ETSI TS 103 425 V1.1.1 (2016-11)

Publicly Available Specification (PAS)
Smart Machine-to-Machine communications (SmartM2M)
Home Gateway Initiative
RD039-Requirements For Wireless Home Area Networks (WHANs) Supporting Smart Home Services

CAUTION

The present document has been submitted to ETSI as a PAS produced by HGI and approved by the ETSI Technical Committee Smart Machine-to-Machine communications (SmartM2M).

Reference
DTS/SMARTM2M-103425

Keywords
gateway, home gateway, intelligent home & building

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

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 (https://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 Specification (TS) has been produced by ETSI Technical Committee Smart Machine-to-Machine communications (SmartM2M), as result of the PAS process for document HGI-RD039 developed by the Home Gateway Initiative.

The Home Gateway Initiative, a non-profit organization closed on June 2016, produced guidelines, requirements documents, white papers, vision papers, test plans and other documents concerning broadband equipment and services which are deployed in the home.

HGI worked on Specifications for home connectivity and Services enablement, in particular to encompass a delivery framework for Smart Home services. The defined architecture includes support for a standard, general purpose software execution environment in the HG (for third party applications), API definitions, device abstraction, and interfacing with Cloud based platforms.

The HGI's methodology ensured that projects undertaken reflected items of strong interest to the Broadband Service Providers (BSPs), as well as brought in opportunities at every stage for vendor input, suggestions and participation.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

1 Scope and purpose of the present document

The use of Wireless Home Area Networks (WHANs) will expand with the advent of Smart Home services to enable energy management, home automation etc. In many scenarios it is appropriate to use a smart home gateway (HG) to connect the devices and various systems in the house (e.g. lighting, thermostats; heating systems and others).

The present document provides guidance on WHAN technologies to companies or fora that are designing or specifying home automation or service systems.

The wireless In-home communication technology normally supports several functions:

- Bidirectional communication
- Pairing of devices with coordinators
- Application layer interoperability

The present document focuses on the first two functions only.

2 References

2.1 Normative 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 referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://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.

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

[1] IETF RFC 3565: "Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)".

[2] NIST SP800-22: "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications".

2.2 Informative 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 referenced document (including any amendments) applies.

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

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] Void.

[i.2] "Wi-fi simple configuration technical specification" Version 2.0.2.

[i.3] HGI-RD008-R3 (2013): "Requirements for Software Modularity on the Home Gateway".

[i.4] ZigBee™ Pro Test Plan - 07-5035 rev 06.

[i.5] ZigBee™ IP Network Test Specification - 12-0227 rev09.

3 Definitions, symbols and abbreviations

3.1 Definitions

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

Cloud: network of remote servers hosted on the Internet and used to store, manage, and process data in place of local servers or personal computers

Coordinator: device in a WHAN, which (a) converts any commands (or requests for data) from a user or an external agent into data packets, which it routes/transmits to the intended device and which (b) receives data packets from devices and acknowledges, records, or converts the packets into signals for the user or controlling software

NOTE: There is only one coordinator in a WHAN.

Device: piece of hardware that provides connectivity and functionality

Gateway Operator (or just operator): Primary responsibility of the Gateway Operator is to control who is allowed to deploy services to the Service Platform in question i.e. control which Service Deployment Managers are allowed to manage the particular Service Platform. In addition to this, the Gateway Operator can also manage other functions related to a specific Service Platform instance.

Network Provider: Provides and manages wide area network connectivity between the Service Platform and other parties, which include the Gateway Operator and other Service Providers. In the case where the Service Platform is connected via the Internet, the Network Provider also supplies the Internet Service Provider (ISP) functionality.

Remote Controller: device which allows a user to remotely operate another device e.g. switch another device on/off

Response Time: time between the trigger event and the user getting feedback

Service Customer: subscribes to services and pays the charges that are incurred using those services

Service Provider: Is a business entity. The Service Provider supplies the necessary means to provide the business related support of a specific Service Application. The Service Provider is also responsible for delegating the task of service deployment to the Service Deployment Manager.

Smart Home Services: autonomous or software-assisted automation system within the home, for example automation of lighting, security alarm systems, energy management systems, health monitoring and alert systems

Sniffing: successful reading of information by a person (or software) different to the intended recipient(s)

Wireless Home Area Network (WHAN): wireless communication network for interconnecting devices centred around an individual person's workspace or home

3.2 Abbreviations

HG	Home Gateway
HGI	Home Gateway Initiative
WHAN	Wireless Home Area Network(s)

4 Purpose of the present document

4.1 Rationale

Network providers (i.e. telecommunication carriers) have begun developing and deploying Smart Home services. To realize these services, it is useful to work with other industry players such as device manufacturers, service providers and platform operators to develop communities of interest and construct ecosystems for the services. It is necessary to adopt new technologies for low-power wireless communications to enable smart HG functions which often involve battery powered devices. Network providers are not yet in a position to select a single WHAN technology, but whatever is chosen it is expected to provide a good user experience in addition to technical capability and performance.

4.2 Problem statement

Wireless in-home connectivity is an essential element in providing Smart Home services; installing new wiring just for a Smart Home service is usually unacceptable being difficult, costly and aesthetically displeasing. However, although there are many types of wireless technologies available, none can currently satisfy all the user and service provider requirements.

The present document describes the requirements for Smart Home wireless in-home connectivity to indicate the direction in which such technologies need to develop to support both current and future needs.

4.3 Benefits for the industry

The current status of WHAN technologies is hampering the development of the Smart Home market. The lack of a ubiquitous, plug and play wireless technology is a major barrier to mass-market adoption of Smart Home services. None of the operational entities [i.3], from service provider to user, can be sure which technology will become the de facto standard/market leader and so may be reluctant to choose or invest.

4.4 Roles and responsibilities

The **manufacturer** produces equipment for the home, such as sensors, actuators, smart appliances, and other sub-systems (alarm, home automation), and smart HGs. The manufacturer integrates the chipset, software stack, and the application programming interfaces. In some cases, they may also directly produce devices. Some requirements for device certification are usually set by the platform operators and/or service providers.

The **platform operator** manages a Smart Home platform, which includes a smart HG and a WHAN in the home, as well as servers in the Cloud. The platform operator may be a network provider or a gateway operator, e.g. a telecommunication carrier.

The **service provider** builds their services on the Smart Home platform and offers them to resellers or directly to service customers.

Service customers are the people who use the Smart Home services. They obtain the necessary devices from the service provider, platform operator, or even a retail shop. To provide Smart Home services cost effectively, it is necessary to avoid dispatching technicians to each house for initial installation or maintenance. Therefore service customers need to be able to install devices and configure their WHAN themselves, even though they will not be technology experts.

5 Key WHAN attributes

5.1 Installation and configuration of devices

One of the most important elements in driving widespread deployment of user-friendly Smart Home services is that installation and configuration of the WHAN should be very easy. With wireless networks, it is potentially easy to eavesdrop or to spoof, so "man in the middle attacks" shall be prevented especially during the installation procedure. The WHAN shall have easy setup functionality and easy maintenance functions. If only specialists can set up the network, then deployment costs will be prohibitive.

A variety of installation methods is needed to provide an acceptable user experience. Any WHAN system shall support all of the below.

1) **Pre-configured devices:** The devices are configured by the manufacturer or platform operator to automatically connect to the WHAN. Usually such devices can connect only to a pre-configured WHAN coordinator.

2) **Easy local setup:** The devices are configured using an easy-setup mechanism that requires only simple operations, such as pushing buttons on the coordinator and the device near simultaneously (see e.g. [i.2]). Sometimes a customer will also need a step-by-step installation and configuration tool. To make the procedure user-friendly, the same procedure for easy-setup should apply to all devices.

3) **Remote setup:** Installation and configuration of devices is done remotely by a service provider or a platform operator.

A typical customer may not know what devices can be used on their WHAN. Therefore, devices should be sold with appropriate labels, which clearly show compatibility, from a certification organization which provides public access to lists of certified products.

5.2 WHAN performance

5.2.1 Reliable wireless communication

To provide reliable service over the WHAN, service providers need to consider issues affecting wireless performance, such as radio interference and coverage, and also ensure that the WHAN does not send data to the wrong device (e.g. switch on/off the wrong light, or connect to devices in a neighbour's apartment).

For example, the WHAN may be used for turning a room light on and off. In this case, rapid and reliable response is required. So the WHAN needs to support delay sensitive communication. Delay sensitive applications usually require less than a few seconds response time, with some being far more demanding. The WHAN also may be used for sending the accumulated data from a series of measurements, thereby requiring the transfer of significant amounts of data, which could take a considerable time on a slow link. However the impact of this on customer experience may be minimal. The below list indicates the maximum acceptable response time for a variety of actions from the perspective of user experience or the service needs (e.g. for alarms).

a) Light switching and dimming: 300 ms.

b) Switching on/off general: 1 000 ms.

c) Actions where visual feedback is expected by user: 1 000 ms.

d) Sensor values with sudden events (motion sensor, smoke detector): 1 000 ms.

e) Sensor values general: 3 000 ms.

f) For some applications the user might accept longer response time, e. g. heating control. Further, some sensors measure parameters that do not change much in the short-term, like room temperature. Such values might be buffered by the coordinator and not require instant reporting from a sensor. The maximum tolerance for such applications can be significantly higher than 3 000 ms. The present document does not define a maximum response time for such applications.

To transfer data effectively, the WHAN should support reliable communication with the worst-case performance still meeting the customer experience or service needs. Re-transmission is likely to be needed in this low-power, high noise environment. However re-transmissions on a slow or very noisy link may not succeed, or may take too long, and can shorten battery life.

The impact of radio interference, both from and into other systems needs to be considered. The 2,4 GHz band in particular is already used widely in the home by various systems, such as Wi-Fi and Bluetooth. Mobile communication services at various frequencies have also become popular. The WHAN needs to coexist with these systems with the minimum amount of mutual interference. The radio frequency bands used by the WHAN (and even the channels within those bands), should be therefore be selected carefully.

As so many home systems already use the ISM band (2,4 GHz), a less crowded frequency region should be considered for the WHAN, e.g. sub 1 Gigahertz. There are already bands reserved for WHAN use in this frequency region. Use of such frequencies would allow the WHAN to continue to work well even in highly congested Wi-Fi areas.

Coexistence of Wi-Fi and the WHAN shall be possible even when they use frequencies quite close to each other, even when the physical interfaces are in close physical proximity. An interference avoidance function therefore needs be supported by the WHAN to address all these issues. This would make it possible to install multiple networks in one area. In Europe, LTE at 800 MHz may adversely impact the 868 MHz band allocated for WHAN use. If the 868 MHz radio band is used for the WHAN, measures shall be taken to prevent interference from the LTE systems.

Wireless channel selection functions are also required to select the channel subject to the least interference. Interference mitigation techniques are also required to provide a reliable and stable network. These include carrier sensing, dynamic selection of the most suitable channel, and even scheduling functions (e.g. Time Division Multiplexing between Wi-Fi and WHAN).

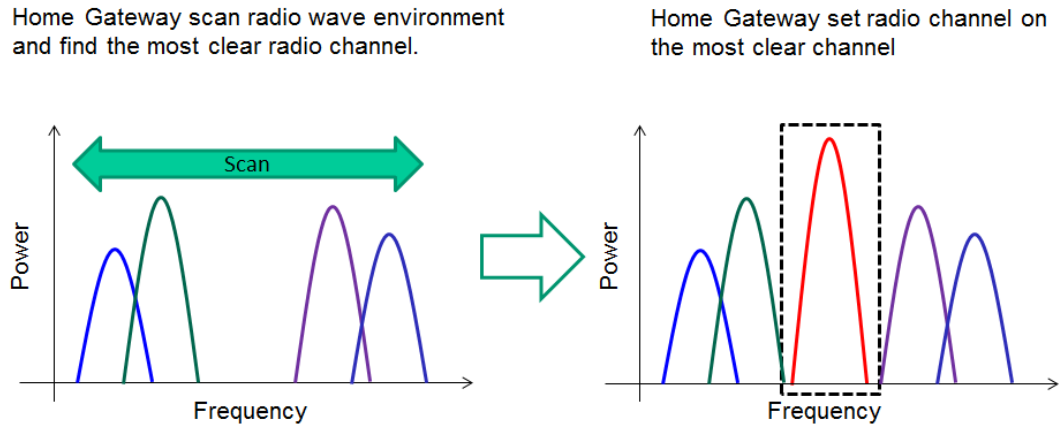

Figure 1: Wireless Channel Selection Function Image

The WHAN should provide reliable operation for many years as WHAN devices may not be replaced very often. Reliable operation shall be maintained even when the user or a neighbour installs additional devices.

The radio frequency and transmit power shall of course comply with the radio regulations in each country.

As for coverage, the WHAN has to cover the whole home. However it may be difficult to achieve this using a direct connection from each device to the coordinator. Therefore some function to extend coverage is required, e.g. repeaters or meshing.

It would be useful for devices to be able to indicate where the radio link performance is acceptable, especially during installation. This will require a low level testing mode.

Smart Home services typically use at least some battery-powered devices, for example remote controllers of home electrical appliances and sensor devices. Typically, home electrical appliances and remote controllers only need to communicate between several and a few dozen times each day. Sensor devices may communicate more frequently, once every several minutes, with metering devices being similar. The WHAN should support this range of occasional operation, thereby enabling long battery-lifetime. The HGI operators expect the following battery life times under normal operation mode:

a) home electrical appliance remote controller: 2 years

b) sensor devices (like temperature sensor): 2 years

c) metering devices (like gas meter): 10 years

However for certain device types it is possible to use self-powered, energy harvesting technology, thereby avoiding the need for batteries, and thus providing an indefinite lifetime. Such technologies are also within the scope of the present document.

5.2.2 Management, configuration and maintenance

To provide services via the WHAN, it may be necessary for all the interested parties (i.e. the service customer, service provider and platform operator - hereinafter "all parties"), to have some management visibility and/or control, however the well-known problem of multiple management entities with regard to conflicting commands shall be avoided.

All WHAN devices on a given network need to be discoverable by all parties. Any network failures need to be recognized quickly, however most customers are not network experts, and so the service provider and/or a platform operator need to be able to diagnose the network remotely. For easy operation and maintenance of the WHAN, logical addresses for routing of commands/data within the WHAN may be useful. The WHAN coordinator should be able to configure a replacement for a defective device with the original logical address.

All parties need to be able to check that a newly installed device has associated with the correct network; there may be more than one WHAN delivering Smart Home services, both within that home and a neighbouring home. Two networks using the same wireless technology and the same network ID would clearly cause a problem.

All parties should be able to confirm that the network is working properly. If a failure occurs, they should be able to identify the type and location of the failure. Testing functions are therefore required and some periodic automated testing function may be useful to pre-empt failures and/or build up a performance history. Such a logging function may be useful to know what happened on the WHAN just before the failure occurred. However the impact of this monitoring on battery lifetime needs to be taken into account.

If a malicious user tries to insert a device into the WHAN, the attempt should be prevented by authentication and authorization functions such as a pairing mechanism.

When a coordinator is exchanged for a new one, efficient ways are needed to avoid manually pairing each device again.

If a device is removed from the WHAN, all parties should be able to determine the impact on network functionality. Prior to such a removal, all parties should be able to check its likely impact on the network, e.g. in a multi-hop network, removal of a wireless-router or relay may affect the connectivity of other devices.

5.3 Network Security

Wireless networks are vulnerable to eavesdropping and spoofing. Therefore the WHAN shall support security functions to protect sensitive data such as billing related information. This means that the WHAN has to authenticate all devices, protect data integrity and privacy (e.g. by encryption) and provide protection against replay attacks; such attacks are a particular concern where the WHAN is used to support a security related application (people and/or property).

Typical WHAN devices have very limited resources to achieve low cost and long battery lifetime, but security still needs to be supported. The security is expected to be provided the WHAN technology and the platform operators; service providers do not expect to have to implement additional security.

WHANs shall have an authentication function to maintain their integrity [i.4] and [i.5]. There are several authentication standards for WHANs. Some use shared keys, others rely on unique MAC addresses or verifiable digital certificates. Whatever methods are used, product types shall have undergone certification by a recognized independent authority and carry the appropriate labelling and technology logo.

When a coordinator is exchanged for a new one, some method is needed to transfer security configuration(s) from the old coordinator to the new one via a secure backup/restore function, without requiring manual pairing/confirmation for every connected device.

6 Functional and technical requirements

6.1 Installation and configuration of devices

Table 1

N°	Requirement
R7.1.1	**Interoperability** WHAN devices carrying the same certification logo or technology logo SHALL be interoperable regardless of the vendor or manufacturer.
R7.1.2	**Certification** The platform operator or service provider SHALL specify, in a format accessible to the service customer the type of WHAN certification required in order for a product to be suitable for connection to a given platform or service.
R7.1.3	**Step by step installation procedure** A step by step installation guide SHALL be available to the service customer.
R7.1.4	**Installation procedure** The installation procedure SHALL be as similar as possible for all device types.
R7.1.5	**Network Configuration** Devices SHALL be able to be installed and configured in the home network without requiring connection to any other network. Devices SHOULD be able to be configured remotely.
R7.1.6	**Easy Pairing by Hardware Button** The WHAN SHALL support push button pairing between any device and the coordinator.
R7.1.7	**Easy Pairing by Soft Button** The coordinator SHOULD also provide a soft button for pairing accessible via a GUI or API.
R7.1.8	**Pairing security** Installation and configuration of devices supporting bi-directional communication SHALL be protected against man-in-the-middle attacks. Installation and configuration of devices supporting only uni-directional communication SHALL be secured against man-in-the-middle attacks if they are used in a security application.

6.2 Reliable performance

Table 2

N°	Requirement
R7.2.1	**Minimization of interference with other radio systems** The WHAN SHALL minimize the impact of interference from other systems. The WHAN SHALL minimize the generation of potential interference to other radio systems.
R7.2.2	**Channel selection** The WHAN technology SHALL be able to be used in environments with multiple radio systems, both in the same band, and adjacent bands. The WHAN SHALL support a function to automatically select the most suitable channel within a given band.
R7.2.3	**Multi-hop networks** The WHAN SHALL support a multi-hop network (e. g .via repeaters or meshing).
R7.2.4	**Transmission Power** Transmission power and technology SHALL achieve a minimum range of 30 m within wood-frame houses, for transmission at 1 kbps.
R7.2.5	**Response Time** The WHAN SHALL support delay sensitive communication. The response time is application dependent but is typically no more than 3 seconds. The response time includes any re-transmission, and application layer delays. The maximum acceptable response times for various actions are: a) Light switching and dimming: 300 ms b) Switching on/off general: 1 000 ms c) Actions where visual feedback is expected by user: 1 000 ms d) Sensors with sudden events (motion sensor, smoke detector): 1 000 ms

N°	Requirement
R7.2.6	**Robustness** The WHAN SHALL support the following functions to improve reliability and stability. error-detection error-correction re-transmission (but with mechanisms to avoid draining battery-powered or energy-harvesting devices) avoiding noisy or congested RF channels (where there is more than 1 channel in a band)
R7.2.7	**Power consumption** Device power consumption SHALL be such that a battery lifetime of at least 2 years is achieved. Metering devices SHOULD have a significantly longer battery lifetime.
R7.2.8	**Power consumption under fault conditions** Fault conditions SHOULD not result in a significant increase in device power consumption
R7.2.9	**Reconstruction of the network** The WHAN SHALL be automatically reconfigured and start to work again when the coordinator and/or devices are rebooted. When a coordinator is exchanged for a new one, it SHOULD be possible to transfer the security configuration via a secure backup/restore function from the old coordinator to the new one without requiring manual re-pairing of every connected device.

6.3 Management and maintenance of devices

Table 3

N°	Requirement
R7.3.1	**Device management** The WHAN SHALL support the reporting of all devices associated with a given network. This information SHALL be available to the management software running on the HG.
R7.3.2	**Hardware ID** Each WHAN device SHALL have a hardware-ID which is globally unique for a given technology. The change of the hardware-ID of a given device SHALL be prevented. The hardware-ID SHOULD be printed on the device.
R7.3.3	**Logical address management** If the WHAN supports logical addressing, it SHALL be able to dynamically assign logical-addresses to each device hardware-ID. The pairings of Logical address and Hardware ID SHALL available to the management software running on the HG.
R7.3.4	**Device management** The WHAN SHALL be able to access a device for management purposes on the basis of its hardware-ID.

6.4 Connectivity Management

Table 4

N°	Requirement
R7.4.1	**Connectivity management** Where a WHAN supports meshing, it SHALL also support direct management of routes between devices (i.e. override automatically selected routing). The coordinator and permanently powered devices SHALL support periodic checking of their connectivity. For devices that do not support periodic connectivity checks due to power restrictions, a lack of connectivity SHALL NOT harm security of people or property. The WHAN SHALL be able to determine the network connectivity map, and provide it to the management software.
R7.4.2	**Wireless signal strength test (Coordinator)** The coordinator SHALL be able to measure its received wireless signal strength from each device. The coordinator SHALL be able to report the information to higher applications or management systems in the HG or elsewhere.

N°	Requirement
R7.4.3	**Wireless signal strength test (End-device)** Each device SHOULD be able to measure its received wireless signal strength and notify the coordinator of the value. (See note 1)
R7.4.4	**Connectivity check test** The WHAN SHALL be able to test the connectivity between each device and the coordinator. The coordinator SHALL be able to send an echo request to a given device. All devices except those that are only powered when actuated or only push data SHALL support echo reply functionality. The echo functionality SHALL be implemented on network or link layer.
R7.4.5	**Route test** The WHAN SHALL support functionality to test the connectivity along the route between any given device and its coordinator. (See note 2)
NOTE 1: This requirement does not apply to devices that are only powered when actuated. NOTE 2: A connectivity test will fail if any of the devices on the route are in sleep mode.	

6.5 Proven security

Table 5

N°	Requirement
R7.5.1	**Freshness** Any WHAN technology devices designed for use in a security related application SHALL provide protection against delay attacks.
R7.5.2	**Integrity** The WHAN SHALL guarantee the integrity of data packets
R7.5.3	**Authentication** The WHAN SHALL NOT allow communication with unauthorized devices, e. g. a device that has not successfully paired with the coordinator.
R7.5.4	**Encryption** The WHAN SHALL support encryption. The encryption level SHOULD be as strong as AES-128. Equipment manufacturers SHALL specify the strength and nature of the encryption method. The method of generating the encryption key(s) SHALL be at least as strong as recommended in IETF RFC 3565 for AES128 [1] (refer http://tools.ietf.org/html/rfc3565). Key delivery SHALL be secured.
R7.5.5	**Random number generation** If security protocols include use of random numbers, then each device SHALL have a True Random Number Generator. A pseudo random number generator SHALL NOT be used. The Random Number Generator SHALL comply with the NIST SP800-22 TEST [2]. Dedicated crypto hardware is not required.
R7.5.6	**Security Certification** The WHAN technology SHALL support device security certification. Each device model SHALL be security-certified by a recognized independent authority.

History

Document history		
V1.1.1	November 2016	Publication