Self Qualification Report for NB-IoT Devices

from Supplier

Supplier Contact

Date

History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Modified by | Comment |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Versioning Legend

|  |  |  |
| --- | --- | --- |
| Version | Comment | Status |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Authors

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Company | Phone no. | e-Mail |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Supplier Approval

|  |  |  |
| --- | --- | --- |
| Name | Role | Signature |
|  |  |  |

TABLE OF CONTENTS

[1. Introduction 7](#_Toc483407920)

[2. Technical description of the tested device 7](#_Toc483407921)

[2.1 Sensors and Interfaces: 7](#_Toc483407922)

[2.2 connectivity 8](#_Toc483407923)

[2.3 Supported Protocol Layer/Frameworks 8](#_Toc483407924)

[2.4 PHYSICAL SPECIFICATION 8](#_Toc483407925)

[2.5 Electrical SPECIFICATION 8](#_Toc483407926)

[2.6 Supportet Cloud of Things Use CaseS 9](#_Toc483407927)

[2.7 Certificates 9](#_Toc483407928)

[3. Safety and Security 10](#_Toc483407929)

[3.1 General 10](#_Toc483407930)

[3.2 Hardware 10](#_Toc483407931)

[3.3 Hardware Security Module 10](#_Toc483407932)

[3.4 Hardware Housing 10](#_Toc483407933)

[3.5 Firmware and OS 10](#_Toc483407934)

[3.6 Bootloader 11](#_Toc483407935)

[3.7 Operating System (OS) 11](#_Toc483407936)

[3.8 Applicastion execution environment 12](#_Toc483407937)

[3.9 System update 12](#_Toc483407938)

[3.10 System hardening 12](#_Toc483407939)

[3.11 Data Encryption 13](#_Toc483407940)

[3.12 System Reset 13](#_Toc483407941)

[3.13 Remote device management 13](#_Toc483407942)

[3.14 Authentification 13](#_Toc483407943)

[3.15 Optional Modules and Services 14](#_Toc483407944)

[4. Self qualification Test Documentation 15](#_Toc483407945)

[4.1 Data of the Device used in the SELF qualification Tests 15](#_Toc483407946)

[4.2 Technical Contact 15](#_Toc483407947)

[4.3 Commercial Contact 15](#_Toc483407948)

[5. Self qualification Test Documentation 16](#_Toc483407949)

[5.1 Chapter 1. Device registration 16](#_Toc483407950)

[5.1.1. Request device credentials 16](#_Toc483407951)

[5.1.2. Pre-provisioning of devices 20](#_Toc483407952)

[5.2 Chapter 2. OPERATION ON DEVICE 21](#_Toc483407953)

[5.2.1. Downlink MEssage 21](#_Toc483407954)

[5.3 Chapter 3. Configuration Update OTA, Recording of Signal Strength 23](#_Toc483407955)

[5.4 Chapter 4. Reliability – reconnection/send & receive data after connection loss (client/server) 24](#_Toc483407956)

[5.4.1. Device resends all buffered data after reconnect 24](#_Toc483407957)

[5.5 Chapter 5. Send an Alarm 26](#_Toc483407958)

[5.5.1. Create an alarm from Device 26](#_Toc483407959)

[5.6 Chapter 6. Send an event – mapping correct/usage of sensor/device management library 27](#_Toc483407960)

[5.6.1. Send an event from the device 27](#_Toc483407961)

[5.7 Chapter 7. Send Measurements 29](#_Toc483407962)

[5.7.1. Send SIMPLE Measurement Data 29](#_Toc483407963)

[5.7.2. Send COMPLEX Measurement Data 30](#_Toc483407964)

[5.8 Chapter 8. Session Resumption 31](#_Toc483407965)

[5.8.1. Disconnect and Reconnect Device 31](#_Toc483407966)

[5.9 Chapter 9. Stability test (required for being added to portfolio) 34](#_Toc483407967)

[5.9.1. Long time test 34](#_Toc483407968)

[5.9.2. Device Handling after Power Blackout 36](#_Toc483407969)

[5.10 Chapter 10. Traffic 39](#_Toc483407970)

[5.10.1. Check amount of transmitted data 39](#_Toc483407971)

[5.11 Chapter 11. Final Test Activities 42](#_Toc483407972)

[5.12 Chapter 12. Further Specifications 43](#_Toc483407973)

## Introduction

The document includes all relevant information for Deutsche Telekom AG to review the NB-IoT self qualification of the supplier, check the results and provide the technical feedback. Usually the feedback is provided within 15 working days after successful transfer of the document.

The finished document shall be provided via email to the functional mailbox [m2m-hardware-support@telekom.de](mailto:m2m-hardware-supprt@telekom.de) for further processing.

## Technical description of the tested device

Please provide the status of each criteria of your device. If seen as required you might add additional comments in the text field after the selection box.

## Sensors and Interfaces:

Accelerometer

3D G-Sensor

GNSS (GPS)

Temperature Sensor

Real time Clock

LAN/ Ethernet

USB

RS 232

RS 485

I2C Bus

Digital In       (numbers of)

Digital Out       (numbers of)

CAN

LIN Bus

1-Wire

SPI

Analog to Digital Converter

Digital Analog Converter

Audio In/Out

Other Interfaces/Sensors/ Comments

## connectivity

Cellular Connectivity

NB-IoT

External Antenna connector

Fixed Line Connectivity

Bluetooth

2.1

Bluetooth Low Energy (only)

Bluetooth 4.0

Other

## Supported Protocol Layer/Frameworks

CAN-Bus

Direct current signals according to EC 60381-1

Other:

## PHYSICAL SPECIFICATION

Maximum Device Size      mm      mm      mm

Switchboard Installation

IP –Class required IP

Operating Temperature min      °C max      °C

Storage Temperature min      °C max      °C

Operating Humidity max      %

Storage Humidity max      %

Other (explosive area classification, acceleration, etc.)

## Electrical SPECIFICATION

Fixed Battery

Rechargeable battery

Usage with one battery (capacity)       years

Power Supply Voltage       Volt

Other (e.g. withstand 2KV Voltage Peak, etc.)

## Supportet Cloud of Things Use CaseS

Measurement values

Events will be sent to client

Alarms will be sent to client

Tracking data will be sent to backend

Remote Control

Other

## Certificates

Product can be sold in Europe

Automotive Certification

TÜV-GS

FCC

Lithium Battery CB

Other (e.g. other countries, additional certificates)

## Safety and Security

## General

|  |  |
| --- | --- |
| Provide an overview of all implemented functions: |  |
| Provide an overview of all available network Services: |  |
| Please provide the used security algorithms and other implemented security features: |  |
| Does the system include mechanisms which ensure the integrity and confidentiality of the data? |  |
| Does the device include HW and/or SW components which are not maintained by the manufacturer, developer or supplier? |  |

|  |  |
| --- | --- |
| Are all HW developer Interfaces (e.g. JTAG and BDM) removed or safe deactivated? |  |

## Hardware

## Hardware Security Module

|  |  |
| --- | --- |
| Does the device include a Hardware Security Module or an interface to an external Hardware Security Module? |  |
| Is the access to the Hardware Security Module interface restricted, e.g. limited to trusted processes? |  |

## Hardware Housing

|  |  |
| --- | --- |
| Is the device secured against external access, e.g. housing made from reinforced plastic? |  |
| When data is processed, which needs to be secured against manipulation from unauthorized users, which additional security features have been implemented on the housing side? |  |

## Firmware and OS

|  |  |
| --- | --- |
| Does the device save confidential data encrypted via the Advanced Encryption Standard (AES) in the Software/Firmware? |  |
| Does the system provide mechanisms (e.g. signatures) to protect integrity of the data which requires protection? |  |
| Does the device provide functions (test and diagnosis, APIs, Menu points, comfort functions) which allow it for an unauthorized user or application to extract confidential data from the persistent memory? |  |

## Bootloader

|  |  |
| --- | --- |
| Does the device ensure that the integrity of the firmware image is verified before being executed via a safe bootloader? |  |
| Does the bootloader ensure that extracting confidential data in clear text is not possible? |  |
| Does the bootloader ensure that the flash memory cannot be extracted? |  |
| Is the bootloader optimized in a way to ensure that only the minimum required functions are included? |  |
| Is the bootloader protected against manipulation and in the One Time Programmable (OTP) area of the flash memory? |  |

## Operating System (OS)

|  |  |
| --- | --- |
| Does the device use a Linux OS with a current stable kernel and extended support period? |  |
| Does the TLS implementation of the embedded Linux operating system support the current TLS cipher suites? |  |
| Does the operating system of the device enforce a strong memory protection? It must be prohibited that a process destroys data to structure in the address space of another process or within the kernel address space? |  |
| Does the OS implement Unix-like user rights and file system permissions? Is each service started with the minimum necessary privileges? |  |
| Is it ensured that only protocol and status messages without confidential data can be extracted via a serial console interface? |  |
| Is there shell access or another console interface implemented? |  |
| Does the system provide mechanisms for secure data storage, access control, user authentication and authorization to access protected resources? |  |

|  |  |
| --- | --- |
| Does the device provide a mechanism that supports the integrity and authenticity check of executable program code before it is being executed? |  |
| Does the device provide appropriate standard mechanisms (eg, an API) for secure data transmission? |  |
| Does the device provide mechanisms for secure data storage, access control, user authentication and authorization of access to protected resources? |  |
| Does the device run applications in dedicated execution environments (e.g. sandbox) and provide dedicated interfaces for accessing user data and device functions outside of the application context with the possibility of restricting this access? |  |

## Applicastion execution environment

## System update

|  |  |
| --- | --- |
| Are all known weak points in the software or hardware of the system fixed or contained? |  |
| Does the device (e.g its bootloader) allow the update of the entire device firmware(s)? |  |
| Does the device allow updates / patches from parts of the software? |  |
| Are updates provided promptly and as signed patches? |  |
| Does the device allow a rollback to the last known correct firmware when the import of an update / patch fails? |  |

## System hardening

|  |  |
| --- | --- |
| Are all unnecessary functions and services removed or safely deactivated? |  |
| Is the system robust against unexpected inputs? |  |
| Are there accounts with predefined authentication features on the device? |  |
| Do system messages contain sensitive data such as cryptographic keys or passwords? |  |
| Are only the required network services activated at delivery of the embedded system? |  |
| Do all applications on the device that have a password-based authentication provide measures against systematic guessing of the passwords (e.g. brute force protection)? |  |

## Data Encryption

|  |  |
| --- | --- |
| Is the data encryption key generated based on a key-specific set of device attributes? Are the attributes stored obscured within the firmware image file? Is the attribute a random number? |  |
| Is the data encryption key unique for each firmware version/each device ? |  |

|  |  |
| --- | --- |
| Does the device provide a reset mechanism to factory default, which includes the deletion of all data (confidential data, configuration data)? |  |

## System Reset

## Remote device management

|  |  |
| --- | --- |
| Does a device has access to any other device that is managed by the RDM system? |  |
| Does the system have a secure bootstrap / provisioning process, that provides the authentication features (credentials, certificates) to the device ? |  |
| Is the confidentiality and integrity of the data between the device and the RDM system ensured ? |  |

## Authentification

|  |  |
| --- | --- |
| Does each device have its own individual authentication feature (credentials, certificates)? |  |
| Is the device password preconfigured or does it need to be changed when being used the first time? |  |
| Does the system ensure that the password complexity policy is used in case username and password are used? |  |
| Does the system support mutual, certificate-based authentication between the device and the back-end server (e.g., Device Management Server)? |  |
| Does the system provide an effective protection mechanism against the systematic guessing of the password(s)? |  |

## Optional Modules and Services

|  |  |
| --- | --- |
| Are all protocol stacks on the device implemented robust? |  |

## Self qualification Test Documentation

## Data of the Device used in the SELF qualification Tests

Device Serial Number

Device FW Revision

Device HW Revision

Device IMSI

Modem FW Revision

Other FW Revision

## Technical Contact

Name

Contact Data

## Commercial Contact

Name

Contact Data

## Self qualification Test Documentation

## Chapter 1. Device registration

## Request device credentials

Summary:

Test successful

Verification point 1:

Figure 1 screenshot of Cloud of Things frontend (registration list)

Verification point 2:

Figure 2 MQTT-SN “CONNECT” message from step 3 and corresponding POST response

Verification point 3:

Figure 3 Screenshot from CoT frontend (registration list)

Verification point 4:

Figure 4 POST request from step 6 and corresponding response

Verification point 5:

Figure 5 Screenshot from CoT frontend (registration list)

Verification point 6:

Figure 6 Screenshot from CoT frontend (device credentials)

Verification point 7:

Figure 7 Screenshot from CoT frontend (detail page of the device credentials)

## Pre-provisioning of devices

Summary:

Test successful

Verification point 1:

Figure 8 Screenshot from CoT frontend (device credentials)

Verification point 2:

Figure 9 Screenshot from CoT frontend (detail page of the device credentials)

## Chapter 2. OPERATION ON DEVICE

## Downlink MEssage

Summary:

Test successful

Verification point 1:

Figure 10 Screenshot from CoT frontend (showing the downlink message)

Verification point 2:

Figure 11 Screenshot from CoT frontend (list of operations from table device control)

Verification point 3:

Figure 12 Screenshot from CoT frontend (info dialog of operation)

Verification point 4:

Figure 13 Screenshot from CoT frontend after Status change (info dialog of operation)

List all operations on the device supported by the Cloud of Things implementation:

## Chapter 3. Configuration Update OTA, Recording of Signal Strength

N/A

## Chapter 4. Reliability – reconnection/send & receive data after connection loss (client/server)

## Device resends all buffered data after reconnect

Summary:

Test successful

Verification point 1:

Figure 14 Screenshot from CoT frontend (info dialog of event)

Verification point 2:

Figure 15 Screenshot from CoT frontend (e.g. logfile or status dialog)

Verification point 3:

Figure 16 Screenshot from info dialog after reconnection

Verification point 4:

Figure 17 Screenshot from measurement dialog

## Chapter 5. Send an Alarm

## Create an alarm from Device

Summary:

Test successful

Verification point 1:

Figure 18 MQTT-SN ALARM message and corresponding POST response

Verification point 2:

Figure 19 Screenshot from CoT frontend (Alarm table)

## Chapter 6. Send an event – mapping correct/usage of sensor/device management library

## Send an event from the device

Summary:

Test successful

Verification point 1:

Figure 20 MQTT-SN “EVENT” message request from step 1 and corresponding POST response

Verification point 2:

Figure 21 Screenshot from CoT frontend (event table)

Verification point 3:

Figure 22 Screenshot from CoT frontend (info dialog of event)

## Chapter 7. Send Measurements

## Send SIMPLE Measurement Data

Summary:

Test successful

Verification point 1:

Figure 23 MQTT-SN “MESSAGE” request from step 1 and corresponding POST response

Verification point 2:

Figure 24 Screenshot from CoT frontend (diagram “<Measurementtype>”)

## Send COMPLEX Measurement Data

Summary:

Test successful

Verification point 1:

Figure MQTT-SN MES request from step 1 and corresponding POST response

Verification point 2:

Figure Screenshot from CoT frontend (diagram “<Measurementtype>”)

## Chapter 8. Session Resumption

## Disconnect and Reconnect Device

Summary:

Test successful

Verification point 1:

Figure 27 Provide Name of the device + configured time interval from preconditions and Screenshot from CoT frontend (list of all devices)

Verification point 2:

Figure 28 Screenshot from CoT frontend (list of all devices) during disconnect

Verification point 3:

Figure 29 Screenshot from CoT frontend (list of all alarms) during disconnect

Verification point 4:

Figure 30 Screenshot from CoT frontend (Measurements overview) during disconnect

Verification point 5:

Figure 31 Screenshot from CoT frontend (Measurements overview), describe he behavior of the device after it has been reconnected to the Cloud of Things (e.g. measurement data during disconnect are stored and sent after a connection has been established again, measurement data during disconnect is lost and not sent to the Cloud of Things after reconnect etc.)

## Chapter 9. Stability test (required for being added to portfolio)

## Long time test

Summary:

Test successful

Verification point 1:

Figure 32 Provide Name of the device + configured time interval from preconditions and Screenshot from CoT frontend (list of all devices)

Verification point 2:

Figure 33 Screenshot from CoT frontend (list of all alarms)

Verification point 3:

Figure 34 Screenshot from CoT frontend (Measurements overview)

## Device Handling after Power Blackout

Summary:

Test successful

Verification point 1:

Figure 35 Provide Name of the device + configured time interval for sending messages from preconditions and Screenshot from CoT frontend (list of all devices)

Verification point 2:

Figure 36 Provide Name of the device + configured time interval for sending messages from preconditions and Screenshot from CoT frontend (list of all devices)

Verification point 3:

Figure 37 Screenshot from CoT frontend (list of all alarms)

Verification point 4:

Figure 38 Screenshot from CoT frontend (Measurements overview) during disconnect

Verification point 5:

Figure 39 Screenshot from CoT frontend (Measurements overview) after reconnection, describe the behavior of the device after it has been reconnected to the Cloud of Things (e.g. measurement data during disconnect are stored and sent after a connection has been established again, measurement data during disconnect is lost and not sent to the Cloud of Things after reconnect etc.)

## Chapter 10. Traffic

## Check amount of transmitted data

Summary:

Test successful

Verification point 1:

Figure 40 Amount of data that has been transmitted between NB-IoT Connector and the device during execution of test case “Request device credentials”

Verification point 2:

Figure 41 Amount of data that has been transmitted between NB-IoT Connector and the device during execution of test case “Send a downlink message”

Verification point 3:

Figure 42 Amount of data that has been transmitted between NB-IoT Connector and the device during execution of test case “Create an alarm from the device”

Verification point 4:

Figure 43 Amount of data that has been transmitted between NB-IoT Connector and the device during execution of test case “Send an event from the device”

Verification point 5:

Figure 44 Amount of data that has been transmitted between NB-IoT Connector and the device during execution of test case “Send a simple measurement”

Verification point 10:

Figure 45 Table for all other operations possible via CoT e.g. e.g. send temperature sensor date,( if available),... this data will allow to calculate a suited tarif fort he device

## Chapter 11. Final Test Activities

N/A

## Chapter 12. Further Specifications

Please provide device specification and an overview which operations, events and measurements (type, measurement, units, etc.) are supported by your devices.