing digest authentication and the special case designed by a "3gpp" string in the HTTP header.
- A means to dialog with the SIM card and sign the challenge sent by the BSF

5.2.7.3 Weaknesses of GBA

Although GBA is relatively easy to roll out and well standardized not many Mobile Operators are providing the capability at this moment.

5.2.7.4 Advantages of mobile health application on the UICC

The mobile health application on the UICC provides several advantages:

- Universal solution: a UICC is present in all GSM / 3G / 4G handsets
- Portability: removable cards allows users to migrate credentials between handsets and devices
- Accessibility: fully manageable through secure Over-the-Air (OTA) protocols
- User-friendly: web 'look and feel' interface delivered through Smartcard Web Server
- Standardised: robust and interoperable, the result of two decades of continuous standardisation efforts by the UICC industry
- Secure: state-of-the-art security proven by accredited certification, verified by independent labs
- Multi-party services hosting: seamless integration and compatibility with all functional and security requirements of payment, access, and transport cards
- Multi-party services management: dedicated security domains allows individual service providers to manage contactless services within the UICC

5.2.7.5 Weaknesses of mobile health application on the UICC

The mobile health application on the UICC needs to be designed and developed completely from scratch. The necessary standardisation could take time and then the infrastructure will need to be implemented by the Mobile Operators.

5.2.8 GBA or application on the UICC

In summary the GBA solution is low cost, can be implemented right away in every GSM network and meets the security requirements needed for the use cases described earlier. The application on the UICC, however, provides more flexibility and may achieve higher levels of security. At this moment the first mobile services that use an application on a UICC are coming to the market. Mobile health could very well follow these developments. In theory both solutions also work in roaming scenario's as the roaming network will only be used as data connection. In practice it could depend on the implementation of the elements in the network.

5.3 Access control to the device

Requirement 11 states that the Patient needs to authenticate to the mobile health application while requirement 5 states that the Patient needs to authenticate to the mobile health device. The GBA and application on the UICC solutions secure the data transmission. Access control can be an extra security layer that works together with the encryption to protect the integrity of the service and of the data that is (temporarily) stored on a mobile health device.
In the use cases where more people could use a mobile health device there is a need to know which Patient is sending data. Authentication can be as simple as clicking on your own name in a list before data is transmitted. It can be more difficult providing user name and password, or even pass biometric testing.
With a mobile health device the assumption could be made that the person using the device is the Patient, and no extra access control is needed. That is the most Patient friendly solution, but this may not be a suitably trusted solution for a healthcare provider.

Other relatively Patient friendly access control methods on a mobile health device are biometric control or an NFC card that is held close by to authenticate the Patient.

Access control can also be done on the level of the mobile health application. The application could use the access control of the device or have its own access control like PIN or username / password.

If the security assessment asks for save storage of patient data on the mobile health Device, access control on the device or the application level could be combined with encryption of the stored data.

Access control and encryption of the device can be integrated into the full end to end security by using the code that is used for access (like a PIN of a NFC code) as part of the key that is used to generate the encryption key.

6 M2M (Machine 2 Machine)

Mobile health is one of many possible machine-to-Machine (M2M) applications. In 3GPP, M2M is referred to as Machine Type Communication (MTC). One of the areas where 3GPP focuses on in MTC standardisation is the management of many (thousands – millions) of MTC devices. For managing so many devices, an MTC server is envisioned that can control the devices. A common MTC use case is an electricity company remotely polling thousands of meters. In this case the smart meter is owned by the electricity company who controls these devices. The electricity company is initiating the reading of the smart meters.

MTC features that are addressed in 3GPP are dealing with large numbers of MTC devices on a scale not envisioned before. The address space used today (MSISDN/IMSI) may not be enough to identify each MTC device. So new ways of identifying and addressing MTC devices are specified that are unique within a MTC addressing space. In some countries regulations may even mandate the use of dedicated MTC address space of MTC devices in order not to put a strain on the public phone numbering plan. An MTC server plays an important role in controlling the MTC devices, and this includes mechanisms to trigger these uniquely identifiable devices.

The M2M standard is still in development. Common interfaces that have been identified but not yet fully specified are the Interface of the MTC server to the short messaging service centre (SMSC), Home Location Register (HLR) and Packet data network. These interfaces and others that are developed can be utilized by a mobile health system once these interfaces (common application programming interface (API)) are implemented in networks.

In the mobile health use cases considered in this context, the mobile health devices are not managed by a central server. In the mobile health use case the mobile health server collects information that is sent by the device, and in general initiated by the user. We have not identified the need for a MTC server in one of the three mobile health use cases.

Servers in use today, to send SMS messages to remind patients to take their medicine for instance, do not require a MTC server but only a large account coupling to a SMSC. For an mobile health Service Provider there are tools available to manage subscriptions and do the provisioning similar to the tools available to Mobile Service providers that make use of a Mobile operator network. These tools include activating/deactivating subscriptions (SIMs) and managing subscription profiles (allowed services, data rates, roaming).

Remote application or device configuration can be done when the device contacts the mobile health server, much like updates of apps done today via an app-store. Other mobile health use cases can be envisioned where it is possible that the Clinician or the mobile health Platform need to initiate the read-out of the mobile health Devices (data pull from the clinician). These will be use cases that are less focused on self-management by the Patient or include emergency situations with emergency messaging or involve the remote control of a mobile health actuator like an insulin pump or implantable cardioverter-defibrillator (ICD). If Patients are unable to initiate the telemonitoring then M2M communication might be a solution to keep the involvement of the Patient as low as possible. It could also apply to embedded mobile health sensors that measure the context of a Patient instead of a body parameter. For instance, it could be beneficial to measure air quality in a house of a COPD Patient and combine those readings with his health status. The air quality sensor does not need to be controlled by the Patient.

7 Roadmap

The three use cases show a build-up in complexity of a mobile health service. But next to complexity and functionality the roadmap of mobile health shows several other developments.

- **Personal Area Network interface**
  The PAN (Personal Area Network) interface is the connection between a mobile health sensor and a mobile health gateway or Smartphone. Not much attention is given to this mostly wireless interface. Bluetooth and Zigbee provide well known technologies to connect. By following the Continua PAN (including Bluetooth HDP) and Sensor-LAN (Zigbee) interface guidelines it might be possible to have sensors that can connect to an eHealth gateway as well as being used in combination with a mobile health Gateway or Smartphone. The wireless PAN interface could be more secure if the sensor and gateway are both NFC enabled. NFC pairing is then possible by just tapping the sensor to the gateway to initiate the pairing process. This is more secure because the pairing process does not involve a discovery process.

- **Healthcare IT connection**
  The Healthcare IT connection focuses on exchanging Patient data with an Electronic Health Record or with a Patient Health Record. In this field a lot of development is going on to standardise and implement standards to make it easier to exchange patient data between systems and services. These standards are mentioned in paragraph 4.4.1 under B2B Medical data exchange. Mobile health service providers should focus on providing the necessary range of interfaces based on the IT systems that the connected Healthcare Providers are using while striving for more standardisation on transport, messaging and data semantic level.

- **Embedded UICC**
  Next to the well-known SIM card the embedded SIM will soon be available. It is a chip with the same functionality that makes it easier to manage subscriptions because it can be remotely activated. A mobile health Device with an embedded SIM can be provisioned over the air with operator credentials. That means a device that is mass manufactured can be put in operation by any operator anywhere in the world without having to change or insert a SIM card.
  Taking this development a bit further could mean that mobile health sensors no longer need to connect to a gateway or Smartphone but have their own connection to the mobile health Platform. To review the data that is transmitted by these sensors, another mobile device could be used that has its own connection to the mobile health Platform

- **GBA first and later application on the UICC**
  With GBA it is possible to provide Mobile Operator asset based security for many mobile health services. Setting up an infrastructure for mobile health security based on an application on the UICC may take more time to develop because it is relatively new. When starting with the applications on the UICC it may be a good choice to start at the Clinician

side. If all the Clinicians of a Healthcare Provider were subscribed to the same Mobile Operator on the company subscription, it would ease the implementation of the solution.

- **Wellness, Medical, Emergency**
  To introduce a service on the mobile health market that is mostly about wellness is relatively easy as it is similar to many consumer services. The Mobile Operator assets however become of more value if they are applied to medical services (prescribed by a Clinician). The use cases 2 and 3 are medical mobile health services but at the same time the medical risks involved are relatively low. When going into mobile health services that include applications to service a clinical emergency then the requirements in this whitepaper are no longer sufficient.

- **Fixed Mobile integration**
  mobile health can be beneficial if integrated with eHealth. eHealth uses the existing landline communications network while mobile health uses the mobile telecommunication network. As an introduction strategy mobile health could be a logical extension of an already successful eHealth service. In fact most parts of the mobile health Platform presented in our reference architecture could also be part of an eHealth Platform.

An important question is how mobile health compares to eHealth. In the end, eHealth (assumed to be connected through a fixed infrastructure such as asymmetric digital subscriber line (ADSL)) and mobile health will need to work together as much as possible. The mobile health platform does not necessarily differ that much from an eHealth Platform.

There are logistical advantages in mass producing mobile health devices that can be shipped all over the world and activated at first use, independent of place and time and operator, while providing a secure connection to the mobile health Service of choice. That secure connection is independent of any private business or individual IT infrastructure so is highly controlled but still flexible.

This mobile health reference architecture provides concepts for high levels of security while still being user friendly, which can lower the barriers to adoption. Mobile health provides both the highly demanding security requirements for Healthcare as well as the need for devices that everybody can use.

But will this Mobile Operator based mobile health reference architecture be able to compete with the app store model of mobile health? In theory, apps that are used independently of the network and are just downloaded on a Smartphone or gateway device will be able to provide similar secure connections and functionality. However the security will be more dependent on the operating system of the device or needs to be handled completely in the application and that means more work for application developers. The operator based mobile health model provides greater standardisation and flexibility as well as a worldwide infrastructure for provisioning of mobile health Services. Those advantages give the Mobile Operators a head start if they collaborate to develop this mobile health market for the benefit of all.

8 Conclusion

This report provides a high level reference architecture that shows that Mobile Operators can use their unique assets to play a major role in mobile health. The involvement of Mobile Operators and their unique assets provides added value to Clinicians, Healthcare Providers as well as to mobile health Service Providers and mobile health Application Providers, and ultimately an enhanced mobile health service to the Patient compared to a traditional Healthcare Provider.

Mobile operators have over 25 years' experience of managing billions of mobile devices within networks that cover over 95% of the world's population, they develop user centric solutions that are secure, interoperable and consistently updated. The main assets of the Mobile operators are available worldwide and are developed from globally standardised building blocks.

Healthcare services of the future will move from a centralised, doctor lead approach towards a focus on patient and a dependence on self-management. If this shift in focus is going to be successful then systems need to be provided that will enable patients to access healthcare wherever and whenever it is required in simple and easy to use way. The only viable option for providing this level of access is through a mobile device.

Along with providing mobility, Mobile Operators can leverage a number of network capabilities that are readily available in the other services they provide. Integrating them into future mobile health developments will enable Mobile Operators to provide advanced secure mobile health devices and services worldwide. These capabilities will allow mass market distribution, remote provisioning, remote device and application management, flexible billing and possible location based services. The combination of these abilities will enable Mobile Operators to provide mobile health services with enhanced user experiences when compared to 'over the top' mobile health solutions.

Confidence in the security of patient data will be critical to the success of future mobile health products and services. Whether the data is being communicated over the mobile network or stored within the mobile health platform, strong, robust measure will need to be implemented that meet the requirements of users and regulators. The mobile industry has a proven track record of delivering secure networks and has developed new enhanced end to end security mechanisms to meet the needs of other adjustment markets, e.g. GBA and applications that uses the UICC (better known as the SIM card). The implementation of these security mechanisms should be considered in the deployment of future mobile health products and services.

The standardisation of M2M capabilities will also provide an opportunity to simplify the implementation of mobile solutions for service providers and developers. A number of the leading standards organisations have aligned to form a group called One M2M[8] with the aim to limit fragmentation and duplication of the standards that are being developed. The aim is to develop common protocols and API's, security, privacy and charging aspects and interoperability capabilities. Mobile Operators should continue to support these activities as it will improve the economies of scale in delivering mobile health service and their speed to market.

[8] www.etsi.org/WebSite/NewsandEvents/2012_01_M2M_Global_Initiative.aspx

Within this document the mobile health platform is described as a single entity, however it is likely that this will be a number of specialised separate elements. It should be possible for a Mobile Operator to provide all of these elements, but they should consider if there are any service providers with experience in the healthcare that industry that could support the integration.

In essence, Mobile Operators already have the secure networks and capabilities to provide a user centric mobile health solution. Although healthcare has its own high priority requirements, the standardised capabilities that are being developed for other market verticals will provide the capabilities needed to meet these new needs. Mobile Operators are already implementing mobile health, and if they continue to focus on standardisation work that is underway and their key network assets then they will be able to significantly differentiate themselves from traditional healthcare providers. Close partnerships with Mobile Operators will offer healthcare providers the gateway to the mass market to provide the user centric and remotely managed secure mobile health services of the future.

9 References

- Global Platform Card Specification v2.2.1
- GBA (http://en.wikipedia.org/wiki/Generic_Bootstrapping_Architecture)
- 3GPP (http://www.3gpp.org/ftp/Specs/html-info/33220.htm)
- SIM alliance whitepaper: Open Mobile API specification v1.2, 12-07-2011
- Mobile Contactless Payments (MCP) Service Management Roles, Requirements and Specifications, (EPC 220-08, Version 2.0) of October 2010,
- Common smart card specification IAS-ECC (*Identification Authentication Signature – European Citizen Card*)

10 Abbreviations

- **3GPP** 3rd Generation Partnership Project
- **API** Application Programming Interface
- **ADSL** Asymmetric digital subscriber line
- **BSF** Bootstrapping Server Function
- **B2B** Business to business
- **CDR** Call Detail Record
- **EHR** Electronic Health Record
- **ETSI** European Telecommunication and Standardisation Institute
- **GBA** Generic Bootstrapping Architecture
- **GGSN** Gateway GPRS Support Node
- **GP** General Practitioner
- **GSMA** GSM Association
- **HCP** Healthcare Provider
- **HIPAA** Health Insurance Portability and Accountability Act
- **HITECH** The Health Information Technology for Economic and Clinical Health Act
- **HLR** Home Location Register
- **IEEE** Institute of Electrical and Electronics Engineers
- **IHE** Integrating the Healthcare Enterprise
- **IMEI** International Mobile Equipment Identity
- **IMSI** International Mobile Subscriber Identity
- **NAF** Network Application Function
- **NFC** Near Field Communication
- **MAC** Message Authentication Code
- **mobile health** mobile Health
- **MN** Mobile Node
- **MNO** Mobile Network Operator
- **OTA** Over the Air
- **PAN** Personal Area Network
- **PDN** public data network
- **PHR** Personal Health Record
- **PIN** Personal Identification Number
- **PKI** Public Key Infrastructure
- **SLA** Service Level Agreement
- **SEPA** Single Euro Payment Area
- **SGSN** Serving GPRS Support Node
- **SP** Service Provider
- **TLS** Transport Layer Security

- **TLS-PSK** TLS using a Pre-Shared Key (PSK)
- **TTP** Trusted Third Party
- **UICC** Universal Integrated Circuit Card
- **USSM** UICC Security Service Module
- **WCDMA** Wideband Code Division Multiple Access
- **XML** Extensible Markup Language

www.gsma.com