ETSI TR 102 732 V1.1.1 (2013-09)

Technical Report

Machine-to-Machine Communications (M2M); Use Cases of M2M applications for eHealth

Reference

DTR/M2M-00005ed111

Keywords

ageing, emergency, health, interworking, M2M, use case

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Machine-to-Machine communications (M2M).

The present document is a TR and therefore, the content is informative, but when referenced by a TS, the referenced clauses may become normative with respect to the content of the referencing TS.

1 Scope

The present document collects Use Case descriptions for eHealth applications in context of Machine-to-Machine (M2M) communications. The described Use Cases will be used to derive service requirements and capabilities of the functional architecture specified in ETSI TC M2M.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] IEEE 11073: "Health Informatic--Personal health device communication".

[i.2] BS 8521:2009: "Specification for dual-tone multi-frequency (DTMF) signalling protocol for social alarm systems".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

eHealth: generic term for a class of applications that serve the purpose of improving health care and medical services by means of electronic information or communications technology

NOTE: The definition of eHealth for the purpose of the present document covers many different applications.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ECG	Electrocardiography
EHR	Electronic Health Record
EMR	Electronic Medical Record

NOTE: Typically maintained and managed by the provider.

EMT	Emergency Medical technician
M2M	Machine-to-Machine

NOTE: Communications.

MVLBS	Measurement of Very Low Voltage Body Signals
PGP	Pretty Good Privacy

NOTE: Security protocol for email.

PHR	Personal Health Record

NOTE: Typically maintained and managed by the patient.

RMD	Remote Monitoring Device
RPM	Remote Patient Monitoring
SCL	Service Capability Layer
TLS	Transport Layer Security protocol

NOTE: Successor to SSL.

WAN	Wide Area Network

4 M2M applications for eHealth

4.1 General description of M2M applications for eHealth

M2M applications for eHealth enable:

- the remote monitoring of patient health and fitness information;
- possibly the triggering of alarms when critical conditions are detected;
- in some cases also the remote control of certain medical treatments or parameters.

In order to acquire the information on a patient's health or fitness, appropriate sensors have to be used. For this reason, the patient or monitored person typically wears one or more sensor devices that record health and fitness indicators such as blood pressure, body temperature, heart rate, weight, etc., see Figure 1. Because typically these sensors have to cope with severe limitations on form factor and battery consumption, in most cases it is expected that they need to forward the collected data with some short range technology to a device that can act as a aggregator of the collected information and a gateway towards a back-end entity that is supposed to store and possibly react to the collected data. It is also possible that the sensors used to monitor parameters related to the health condition of the patient are located somewhere in the environment of the patient.

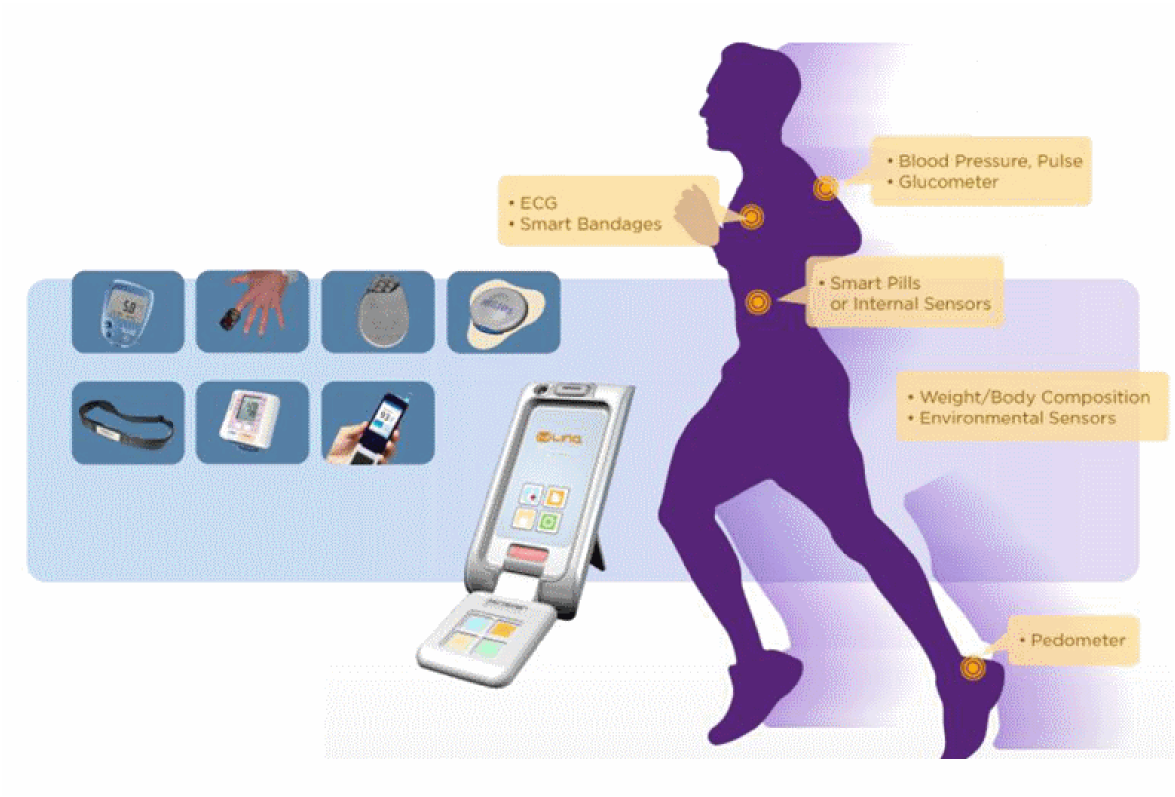

Figure 1: Wearable sensors

This model of aggregating and forwarding collected information by a gateway device is referred to as gateway model in what follows. Wearable sensors often use short-range wireless links to a gateway device that has WAN connectivity. For instance, the gateway could be a fixed device such as a PC or set-top box, or a mobile device like a cell phone or a standalone device carried on a keychain or worn around the patient's wrist or neck. The gateway device can then send health data to a back-end server over the WAN, where it can be viewed by doctors and patients.

In other cases the gateway model might not apply. For instance when sensors would have capabilities to support a link to a back-end server directly without the help of a gateway device. This could apply to sensors that have an integrated WAN communications module.

4.2 Specific examples for M2M applications for eHealth

4.2.1 Disease management

A common use of M2M applications for eHealth is to support the remote management of patient illnesses. The process of managing patient illnesses is termed disease management inhere. Examples include:

- Management of diabetes (tracking blood sugar levels, controlling insulin dosage).
- Management of cardiac arrhythmias (an example is the Cardionet system, which records infrequent abnormal heart rhythms and sends the data over the WAN for analysis).

In disease management applications health data is typically collected by one ore more sensors and sent to a back-end server in regular intervals. The amount of data to be collected and forwarded to the server per time and the frequency of reporting depends on the particular needs to manage a specific disease. For some disease management applications an alarm function is needed to trigger an alarm to get attention of a doctor or the patient in order to react to a critical health condition. The tolerable latency for these kind of alarms depends on the specific needs to react (e.g. life threatening versus just impacting comfort). It is also important to be able to configure disease management devices (e.g. adjust the reporting period) and to verify correct operation of the system (check on correct functioning of the sensors as well as verifying connectivity).

4.2.2 Aging Independently

M2M application for eHealth can enable the elderly to live an independent life and remain in their homes in cases when normally assistance would be needed. Examples include:

- Remote monitoring of patient vital signs (pulse, temperature, weight, blood pressure) to minimize the number of required doctor office visits.
- Making sure that patients are taking their medications according to the required schedule.
- Tracking the activity level of seniors (e.g. time spent in bed each day, amount of daily movement in their homes) as a way of inferring their overall health and detecting changes that may require a doctor's or some other person's attention.

As in the case of disease management, M2M applications to support independent ageing or elderly will require the monitoring of health or behavioural data. The main mechanism here is also the continuous collection of that data and the forwarding to a back end server that provides the interface for doctors or caring people (family, loved ones) to get attention when needed.

4.2.3 Personal fitness and health improvement

M2M applications for eHealth can be used to record health and fitness indicators such as heart and breathing rates, energy consumption, fat burning rate, etc. during exercise sessions. They can also be used to log the frequency and duration of workouts, the intensity of exercises, running distances, etc. When this information is uploaded to a back-end server, it can be used by the user's physician as part of their health profile, and by the user's personal trainer to provide feedback to the user on the progress of their exercise program. It allows to adapt exercise programs or physiotherapy more precisely and more quickly to the needs of the patient/user.

In contrast to the M2M applications in support of disease management and ageing independently, the support of personal fitness and health improvements will most likely require less frequent logging or uploading of data and is more tolerant to delays in uploading as it is not very critical when the data is available.

5 eHealth use cases

5.1 Remote Patient Monitoring (RPM)

5.1.1 General Description

At the highest level the generic remote monitoring detailed use case focuses on the communication of patients' remote device sensor measurements to their clinicians' supporting systems, EHR and/or their personally controlled health record (PHR). Within the Machine to Machine scope, the use case is focused on the transport of messages between the remote monitoring devices and the M2M service capability provider layer. Architecturally, elements or interfaces above the service capability provider layer, such as supporting electronic systems used by the clinicians or intermediaries, is beyond the scope of the present document and are included only to provide systematic grounding. Issues highlighted include, two way message traffic, network availability for critical missions, network information security, secure device addressing and message tagging.

5.1.2 Stakeholders

Patient: The "patient" may be any individual or surrogate, who could use a *remote monitoring device* to gather measurements, data, or events. The patient measurements may be taken in various clinical such as in hospitals or non-clinical settings such as at home, at work, at school, while traveling, or in assisted living facilities.

Remote Monitoring Device (RMD): Electronic M2M device with a sensor, user interface and/or actuator and an interface into the M2M network. The device collects patient information and communicates to the appropriate M2M service capability provider and/or M2M application via the M2M network. A RMD may communicate with these entities via a M2M gateway, too. Further, the device may receive and/or act upon commands from the M2M service capability provider and/or M2M application or provide information to the Patient. Low power, low complexity protocols are likely required for these devices.

M2M service capability provider: Network entity that provides M2M communication services to the M2M application entities. These applications may support specific functional capabilities which assist in facilitating health information exchange activities. Additionally, the M2M service capability provider communicates with the Remote Monitoring Device to collect data or send commands.

M2M application entity: Term created to bundle together, and treat as a single system element, stakeholders above the M2M scope. High-level application such as free-standing or geographic health information exchanges, data analysis centers, integrated care delivery networks, provider organizations, health record banks, or public health networks and/or specialty networks are all examples of M2M application entities. The term M2M application entity also includes the following typical RPM stakeholders such as the:

> **Care Coordinator:** The care coordinator includes individuals or applications under clinical supervision that monitor the information received from the patient's device(s). A care coordinator may intervene if measurements or alerts indicate that there has been a change in the patient's health status, or if the measurements fall outside of a predetermined range. The care coordinator may also inform the patient's clinician if measurements indicate a potential health issue.
>
> **Electronic Health Record:** Either a medical record maintained by the health care system in digital form for an individual (EHR) or a medical record maintained by the individual for himself or another (PHR).
>
> **Clinician:** The clinician includes physicians, nurses, nurse practitioners, physician assistants, psychologists, and other clinical personnel who clinically evaluate the remote measurements determine appropriate clinical interventions if needed to manage patient care.

5.1.3 Scenario

Initialization

The remote monitoring device is prepared for use and communication by the action of the patient or clinician. This may involve physically attaching or placing the device, registering the device, setting up the communications channels to M2M application entities, setting up the communications capabilities of the device and providing for secure communications. For life-critical applications, the initialization may require secure authentication and device state verification of the RMD by the M2M service capability provider and/or the M2M application entity.

Patient Telemetry

The remote monitoring device gathers patient measurements, data and or events. Data may be communicated each time the device gathers the data, accumulated measurements may be communicated periodically (e.g. hourly, daily), or data may be delivered upon request or upon certain events.

Further, life threatening or otherwise critical measurements or events may need to be detected and sent on a guaranteed time critical and ordered basis. For these measurements, the device state of the RMD may need to be frequently verified by the M2M service capability network and/or the M2M applications entity.

Data Packets are sent to the M2M network application and routed up to M2M application entities may be managed by the clinician, Care Coordinator or EHR.

Telemetry data or even the existence of medical telemetry is patient information and as such may need to be protected for privacy.

In some applications, multiple RMDs would send patient telemetry data, which would be collected, aggregated, and/or otherwise further processed, by a M2M gateway, and only such collected, aggregated, and/or otherwise processed data may be sent to the M2M service capability provider and/or the M2M application entities.

Remote Configuration

The remote monitoring device may be configured by via the M2M network by the M2M application entities. The configuration capability could span simple parametric changes, such as, reporting rates, event or alarm trigger levels, and dosing levels to downloading and securely restarting new operating SW.

Secure, ordered, and confirmed messaging would be required.

Acknowledgement, from the RMD, of the remote configuration message, and, further, of achieving the desired configuration state, would be desired, too.

In some applications, multiple RMDs would be remotely configured, with either same or individualized settings, by the M2M service capability provider. M2M gateways may distribute some or all of such configuration messages to multiple RMD devices that are connected to them.

Device configuration or even the device type is patient information and as such may need to be protected for privacy.

Remote Control

The RMD may be capable of acting on or communicating with the patient. The control may include time critical or ordered elements to provide one time dosing or electrical pulses to simple text messages requiring patient action or response.

For most applications, remote control messages should be secure. Further, the RMD that receives a remote control message may need to be verified for authenticity and/or device integrity state.

In some applications, multiple RMDs may receive same or individualized remote control messages from the M2M service capability provider. M2M gateways may distribute such multiple remote control messages to the RMDs that are connected to them.

5.1.4 Information Exchanges

Registration

The device communicates with the M2M service capability provider to provide for initialization of the device into the M2M system. Registration includes the capability to maintain information describing the remote monitoring device, the patient being monitored (if privacy is not considered as an issue according to policies and patient pre-approvals), and the M2M application who will be reviewing the monitoring data. For example, this may include registering the device with the manufacturer or data intermediary and performing other functions to uniquely identify the device. Registration may also include registering data that can be used to verify the state of the RMD device by the M2M service capability provider.

Data Retrieval

Capability to locate and retrieve requested data subject to access rights and local policies. The remote monitoring data is received via the M2M service capability provider and associated with the appropriate data recipients.

Data Delivery

Capability to securely deliver data to the intended device or M2M service capability provider and confirm delivery, including the ability to route data based on message content, if required. For example critical life events have to be routed via high reliability channels with guaranteed timely delivery.

5.1.5 Potential new requirements

5.1.5.1 Device Initialization and Registration

This clause describes the steps necessary to initialize and register the RMD and establish communication. The steps in this clause may require action by the patient and clinician.

At a high level the following steps are:

1) The RMD may require physically attaching the device to a laptop or other device to enable the initial transfer of information.

2) The RMD should perform initial power up sequence that may perform basic diagnostic checks to ensure the device is functioning properly.

3) In certain life-critical applications the device may be required to perform a secure start-up procedure that includes integrity checking. Failure of the health device/application to verify the device integrity should block registration, and optionally alert the user of a device failure.

4) Upon successful initialization the RMD initiates registration procedures.

5) The patient and provider health device/applications are independently authenticated and registered with the service capabilities layer and declare/confirm their service class (and device class) requirements.

6) If the request is valid, the systems are authenticated and authorized.

7) Name/address translation are established for routing purposes.

8) Communications capabilities and configuration are established.

The functional mapping of the above steps are as follows:

1) The RMD device may require a physical connection (e.g. via USB) for initial device configuration.

2) Life-critial RMD validation should perform integrity verification based in a trusted execution environment.

3) Failure of the RMD initialization should trigger an alarm signal on the device.

4) The M2M Application (in the network and device domains) registers with the service capability entity in order to establish operation.

5) The M2M Gateway (if applicable) forwards (routes) the registration request to the network (establish access to needed capabilities in the network).

6) The appropriate Service Capability entity performs the registration, authentication, and authorization of the M2M applications and provides connectivity with other capabilities.

7) The appropriate Service Capability entity monitors and logs initial registration and deactivation of the M2M Device or Gateway. This entity may also perform the name translation.

8) The appropriate Service Capability entity provides name and address mapping and monitors device status.

9) The appropriate Service Capability entity extracts network addresses from the M2M application. It also provides network selection (based on service class and other factors) for devices that support multiple networks or communication services.

10) Registration of a RMD should support the secure storage of sensitive patient data.

5.1.5.2 Device Communications

5.1.5.2.1 Remote Control and Configuration

This clause describes the remote communication between a user (patient or provider) and an M2M Device and/or application. Examples of this communication include remote configuration and control of the device, providers querying a remote monitoring device for a reading or a patient updating his EMR (or health database) with some relevant information.

The following steps are executed for this type of communication:

1) Provider or patient logs into the secure messaging system using their user identity and password (and any other security credentials).

2) The user (patient or provider) select the action and the device they would like to communicate with (in some cases, the device does not need to be online at the time).

3) The user enters the new information or query for the device.

4) The application contacts the device with the request. This is either done in real time or at a later time when the device is connected.

5) The sender of the information is informed of the status of the request and provided the information (if applicable).

The functional mapping of the above steps are as follows:

1) A life-critical M2M RMD should provide secure transmission and reception of message exchanges by use of a secure protocol.

2) The secure messaging AAA entity in the network authenticates and authorizes the user.

3) Message is parsed by the network for the receiving device identity.

4) The appropriate Service Capability entity confirms that the device is registered and looks up the mapping of name to network address. It also provides network selection (based on service class and other factors) for devices that support multiple networks or communication services.

5) The appropriate Service Capability entity checks the current status (reachable or not) of the device and the last known route.

6) The appropriate Service Capability may also provide charging records for use of capabilities.

7) The appropriate Service Capability entity monitors and provides configuration, performance, and fault management (monitors message exchange for errors, faults, etc.) functions.

8) The appropriate Service Capability entity will transport messages between the secure messaging application and the M2M Device, through an M2M Gateway if necessary. It handles retransmissions, reports errors, hides unnecessary information and monitors delivery status.

9) The appropriate Service Capability entity stores copies of messages and delivery status, error reports, etc.

10) The M2M Gateway (if applicable) forwards (or routes) the message to network.

11) The M2M Device receives the message.

12) The appropriate Service Capability entity will update the sender with the message status and requested information (if applicable).

13) A RMD should provide time critical message handling and delivery.

14) A M2M RMD should provide secure storage for private patient information.

5.1.5.2.2 Patient Telemetry (Data Retrieval and Delivery)

This clause describes the communication from an RMD (or application on a RMD) to a Provider (or M2M service).

The follow steps are executed for this type of communication:

1) According to the predefined schedule or based on some event (periodic or on demand-mode of message reporting), the device "wakes up" and registers with the network if not already connected.

2) If the network is unavailable then the message is stored and attempts are made to connect to the network at pre-defined intervals.

3) Once connected, the message is prepared and sent.

4) The message is delivered (if delivery fails, autonomous retransmissions are attempted).

5) The message delivery status is reported back to the sending M2M Device (or application).

6) Life threatening or otherwise critical measurements or events may need to be detected and sent on a guaranteed time critical and ordered basis.

7) Life threatening RMD may need to be frequently verified by the M2M service capability network and/or the M2M applications entity.

8) Life threatening RMD may need to support communications with emergency service or provide routing of specialized messages within the M2M system (ie. notification of critical patient information to emergency service responders.

The functional mapping of the above steps are as follows:

1) Prerequisite: The M2M Device wakes up and registers with the network (detailed in previous clause).

2) The M2M Device prepares and sends the message.

3) The M2M Gateway (if applicable) forwards (or routes) the message to network.

4) The appropriate Service Capability entity performs routing to the service capabilities as needed and may also provide charging records for use of capabilities.

5) The appropriate Service Capability entity abstracts name and connection information from the M2M application and management functions. It also monitors and provides configuration, performance, and fault management (monitors message exchange for errors, faults, etc.) functions.

6) The appropriate Service Capability entity will transport messages between M2M Device, M2M Gateway, and the M2M Application (in the network). It handles retransmissions, reports errors, hides unnecessary information and monitors delivery status.

7) The appropriate Service Capability entity stores copies of messages and delivery status, error reports, etc.

8) The M2M Application (device or network domain) receives the messages.

For a life-critical RMD the following functionality applies:

1) A M2M RMD should support reliable and guaranteed delivery of a message.

2) A M2M RMD should support accurate and secure time synchronization.

3) A M2M RMD should support selection of and use of appropriate communications channels to ensure reliable transmission of critical life event(s).

4) A M2M RMD should provide ordered message delivery based on prioritized service capabilities handling.

5) A M2M RMD should support priority communications to emergency services.

5.1.5.3 Derived potential new requirements

The following are potentially new requirements for the M2M System:

1) Integrity validation based on a trusted execution environment

2) Alarm signalling to indicate initialization failure

3) Support for secure storage of sensitive data

4) Support for secure communication via a secure protocol

5) Support for time critical message handling and delivery

6) Support for secure time synchronization

7) Support for ordered message delivery based on prioritized service handling

8) Support for priority communication to time-sensitive health services

Detailed high level flows and functional mappings onto elementary communication entities are described in the previous clauses, to add rational of why these items were identified as potential new requirements.

5.2 Patient - Provider Secure Messaging

5.2.1 General Description

The term "patient - provider secure messaging" includes secure messages between patients and providers that involve at least one M2M Device or Application. The use of the term "provider" includes both clinicians and clinician support staff. This use case includes the following messaging scenarios:

1) M2M Device (or system/application) to M2M Device (or system/application)

2) M2M Device (or system/application) to User (patient or provider)

3) User (patient or provider) to M2M Device (or system/application)

The use case does not include messaging between patient and provider that are user to user. These could include things such as symptom and treatment questions and answers, providing manually gathered information or questions on existing self-monitoring and/or chronic care regiments, etc.

This form of communication has the ability to enhance general care as well as the management of chronic care conditions. The communication could occur in a number of ways, but the most common would be through secure messaging. Personal health information included in these messages would need to be provided using a secure sending and receiving environment. Such information, while it is stored and handled on M2M devices and systems, should also be protected for integrity and/or confidentiality. M2M devices and system nodes (e.g. gateways, servers, etc.) that handle such information should be secure and trustworthy.

In order to support this type of eHealth application, the following, high level, requirements (or scenarios) have to be supported:

- Support for Patient-Initiated Communication (via Patient's M2M Device)

- Support for Provider-Initiated Communication (via Provider's M2M Application Server or Device)

- Support for Policy, Event or Schedule Based Communication

- Support for Routing of Data Based on Content

- Interoperability (Data Format, etc.)

5.2.2 Stakeholders

This use case includes the following stakeholders:

- Patient - those who receive healthcare services.

- Patient Caregivers - Caregivers, patient advocates, surrogates, family members, and other parties who may be acting for, or in support of, a patient receiving or potentially receiving healthcare services.

- Provider:

    - Clinician - Healthcare providers with patient care responsibilities, including physicians, advanced practice nurses, physician assistants, nurses, psychologists, pharmacists, and other licensed and credentialed personnel involved in treating patients.

    - Clinician Support Staff - Individuals who support the workflow of clinicians. For example, office staff that initially receive and evaluate messages from patients and take steps to provide a response.

- Healthcare Entities - Organizations that are engaged in or support the delivery of healthcare. These organizations could include hospitals, ambulatory clinics, long-term care facilities, community-based healthcare organizations, pharmacies, etc.

- Medical Monitoring/Telemetry Device - a device for monitoring and relaying health related data from the patient to the provider or other healthcare entity.

- EMR/PHR/Health Database - the electronic application, software, or utility that monitors and helps manage the care of a patient.

- EMR/PHR/Health Database Suppliers - Organizations which provide specific EHR and PHR solutions to providers and patients such as software applications and software services.

Medical Device Suppliers - Organizations that provide the medical devices and/or tools to aid in the treatment of health and disease conditions. These devices or tools can support physiological monitoring, secure messaging, and messaging content.

5.2.3 Scenario

5.2.3.1 Secure Messaging Categories and Platforms

5.2.3.1.1 M2M Device (or system/application) to M2M Device (or system/application)

This message category includes messages that are sent autonomously by a health monitoring device, medical record system, sensor, etc. to another M2M Device or Application. This category does not involve any user intervention. Examples of this include periodic reports of physiological data from patient monitoring devices to the provider's EMR (or health database). It may also include the provider's EMR system (or a similar application) autonomously sending requests for readings or configuration information to the patient's health monitoring device.

5.2.3.1.2 M2M Device (or system/application) to User (patient or provider)

This message category includes messages that are sent from an M2M Device or Application where the recipient is a user (patient or provider). Examples of this include a patient's health monitoring device alerting the provider or an emergency care centre of critical vital signs as well as a provider's EMR system autonomously sending reminders to the patient regarding annual physical examinations, screenings, immunizations, or other treatment regiments.

5.2.3.1.3 User (patient or provider) to M2M Device (or system/application)

This message category includes messages that are sent from a patient or provider to an M2M Device or Application. Examples of this include a provider querying a remote monitoring device for a reading, configuring such a device, or a patient updating his EMR (or health database) with some relevant information.

5.2.3.1.4 Messaging Platforms

Two of the three messaging categories discussed above may involve different platforms where one side is the M2M Device or Application and the other side is a more generic computing platform that supports the secure messaging system or application where messages can be sent or received by the patient or the provider. For example, a patient may have a health monitoring device that reports physiological data and have a separate secure messaging application that is web based and/or runs on a laptop for the manually initiated messaging. Alternatively, a common platform may support both functionalities. Of course in either case, proper procedures need to be employed in order to ensure secure handling and the confidentiality and integrity of the data.

5.2.4 Information Exchanges

5.2.4.1 Initial Setup for Secure Messaging

5.2.4.1.1 User Initiated Communication

Before using the secure messaging capability, patients and providers will take steps to setup their access to the system. This includes the establishment of the necessary security information (user identification credentials, etc.) as well as the installation of any necessary security applications (or protocols) that need to run on the end point system (such as a laptop, Smartphone, etc.).

This messaging activity may utilize existing security mechanisms (such as access and application security protocols) in the network, and may require additional M2M specific security capabilities such as platform validation. In addition, the system may need to address the low power and complex security requirements for certain devices classes such as body sensors, etc.

The secure messaging system can be realized in several ways:

- Point-to-point
  - This type of mechanism provides interactions directly between two systems without the need for intermediate routing functions. These endpoints could be part of different messaging applications or different platforms with a common application.
- Web based
  - Relies on the Internet to transmit secure messages and is supported by common or separate (and/or distinct) applications for the patient and the provider.

5.2.4.1.2 Device Initiated Communication

Prior to installation of the health device/system and application, the provider of the system will establish agreement from the service capability provider on the set of capabilities that the application requires or has access to.

This will include information such as Service and Device Class requirements, access technology support, authorized users, etc.

At the time of installation of the device or system, some configuration is necessary to provide for the appropriate connectivity, user access, etc. In many cases, much of, if not all of the configuration can and should be automated (self-configuring) such that the user does not have to have a detailed knowledge of the underlying technology. There may be a limited amount of configuration needed but typically that can be handled with an easy to use interface that prompts the user to enter the necessary information. It is likely that this necessary manual configuration will be more focused on the user access to the device (or application/system) and related properties.

5.2.4.2 Patient Initiated Communication

5.2.4.2.1 User Initiated Communication

Patients can initiate communication to the provider's EMR or health database application using the secure messaging tool for a variety of purposes. Examples include providing manually gathered information on existing self-monitoring and/or chronic care regiments.

To send these messages, the patient has to log into the secure messaging system using their user identity and password (and any other security credentials) and compose and send the message.

When the provider's EMR or health database application receives and processes the message from the patient, it may alert the provider of the update and potentially relay the information to other relevant stakeholders. The patient will be informed that the message was received and processed with an autonomous response from the EMR or, if necessary, the provider will contact them directly with a secure message or a telephone call.

5.2.4.2.2 Device Initiated Communication

Patient health monitoring devices can initiate communication (autonomously) to the provider using the secure messaging mechanism for the following purposes:

- Periodic reports of physiological data (from a variety of medical devices) based on a predetermined schedule
- Event (or threshold) based reports of physiological data

This device will also use a secure messaging mechanism to transport this data. The necessary security capabilities will therefore need to be supported in the M2M functional architecture.

The autonomous report message is delivered to the M2M application/system of the provider. This could be a system on the premises of the provider's office (or hospital, etc.) or at an information center that provides storage and data collection for the provider. This data will be logged into the EMR of the patient and the provider will be alerted that this report has been received. This may be done with any non-secure messaging system since it will not contain any private patient data.

If the report is a periodic report of data, the provider need not take immediate action on this report. It is likely that the data will be reviewed as part of the next scheduled office visit of the patient.

In general, event based reports will fall into two categories. The first category includes events that are emergencies and require immediate attention. The second category is an event that does not need immediate attention but rather gets logged into the providers EMR or health database application. Potential actions for each of these event based reports are as follows:

- Emergency Event Reports - in this case the M2M Device will be configured to contact emergency services as well sending the provider an urgent secure message. The information provided to emergency services will include the nature of the emergency, patient information, and patient location.
- Non-Emergency Event Reports - in this case the M2M Device will report the event data to the provider's EMR or health database application and the provider will be alerted that this event was logged in the system. The provider will evaluate this report either at the next scheduled office visit or check-up or sooner depending on the event criteria setup in the system.

Typically, the device can be configured (possibly by default) to request acknowledgement that the message was delivered and/or read by the recipient. The lack of this acknowledgement, especially in the case of an event based report (which may be critical in nature), should prompt alternative action from the device. This action may include attempting communication with a alternate access technology, forwarding the report to an alternate emergency care center or provider, forwarding to other caregivers (family, etc.), as well as alerting the patient directly.

5.2.4.3 Provider Initiated Communication

5.2.4.3.1 User Initiated Communication

Providers can initiate communication with the patient's health monitoring device for a number of reasons. Examples of this include a provider querying the device for a reading or for configuring such a device.

To send these messages, the provider has to log into the secure messaging system using their user identity and password (and any other security credentials) and compose and send the message to the patient device or system.

5.2.4.3.2 Device Initiated Communication

The providers EMR system (or similar application) can autonomously initiate communication with the patient for a number of reasons. This communication may be directed to the patient or to the patient's health monitoring device. The reasons include the following:

- Reminders for patients for annual physical examinations, screenings, immunizations, etc.
- Issue new reporting criteria to the patient health monitoring device to change reporting schedule, event threshold levels, etc. (may need to be initiated manually).
- Implement a new measurement requirement/capability for the health monitoring device (may need to be initiated manually).

A traditional (unsecured) email or text message can also be used to notify the patient that a secure message has been sent to them and they should check the secure message system to retrieve it. In addition to alerting them of a message for them, they can also be notified that updates have been made to their health monitoring device program (or application). Use of traditional email or text messaging helps ensure that the patients get the messages even when they may not have access to or when they are not logged in to their secure message system.

5.2.4.4 Other Information Exchanges

5.2.4.4.1 Routing Data Based on Content

In the above scenarios, the system can be configured to allow the routing of data based on content. A few examples of this include:

- For an event (or threshold) based report from a health monitoring device, in addition to the message going to the provider's office, it can also be routed to a emergency room or critical care center if the message indicates an urgent life threatening condition.
- If the provider is ordering new tests or a new prescription, the message can be sent to the lab or the pharmacy in addition to the patient to expedite the service.
- Messages from the provider may also be routed to authorized caregivers or coordinators, family members, etc. depending on the nature of the message.

In order to support content based routing, the third parties that may receive this information have to be pre-authorized by the patient and the system.

5.2.4.4.2 Interoperability (Data Format, etc.)

Depending on the particular type of information being conveyed between the patient and the provider in the secure messages, the data may be provided using different formats. For manual communication messages, a structured template (drop down menus, etc.), a non-structured template (free text), or a combination of both may be used. The messaging system should provide for a logical separation of data and in this way, will facilitate improved information flow.

For autonomous communication messages, medical data such as measured readings from the health monitoring device (blood pressure, glucose, etc.) should comply with a standard which defines the format and structure of this information. This provides for interoperability between systems and applications.

There are a number of efforts currently underway to establish a common standard for medical records and data that may be used. These efforts include HL7, European Institute for Health Records (EuroRec Institute), etc.

5.2.5 Potential new requirements

5.2.5.1 Updates to Security Protocols

Current secure messaging suites such as PGP and TLS may not provide a sufficient framework to handle trusted communication. There are regulations concerning the storage, transmission, or destruction of electronic health information. These regulations are inconsistent across different jurisdiction regions. Therefore, enhancements may be necessary for handling trusted communication.

Also some eHealth devices or sensors may not be able to support the necessary hardware and/or software, due to their size and processing limitations. In such cases, the capillary networks and gateway need to support the requirements.

Specifically, the system needs to support the following requirements in order to secure the information exchanges:

- Device security and trust
- Confidentiality and privacy of information exchanged
- Integrity of information exchanged
- Protection (for integrity and confidentiality) of data while in storage on devices
- Protection of data when processed on devices

5.2.5.2 Portability of Connection

The use of M2M Devices for monitoring health related information is not confined to the residence of the patient. The M2M Device and the supporting system (and application), will provide the ability to connect to M2M Gateways (or equivalent components) in other locations and thereby establishing connectivity to the network and the recipients of data reports and/or messages. In addition to the ability to connect to alternate M2M Gateways, the device will ensure that the gateway is a secure and trusted system that will support the secure transfer of information. This requirement may or may not include the requirement to have continuous connectivity. This would imply that the device/connection can support handovers between different gateways, base stations, and/or access technologies.

5.2.5.3 Location Tracking

Coupled with the requirement for portability discussed in the clause above, the M2M Device and the supporting system (and application), will provide the ability to track and report the patients location. This information may be critical in emergency situations to provide location information to EMT or ambulance services, proximity to nearby hospitals, etc.

5.2.5.4 Rationale

Detailed high level steps and functional mappings onto elementary communication entities are described in the succeeding clauses, to add rational of why these items were identified as potential new requirements.

5.2.5.5 Establishment (Registration) of Secure Messaging Capability

5.2.5.5.1 Device Registration

This clause describes the steps necessary to establish the secure messaging capability between health devices or applications and between these systems and the user. The devices/applications can include a patient's dedicated health monitoring device/application, the provider's EMR system, etc. The user can be the patient or the provider or their representative. The focus here is on the device registration. The registration for user device messaging is addressed in the next clause.

At a high level the following steps are required:

1) The patient and provider health device/applications independently authenticate and register with the service capabilities layer and declare/confirm their service class (and device class) requirements.

2) If the request is valid, the systems are authenticated and authorized.

3) Name/address translation are established (for routing purposes) and an activity schedule is logged (if the device requires network access only on a predefined schedule).

4) The device performs a self-configuration based on settings identified by the user or the network application. In some cases the device may need to be manually configured.

The functional mapping of the above steps is as follows:

a) The M2M Device/Application initiates a registration request.

b) The appropriate Service Capability entity establishes the connection and abstracts it from the M2M Application and management functions.

c) The M2M Gateway (if applicable) forwards (routes) the registration request to network (establish access to needed capabilities in the network).

d) The appropriate Service Capability entity performs the registration, authentication, and authorization of the M2M applications and provides connectivity with other capabilities.

e) The appropriate Service Capability entity monitors and logs initial registration of the M2M Device or Gateway.

f) The appropriate Service Capability entity provides name to network address mapping and monitors device status and "reachability".

g) The appropriate Service Capability entity abstracts network addresses from M2M application. It also provides network selection (based on service class and other factors) for devices that support multiple networks or communication services. This entity also considers the service class of the device for the purpose of network and communication service selection.

h) The device and the appropriate Service Capability entity coordinate messages in order to properly configure the device based on the particular application and patient requirements.

5.2.5.5.2 User Registration

This clause describes the steps necessary to establish the secure messaging capability between the patient and the provider for user to device or device to user communication. This communication can be done through an M2M Application running on a centralized system, a standard Internet device (laptop, smart phone, etc.) using a web based interface, or some other point-to-point system.

At a high level, the following steps are required:

1) Each user of the system (patient, provider, etc.) have to perform an initial registration in the secure messaging application

2) The registration includes establishing the identity of the user by collecting detailed personal information necessary for the security checks

The functional mapping is as follows:

a) Prior to user registration (possibly during device registration), the M2M Application will establish a list of authorized users for the device and application. In addition to general access, the level of access has to be noted. For example, is the user authorized to reconfigure the device in addition to being able to retrieve readings from it, etc. This information is stored in the Service Capability entity that is responsible for authorization and establishing connectivity to the other capabilities.

b) The user initiates a registration procedure within the secure messaging application.

c) The user provides personal information to establish the identity of the user as well as passwords and other security mechanisms.

d) The user identity is compared to the authorized list of users in the appropriate Service Capability entity.

e) This entity confirms the devices and applications that the user has been authorized to access as well as the level of access.

f) The user access information and the allowed device/application access is stored in the appropriate Service Capability entity for all future verifications.

5.2.5.6 Communication Use Cases (Patient or Provider Initiated)

5.2.5.6.1 User - Device Communication (User Initiated)

This clause describes the communication between a user (patient or provider) and an M2M Device and/or application. Examples of this communication are providers querying a remote monitoring device for a reading, configuring such a device, or a patient updating his EMR (or health database) with some relevant information.

The follow steps are executed for this type of communication:

1) Provider or patient logs into the secure messaging system using their user identity and password (and any other security credentials).

2) They select the action and the device they would like to communicate with (in some cases, the device does not need to be online at the time).

3) They enter the new information or query for the device.

4) The application contacts the device with the request. This is either done in real time or at a later time when the device is "reachable".

5) The sender of the information is informed of the status of the request and provided the information (if applicable).

The functional mapping is as follows:

a) The secure messaging AAA entity (a Service Capabilities entity) in the network authenticates and authorizes the user.

b) The appropriate Service Capability entity establishes the connection and abstracts it from the M2M Application and management functions.

c) The message is constructed and sent and it is parsed by the network for the receiving device identity.

d) The appropriate Service Capability entity confirms that the device is registered and looks up the mapping of name to network address. It also provides network selection (based on service class and other factors) for devices that support multiple networks or communication services.

e) The appropriate Service Capability entity checks the current status (reachable or not) of the device and the last known route.

f) The appropriate Service Capability may also provide charging records for use of capabilities.

g) The appropriate Service Capability entity monitors and provides configuration, performance, and fault management (monitors message exchange for errors, faults, etc.) functions.

h) The appropriate Service Capability entity will transport messages between the secure messaging application and the M2M Device, through an M2M Gateway if necessary. It handles retransmissions, reports errors, hides unnecessary information and monitors delivery status.

i) The appropriate Service Capability entity stores copies of messages and delivery status, error reports, etc.

j) The M2M Gateway (if applicable) forwards (or routes) the message to network.

k) The M2M Device receives the message.

The appropriate Service Capability entity will update the sender with the message status and requested information (if applicable).

5.2.5.6.2 Device Initiated Communication

This clause describes the communication from an M2M Device (or application) to another M2M Device (or application) or from an M2M Device to a user.

The follow steps are executed for this type of communication:

1) According to the predefined schedule or based on some event, the device "wakes up" and registers with the network if not already connected.

2) If the network is unavailable then the message is stored and attempts are made to connect to the network at pre-defined intervals.

3) Once connected, the message is prepared and sent.

4) The message is delivered (if delivery fails, autonomous retransmissions are attempted).

5) The message delivery status is reported back to the sending M2M Device (or application).

The functional mapping is as follows:

a) Prerequisite: The M2M Device wakes up and registers with the network (detailed in previous clause).

b) The appropriate Service Capability entity establishes the connection and abstracts it from the M2M Application and management functions.

c) The M2M Device prepares and sends the message.

d) The M2M Gateway (if applicable) forwards (or routes) the message to network.

e) The appropriate Service Capability entity performs routing to the service capabilities as needed and may also provide charging records for use of capabilities.

f) The appropriate Service Capability entity abstracts name and connection information from the M2M application and management functions. It also monitors and provides configuration, performance, and fault management (monitors message exchange for errors, faults, etc.) functions.

g) The appropriate Service Capability entity will transport messages between M2M Device, M2M Gateway, and the M2M Application (in the network). It handles retransmissions, reports errors, hides unnecessary information and monitors delivery status.

h) The appropriate Service Capability entity stores copies of messages and delivery status, error reports, etc.

i) The M2M Application (device or network domain) receives the messages.

It should be noted that there is a requirement that the Network or Application domain services are always available. The device however, may not always be connected and therefore store and forward and similar techniques may be required to ensure the delivery of messages and acknowledgements.

5.2.5.7 Device Maintenance

5.2.5.7.1 Software Update

This clause describes the requirements for updating the software or performing other maintenance type procedures on the M2M Device. This presumes that the device has the capability to support a type of "over the air" update using the device's access technology. It further presumes that the device has the ability to store backup version of the software and can "rollback" the software should there be a problem with the new update.

The following steps are executed for this operation:

1) The network identifies that a software update is available for the device.

2) The device is signaled that a software update is available.

3) Depending on the device configuration settings, the software update can be done automatically or may require the user/owner of the device to accept the update.

4) The network initiates the software update to the device. The validity of the software has to be confirmed by the device before it allows the update to begin.

5) The device restarts and begins execution of the new software.

The functional mapping is as follows:

a) The appropriate Service Capability entity, that is responsible for configuration management, is alerted that a software update is available for the device. This can be done through an established process between the network operator and the device/application supplier.

b) The appropriate Service Capability entity establishes a connection to the device and sends a message to the device that a software update is available.

c) The device will either accept, deny, or defer the software update in a manner defined by the device configuration settings (automatic update, prompted update, etc.).

d) Once device accepts the update, the Service Capability entity will download the update to the device.

e) The device will validate that the software update is valid and approved by using appropriate security measures (this Service Capability entity in the network is responsible for applying the security mechanisms to the software download).

f) Once the download is complete, the device will restart and begin execution of the new software.

Once restarted, the device will again register with the network and confirm its service class requirements and configuration.

5.3 Measurement of Very Low Voltage Body Signals (MVLBS)

5.3.1 General Description

In a Remote Patient Monitoring scenario where low voltage body signals need to be acquired for health remote monitoring purposes, the acquisition process could be really disturbed by radio transmission activities, e.g. GSM/GPRS, that can take place on nearest co-located radio parts of the same M2M device.

Where the health monitoring process is continuously applied to the patient, e.g. for discovering arrhythmias, the acquisition activity could be interfered by typical cellular radio communication activities performed by the M2M device.

It becomes highly important to avoid or reduce any possible interference on incoming body signals to achieve a reliable eHealth service, even if it is not characterized as a life saving service.

A mean to cope with unexpected disturbing radio transmissions is to concurrently sample a radio transmission indication signal in order to adjust the signals sampling process aiming at reducing the interference effects, e.g. by discarding or correct those received samples associated to active radio transmission indications, or shifting slightly the time of the signal sampling. Another way could be the control of the radio transmitter by suspending the radio transmission during time limited measurements, then resuming it at the end of the measurement session.

5.3.2 Stakeholders

Stakeholders are the same of the Remote Patient Monitoring use case.

5.3.3 Scenario

The scenario is the same of Remote Patient Monitoring but a very low voltage body signal acquisition is performed by the Remote Monitoring Device.

5.3.4 Information Exchanges

The information exchanged is the same of the Remote Patient Monitoring use case.

5.3.5 Potential new requirements

5.3.5.1 Non-interference with electro medical devices

The M2M system or parts of it, should avoid interfering with the detection and measurement of very low voltage signals to be acquired and used by the M2M Application (e.g. in case of eHealth applications where ECG body signals continuously measured by a wireless sensor body network can be heavily disturbed by nearest GSM/GPRS transmitters, belonging to the M2M Gateway of the electro medical device).

5.3.5.2 Radio transmission activity indication

Depending on the type of M2M service, all the radio transmitting parts (e.g. GSM/GPRS) of the M2M Device (or Gateway) have to provide a real-time indication of radio transmission activity to the application on the M2M Device/Gateway.

5.3.5.3 Radio transmission activity control

Depending on the type of M2M service, all the radio transmitting parts (e.g. GSM/GPRS) of the M2M Device (or Gateway) may be instructed real-time by the application on the M2M Device/Gateway to suspend/resume the radio transmission activity.

5.4 Telecare data traffic between home and remote monitoring centre

5.4.1 General Description

This use case is about enabling an IP communications link for telecare data (alarms, polling data, lifestyle monitoring events) and 2-way voice between the home and the telecare monitoring centre that provides interoperability between different in-home telecare equipments and remote monitoring centre solutions.

Special attention is needed for security and privacy since the link will be used for information that could be used to identify vulnerable individuals.

5.4.2 Stakeholders

This use case includes the following stakeholders:

- Consumer
- Monitoring Service Operator
- Monitoring service engineer/Installation Engineer
- Care provider

5.4.3 Scenario

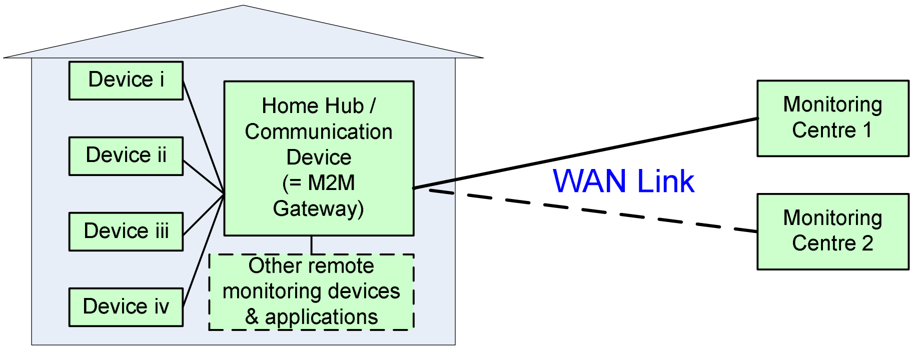
Device i
Device ii
Device iii
Device iv
Home Hub / Communication Device (= M2M Gateway)
Other remote monitoring devices & applications
WAN Link
Monitoring Centre 1
Monitoring Centre 2

Figure 2: Basic scenario for this use case

Most Telecare data will need to be transferred to support real-time critical alarm situations. Alarm situations normally initiate a voice call. In such alarm situations, link availability and reliability are major considerations (possibly requiring contingency solutions).

Some Telecare data may not be considered real-time critical (e.g. batched Activities of Daily Living data, reminder configuration information, etc.) which can be stored and forwarded later should a link not be available.

Increasingly, systems may also generate significant "engineering" traffic polling sensors to confirm they are still active, acquiring battery charge states, etc. Much of this will result in traffic over the WAN.

This use case would seek to establish endorsed requirements for, and specification of, an open protocol for transport of both the above data categories over IP data links by using an M2M SCL.

This use case addresses the interoperability related issues of the WAN interface between home hub (= M2M Gateway) or equivalent personal communications device and monitoring centre.

The scope of this use case can be broken down into two areas:

1) IP connectivity and message definition for alarms and control messaging over the WAN

2) IP connectivity to include streaming for voice or othe real-time interactive streaming data

Generic Process

It is recognized that the bulk work that needs to be accomplished in these examples is independent of the telecare domain. Or in other words, the primary work being done is independent of the payload.

IEEE 11073 [i.1] point of care device series of standards is likely to provide a good starting point for developing globally applicable data standards for the interface, building on standards currently set out in BS 8521 [i.2] and other widely used proprietary formats.

In many cases, it is expected that the Home Hub will do minimal processing of the data from devices.

Even though the data payload is viewed generically like this it is still useful to characterize the data into 5 fundamental types:

- Episodic - data for single asynchronous incident
- Streaming - continuous stream of real time data
- Document - arbitrary large collection of data
- Control - communication that commands the receiver to alter its behaviour
- Alarms - communication that carries a variable sense of urgency

By this categorization we can fragment the problem, as the mechanisms chosen to move the payload would have to match the underlying needs of each category.

The data types would be mapped to communication means that have the needed corresponding QoS properties expected by each data type (e.g. by usage of appropriate M2M Service Classes).

The following is a list of guarantees that the use case is imposing on possible solutions.

In case of failure (e.g. failure of some external WAN interface, degradation, reduced bandwidth, fire detected):

- High resilience is provided for alarms traffic
- No data loss is incurred (potentially all types, or just alarm and certain medical data?)
- On request (etc. by applications, alarms, human interaction) enable voice services to be maintained to accepted performance standards

Has to be able to work simultaneously with a normal array of "home" IP related services running over the same broadband connection (home automation, entertainment, etc. as well as other remote monitoring services, such as telehealth).

External dependency: Home Hub has to be able to continue to pass alarms signals to a monitoring centre in the event of a power-failure in a premises.

5.4.4 Information Exchanges

1) Home Hub (= M2M Gatewa) to Remote Monitoring Centre

   Fundamentally the flow is to deliver data contained on the Home Hub to an arbitrary Monitoring Centre via a WAN interface. The precise steps to accomplish this would be determined as part of the detailed application development implementing this use case but would be probably be along the lines of:

   - Home Hub has data that it wants to communicate to a remote Monitoring Centre. This data probably comes from attached devices but could be other data as well. It may be a single data point or a collection of many data points.
   - The data is augmented. The specifics of this will again depend on the specific application used to implement an example for this use case but it would probably entail augmenting the data with some additional data such as device ID, timestamp, User ID, or any other needed relevant data for this flow.
   - The data is prepared for transmission. Here the data could be converted (information model and/or format). Then the required security and privacy measures would be enacted (the required security may also be done by the transport utilized).
   - The data is sent.
   - An acknowledgement that the data was received successfully by the remote Monitoring Centre.

2) Remote Monitoring Centre to Home Hub

   Typically this flow is to deliver low volume traffic such as command data from a remote Monitoring Centre to the Home Hub via a WAN interface. The precise steps to accomplish this would be part of the detailed application development implementing this use case but would be probably consist be along the lines of:

   - The remote Monitoring Centre has command data that it wants to communicate to a Home Hub. This command may be for use by the Home Hub or could be ultimately for use by a device attached to the Home Hub.
   - The data is augmented. The specifics of this will again depend on the specific application used to implement an example for this use case but it would probably entail augmenting the data with some additional data such as remote Monitoring Centre ID, timestamp, target Home Hub ID, or any other needed relevant data for this flow.
   - The data is prepared for transmission. Here the data could be converted (information model and/or format). Then the required security and privacy measures would be enacted (the required security may also be done by the transport utilized).
   - The data is sent.

  - An acknowledgement back to the remote Monitoring Centre that the data was received successfully by the Home Hub.

5.4.5 Potential new requirements

The following list summarized candidates for possible new requirements:

- The M2M system would need to be capable of handling M2M traffic of different categories (i.e. of different priorities and with different characteristics).
- The M2M system would need to be capable of supporting applications to establish 2-way voice communication at the request of applications and prioritize traffic accordingly.
- The M2M system would need to be capable of supporting applications to establish other real-time interactive or real-time streaming communication (e.g. video) at the request of applications and prioritize traffic accordingly.
- In case of failure of communication links (partial link loss, drop in quality, need to switch to backup, etc.):
  - High resilience is provided for alarms traffic
  - No data loss is incurred (all types, or just alarm and certain medical data?)
  - Enable voice services to be maintained to accepted performance standards
- Has to be able to work simultaneously with a normal array of "home" IP related services running over the same connection (home automation, entertainment, etc. as well as other remote monitoring services, such as telehealth).
- External dependency: Home Hub has to be able to continue to pass alarms signals to a monitoring centre in the event of a power-failure in a premises.

History

Document history		
V1.1.1	September 2013	Publication