|  |
| --- |
| Functional Requirements and Gap Analysisfor the Smart Grid Use Case |
| Date: 2013-05-15 |
| **Authors:**  |
| Name  | Affiliation  | Phone  | Email  |
| Max Riegel | NSN | +49 173 293 8240 | maximilian.riegel@nsn.com |
|  |  |  |  |
|  |  |  |  |
| **Notice:**This document does not represent the agreed view of the OmniRAN EC SG. It represents only the views of the participants listed in the ‘Authors:’ field above. It is offered as a basis for discussion. It is not binding on the contributor, who reserve the right to add, amend or withdraw material contained herein.  |
| **Copyright policy:**The contributor is familiar with the IEEE-SA Copyright Policy <<http://standards.ieee.org/IPR/copyrightpolicy.html>>.  |
| **Patent policy:** The contributor is familiar with the IEEE-SA Patent Policy and Procedures:<[http://standards.ieee.org/guides/bylaws/sect6-7.html#6](http://standards.ieee.org/guides/bylaws/sect6-7.html)> and <[http://standards.ieee.org/guides/opman/sect6.html#6.3](http://standards.ieee.org/guides/opman/sect6.html)>. |

Abstract

The document details the functional requirements for IEEE 802 technologies derived from the Technical Requirements Document of ZigBee Smart Energy Profile 2.0
[ZigBee docs-09-5449-33-0zse]

Gap Analysis for IEEE 802 technologies deployed for SEP2

Evaluation of ‘Smart Energy Profile version 2.0 Technical Requirements Document’
[ZigBee docs-09-5449-33-0zse]

Introduction

An analysis of the requirements of the ‘Smart Energy Profile version 2.0 Technical Requirements Document’ was performed to determine requirements applicable to IEEE 802 technologies for deployment as link technology for SEP2.

The Smart Energy Profile 2 itself is an IP based application layer protocol, which can work over any link technology. The communication stack of SEP2 is aligned to the Internet model and comprises five layers:



Figure 1: Layered communication model of SEP2

The Technical Requirements Document lists requirements for all the five communication layers. Only requirements related to the two lower layers (Link Layer and Adaptation Layer) are considered in scope to the IEEE 802 technologies.

Detailed Analysis

In the following the requirements applicable to IEEE 802 technologies are listed mentioning the chapter numbers of the Technical Requirements Document.

Evaluation results are drafted and require confirmation by technology experts of the particular IEEE 802 access technologies.

***SEP2 Requirements applicable to IEEE 802***

# 5 Device Requirements

## 5.1 Function Sets

void

## 5.2 Device Types

out-of-scope (generic SEP2 requirement)

## 5.3 System Services

### 5.3.1 Network Access Server

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | Requirement | .3 | .11 | .15 | .16 | .22 | Remarks |
|  | *Req[NAccS-1] Each device capable of allowing access to the network to unassociated devices in the Smart Energy Profile Network SHALL be able to perform the function of Network Access Server.* |  |  |  |  |  | Higher layer function out of scope of IEEE 802 |

### 5.3.2 Network Authentication Server

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | Requirement | .3 | .11 | .15 | .16 | .22 | Remarks |
|  | *Req[NAuthS-1] Each data link of a Smart Energy Profile Network SHALL have at least one active authentication server, and MAY have multiple alternate authentication servers.* | X | X | ? | X | ? | Requires 802.1X or native EAP support |
|  | *Req[NAuthS-2] The Network Authentication Server SHALL control the acceptance of devices onto the network and removal of devices from the network.* |  |  |  |  |  | AAA interface into access required |

### 5.3.3 Application Trust Center

out-of-scope (higher layer issue)

### 5.3.4 Energy Services Interface

void

# 6 Link Layer Technical Requirements

## 6.1 General Technical Requirements

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | Requirement | .3 | .11 | .15 | .16 | .22 | Remarks |
|  | *Req[MACPHY-2] The ESI SHALL support at least one of the following MAC/PHYs including (without limitation):**IEEE 802.15.4, HomePlug, IEEE 802.3 (Ethernet, any version), IEEE 802.11 (Wi-Fi, any version), IEEE 1901, ITU G.9960/9961 (G.hn), ITU G.9954 (HomePNA), G3, Prime, ISO 14908, Bluetooth, MoCA, LTE* | X | X | X |  |  | .16 and .22 missing |

## 6.2 802.15.4 Networks

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | Requirement | .3 | .11 | .15 | .16 | .22 | Remarks |
|  | *Req[802.15.4-1] 802.15.4 networks SHALL use IEEE 802.15.4-2006. [802.15.4].* |  |  | X |  |  |  |
|  | *Req[802.15.4-2]802.15.4 networks SHALL use 2.4 GHz band. This is a core requirement for interoperability.* |  |  | X |  |  |  |
|  | *Req[802.15.4-3] Other, non-interoperable, 802.15.4 MAC/PHY implementations MAY be used with the Smart Energy Profile (e.g., 900MHz band, 802.15.4-2010, etc.); however, they SHALL NOT be labeled, branded, or marketed in any way that will allow retail Consumers to mistakenly purchase them instead of interoperable MAC/PHY products. These networks are treated as an alternate MAC/PHY.* |  |  | X |  |  |  |

## 6.3 HomePlug Networks

out-of-scope (non IEEE 802 technology)

## 6.4 Network Admission & Readmission

out-of-scope (generic SEP2 requirements)

## 6.5 Link Layer Byte Order

out-of-scope (generic SEP2 requirement)

## 6.6 HAN Topologies

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | Requirement | .3 | .11 | .15 | .16 | .22 | Remarks |
|  | *Req[NetworkDeployment-1] Installation With Multiple Physical Interfaces: HAN Device installation procedures SHALL support networks with multiple different physical layers and routers.* |  |  |  |  |  | Further investigation necessary |
|  | *Req[NetworkDeployment-2] Autonomous Network Selection: HAN Devices SHALL provide a facility to discover available networks (e.g., IEEE 802.15.4 or IEEE 1901 according to their physical interface support) and select a network to join autonomously. This SHALL be the default mode of operation.* | ? | X | X | X | X | 802.3 missing network discover function |
|  | *Req[NetworkDeployment-3]Manual Network Selection: HAN Devices MAY provide a facility to discover available networks (according to their physical interface support), and allow the user to manually choose a network to join.* |  |  |  |  |  | Network selection information has to be available to OS |
|  | *Req[NetworkDeployment-4] Autonomous Network Join: Once a Device has selected a network, it SHALL then present its security credentials and await a response as to whether it was admitted.* | X | X | X | X | X |  |
|  | *Req[NetworkDeployment-6] Network Access Failure Recovery: A network join indication SHOULD be provided by the HAN Device to indicate whether the Device has successfully joined the network or not either through the Autonomous Network Selection procedure or the Manual Network Selection procedure. If the HAN Device employed the Autonomous Network Selection procedure, unsuccessful network admission SHALL result in the HAN Device selecting another network from the list obtained in discovery and attempting to join that network.If the HAN Device employed the Manual Network Selection procedure, unsuccessful network admission SHALL be accompanied by a status indication presented at the HAN Device.* |  |  |  |  |  | control interface to OS necessary for manual selection |
|  | *Req[NetworkDeployment-7] Network Access Process: The process of joining and attempting Authorization SHALL continue until the Device has been admitted onto one of the available networks and is Authenticated/Authorized by the Network Access Server and Network Authorization Server (see Section 5.3.2, 5.3.3), or the full list of discovered networks has been exhausted.* |  |  |  |  |  | control interface to OS necessary |
|  | *Req[NetworkDeployment-10] If the Device exhausts the full list of discovered networks without successfully joining and Authorizing on one of the available networks, the Device SHOULD employ a back off or manual input procedure to re-attempt the joining and Authorization procedure at a later time.* |  |  |  |  |  | OS issue |
|  | *Req[NetworkDeployment-8] HAN Integrity: The Network Coordinator (e.g., an ESI) SHALL create an individual HAN and SHALL support HAN Device joining only for Devices associated with the HAN created for that consumer. The determination of whether a Device is associated with a specific network is made using appropriate methods described in technical specifications for network physical and/or data link layers, and might involve out of band (e.g., manual) operations.* |  |  |  |  |  | Requirements for provisioning of credentials; has to be supported by authentication and authorization layers |
|  | *Req[NetworkDeployment-9] Network Boundaries for Submeters: If a submeter is the primary Meter implementing an ESI for a Home Area Network, then the submeter SHALL implement the ESI functions just as if it were a main or master meter, since the submeter marks the delineation between access and premises sides of the network.* |  |  |  |  |  | Out of scope of IEEE 802 |
|  | *Req[NetworkDeployment-11] The Network Coordinator SHALL be able to report out devices currently joined to the network, regardless of their states.* |  |  |  |  |  | Network authentication server must keep state of devices |

### 6.6.1 Network Interconnections and Extensions

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | Requirement | .3 | .11 | .15 | .16 | .22 | Remarks |
|  | *Req[NIE-1] Networks with different MAC/PHYs MAY be interconnected via routing (network layer), not bridging (link layer).* |  |  |  |  |  | Higher layer, ok for all |
|  | *Req[NIE-2] Extension Devices: For some installations, it MAY be necessary to provide an extension Device between the ESI and the premises. Provided that these Devices do nothing other than link the ESI to premises, they MAY operate as bridges or routers.* |  |  |  |  |  | Backhaul issue? |
|  | *Req[NIE-3] Extension Devices: 802.15.4 Extension Devices which allow general network access to the extension media MUST operate as routers. Other MAC/PHYs MAY require this as needed.* |  |  |  |  |  | ok |
|  | *Req[NIE-5] Extension Device Layering: Extension Devices SHOULD not access application layer payloads and SHOULD support routing for packets secured with application layer security (e.g., TLS[RFC 5246]).* |  |  |  |  |  | ok |
|  | *Req[NIE-4] Extension Device Location: When an extension Device is used to provide connectivity to the ESI, the extension SHALL be located on the HAN side of the ESI (not on the access side) and the extension Device SHALL be treated as a repeater HAN Device.* |  |  |  |  |  | ? |

### 6.6.2 Smart Energy Profile Networks with Multiple ESI’s

out-of-scope (generic SEP2 requirements for its application layer)

## 6.7 Architecture or Network Limitations on 802.15.4 Networks

void

# 7 Network Layer Technical Requirements

out-of-scope (requirements for the IP layer)

# 8 Adaptation Layer Technical Requirements

## 8.1 802.15.4 Networks

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | Requirement | .3 | .11 | .15 | .16 | .22 | Remarks |
|  | *Req[Adapt-15-4-1] IEEE 802.15.4 networks SHALL use IETF 6LoWPAN [RFC 4944, et al] to adapt IPv6 to the IEEE 802.15.4 environment.* |  |  |  |  |  | ok |
|  | *Req[Adapt-15-4-2] IEEE 802.15.4 networks SHALL use 6LoWPAN Neighbor Discovery [ID-6ND] to adapt IPv6 Neighbor Discovery to the IEEE 802.15.4 environment.* |  |  |  |  |  | ok |

## 8.2 HomePlug Networks

out-of-scope (non-IEEE 802 technology)

## 8.3 Other Networks

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | Requirement | .3 | .11 | .15 | .16 | .22 | Remarks |
|  | *Adaptation layers for other networks will be identified, and the approach should be consistent with that taken in 6LowPAN [RFC4919], depending on the requirements for the selected MAC/PHY.* |  |  |  |  |  | Further investigation required |

# 9 Transport Layer Technical Requirements

## 9.1 Transport Protocols

out-of-scope (higher layer above IEEE 802 functionality)

# 10 Application Layer Business Objective Technical Requirements

out-of-scope (requirements for the SEP2 application layer protocol)

# 11 Application Layer Supporting Technical Requirements

## 11.1 Base Function Set

out-of-scope (usually operating system functions)

## 11.2 Device Management / Configuration

### 11.2.1 Device Management

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | Requirement | .3 | .11 | .15 | .16 | .22 | Remarks |
|  | *Req[DataLinkMgt-3] The Data Link Layer Management plane on each Device SHALL support getting and setting the management and configuration items. These items are specific to the data link they are associated with.* |  |  |  |  |  | Configuration interfaces towards OS necessary |

Other requirements of this section are out of scope (above IEEE 802 related networking layers)

### 11.2.2 Network Management

#### 11.2.2.1 Data Link Operations

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | Requirement | .3 | .11 | .15 | .16 | .22 | Remarks |
|  | *Req[DataLinkOps-1] All Devices MAY support the following data link operations:*  *Reset Device* |  |  |  |  |  | Ok, OS issue |
|  | *Req[DataLinkOps-2] All IEEE 802.15.4 Devices MAY support data link operations for pre- Commissioning as required by the relevant PHY/MAC specification(s) including, but not limited to:* *Set PAN ID* *Set Global Prefix* |  |  |  |  |  | ok |
|  | *Req[DataLinkOps-4] All 802.11, 802.3, IEEE-1902,and other alternate PHY/MAC Devices if supported MAY support data link operations for pre-Commissioning as required by the relevant PHY/MAC specification(s) including, but not limited to:* *Set Unique Local Address* *Set Global Address* |  |  |  |  |  | Further investigation necessary |

#### 11.2.2.2 Network Layer Operations

out-of-scope (IP layer requirements without impact to lower layers)

## 11.3 Migration of Network Services to Other Devices in the Network

out-of-scope (application layer requirements)

## 11.4 Firmware Download

out-of-scope (higher layer functionality)

## 11.5 Diagnostics & Monitoring

### 11.5.1 Network Monitoring & Connectivity Investigations

#### 11.5.1.1 Data Link Management Plane Responses

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| # | Requirement | .3 | .11 | .15 | .16 | .22 | Remarks |
|  | *Req[ODMNMCI-3] Devices SHALL provide data link status information, some of which MAY be specific to the underlying MAC/PHY, and which MAY include information such as:* *Addressing (e.g., extended IEEE address, short address, MAC address)* *Operational flags (e.g., Association Permit Flag, Receiver on when idle, etc.)*  *Physical network ID (e.g., PAN ID)*  *Physical network parameters (e.g., IEEE 802.15.4 beacon payload)* |  |  |  |  |  | MIB/OS interface necessary |
|  | *Req[ODMNMCI-9] Devices MAY provide link quality metrics for one hop neighbors including:* *Interface identifier, Neighbor address, RSSI (from last received transmission from that neighbor) with timestamp of last received transmission* *Interface identifier, Neighbor address, LQI (averaged over past 5 received transmissions from that neighbor) with timestamp of last received transmission used to form the LQI* |  |  |  |  |  | Further investigation necessary |

Other requirements of this section are out of scope (higher layer functionality)

### 11.5.2 Device Level Logging

out-of-scope (higher layer function)

### 11.5.3 Device Status

out-of-scope (higher layer function)

## 11.6 Handheld Access

out-of-scope (usually implemented as part of the operating system)

# 12 Security Requirements ### for further evaluation ###

## 12.1 Security Tenets

### 12.1.1 Security services provided by cryptography

### 12.1.2 Additional protection mechanisms

## 12.2 Cryptographic Algorithm and Key Size Selection

### 12.2.1 Cryptographic Strength

### 12.2.2 Security lifetime and algorithm selection

### 12.2.3 Selecting Cryptographic Strength

## 12.3 Cryptographic Strength

## 12.4 Key Establishment

## 12.5 Credential Mechanism

## 12.6 Layered Packet Security

### 12.6.1 Use of Symmetric Keys

### 12.6.2 Layer 2 – Link Layer

### 12.6.3 Layer 3 – Network Layer

### 12.6.4 Layer 4 – Transport Layer

### 12.6.5 Security Material

## 12.7 Security Procedure Terminology

### 12.7.1 Entity

### 12.7.2 Environment

### 12.7.3 Procedure

## 12.8 Network Environment Security

### 12.8.1 Network Access

### 12.8.2 Authentication

### 12.8.3 Authorization

## 12.9 Application Environment Security

## 12.10 Identification

## 12.11 Authentication

## 12.12 Authorization

## 12.13 Auditing

## 12.14 Security policies and domains

## 12.15 MRD Security Requirements

### 12.15.1 Types of Communication

### 12.15.2 Cryptographic Protocols

### 12.15.3 Cryptographic Algorithms

## 12.16 Certificates

### 12.16.1 X.509 Certificates

### 12.16.2 Custom Certificates

### 12.16.3 Certificate lifetime

## 12.17 Suggested Cryptographic Algorithms

### 12.17.1 Common cryptographic building blocks

### 12.17.2 Cryptographic cipher suites based on Transport Layer Security (TLS)

## 12.18 Security Policies

### 12.18.1 Static security policies

### 12.18.2 Dynamic security policies

### 12.18.3 Security policy configuration attributes

# 13 Constraints

## 13.1 Platform Constraints

out-of-scope (higher layer functionality)

## 13.2 Device Upgradeability

out-of-scope (higher layer functionality)