APPENDIX 2 – TECHNICAL REQUIREMENTS

1. INTRODUCTION

1.1 This schedule (in this document referred to as this “**Schedule**”) constitutes an integral part of the Managed IoT Connectivity Agreement entered into by Telia and Customer (the “**Agreement**”) and includes technical requirements for use of the Services.

1.2 While a single or small number of misbehaving Devices typically won’t impact other users, a large group of Devices operating in a negative pattern consistently or at the same time may have a very adverse impact on network resources and therefore on other users.

1.3 Standard mobile Devices on the Telia Network, as well as the applications running on these Devices, must operate in a manner consistent with the requirements specified in this document. Customer is solely responsible for complying with Telia’s IoT Technical Requirements. Customer’s failure to comply with the requirements, causing disturbances in the Telia Networks or the networks of Telia’s roaming partners, may *inter alia* lead to the suspension of the Service(s).

2. HARDWARE AND FIRMWARE REQUIREMENTS

2.1 All IoT Devices must have a GCF certified communication module. Non certified communication module will not be allowed in any of Telia’s or its partners mobile networks.

2.2 Firmware requirements to secure that Customer’s Devices do not impact mobile networks in a negative manner:

- The Device must follow the MOCN network specification standards of the GERAN (GSM and GPRS) / WCDM (UMTS) / E-UMTS (LTE) mobile network communication standards. The same shall apply for any NB-IoT or LTE-M Device.
- The Devices embedded software application must adhere to the power-down procedures as specified by the radio module manufacturer. This ensures the Device de-registers from the network when it powers down. This does not apply to devices using Power Saving Mode over NB-IoT or LTE-M.
- All devices must support FOTA (Firmware Over the Air) for updating the communication modules Firmware.
- All device must support SOTA (Software Over the Air) for updating the embedded software application.
- The customer is responsible to contact Telia’s IoT Support before performing any OTA update for more than 10 000 Devices.
- In the instances where a FOTA upgrade is required a per customer approach and analysis will need to be carried out by Telia. This is to ensure a smooth upgrade for the customer and a manageable impact to the Telia network. where the following factors need to be taken into account:
    - A recommended file size not greater than 0.5 MB is to be downloaded.
    - If the file size has to exceed the above size, then compression should be used where possible.
    - The FOTA file server should ideally support a resume function.
    - A randomized approach to download the FOTA upgrade must be employed between Customer’s Devices.
    - The number of downloads in a specific area should be configurable as per Telia’s feedback.

  - The FOTA file server should support file stitching.
  - Telia specific factors such as radio coverage and MTU size support will also need to be considered.

2.3 The following requirements are to secure that Devices do not impact mobile networks in a negative manner:

- For mass deployments of IoT Devices (e.g. >10,000 units within the same mobile network), if the IoT Device supports more than one family of communications access technology (for example 3GPPTM, WLAN) the IoT Device Application SHALL employ a randomized delay before switching to a different family of access technology.
- The Device must support one of the standardized ETSI SIM form factors according to ETSI TS 102 221 (2FF, 3FF or 4FF) or ETSI TS 102 671 (MFF2).
- The Device must support the USIM application toolkit commands.
- The Device must support SIM-OTA. The purpose is to secure that the Device can relay incoming SIM-OTA messages in a correct way to the SIM according to the current standard.
- The Device must support network search and network re-selection procedures.
- No hard-coded MCC/MNCs shall be applied on Customer's Device and Customer shall not lock the Device to a specific operator. The Device operator selection shall be automatic according to the 3GPP standards.
- Customer shall not hard-code any Extended Coverage Levels (ECL) in any NB-IoT or LTE-M Device.
- The Device shall have the Timer_T3245_Behaviour parameter enabled, which controls whether timer T3245 is used by the Device. If T3245 is used, then on expiry it causes the Device to erase the forbidden network list and removes any "invalid SIM" settings. The value of T3245 is defined in 3GPP TS 24.008, and is randomly chosen by the Device from the last 24 hours.
- LPWA devices shall use a PSM parameter with a long periodic timer instead of detaching from the network. PSM TAU shorter than 60 minutes are not supported.
- eUICC profile download functionality prerequisites that a Device must support BIP over HTTPS.
- eUICC profile download functionality prerequisites that a Device must be able support and realize Short Message Service (SMS). SMS is used to trigger the Device to set up a BIP session for a profile download.

3. DEVICE ISSUE MANAGEMENT PRINCIPLES

3.1 The Device must have the ability to receive and enable updates to functions that control the signalling and traffic behaviour.

3.2 The Device must have a method of recovery in case of unexpected behaviour, such as a firmware failure or any similar event. An example of a recovery method is a watch dog timer that will reset the Device when a specific condition is encountered.

3.3 The Device must be able to receive restart commands remotely. Furthermore, the Device must be able to re-boot itself not more than every 24 hours and not less than once a month. These re-boot parameters are not applicable for NB-IoT or LTE-M Devices.

3.4 IoT Device Applications communicating over NB-IoT and LTE-M, should not power down their communication module/chipset. The 3GPPTM power saving features should be used instead, thus avoiding power-draining, system selection scanning procedures.

3.5 If the IoT Service Platform is temporarily offline, the IoT Device Application shall first diagnose if the communication issues to the server are caused by higher layer communications (TCP/IP, UDP, ATM...). Higher layers mechanisms shall then try to re-establish the connection with the server. This is done by assessing (and if necessary, attempting to re-establish) connectivity in a step-wise approach, top-down.

3.6 The IoT Device Application shall not frequently initiate an application-driven reboot of the communication module/chipset. The IoT Devices shall retry connection requests to the IoT Service Platform with an increasing back-off period.

3.7 If the IoT Device detects that the IoT Service Platform is back online, it shall employ a randomized timer to trigger communication requests to the mobile network.

3.8 When GPS coverage is lost, the IoT Device Application shall not reboot the communication module/chipset. The IoT Device Application should perform diagnostics, reboot the affected hardware element and send an alert to the IoT Server Application.

3.9 When LAN or WAN coverage is lost, the IoT Device shall not reboot the communication module/chipset. The IoT Device Application shall retry scanning to acquire mobile network connectivity with an increasing back-off period.

3.10 When in-built sensors or actuators malfunction, the IoT Device Application shall not reboot the communication module/chipset. The IoT Device Application should perform diagnostics, reboot the affected hardware element and send an alert to the IoT Server Application.

3.11 When in-built sensors or actuators are triggered, the IoT Device Application shall not reboot the communication module/chipset. The IoT Device Application should instead send an alert to the IoT Server Application.

3.12 When the IoT Device's memory is full, for example due to the amount of collected data or an unwanted memory leak, the IoT Device Application shall not reboot the communication module/chipset. The IoT Device Application should perform diagnostics, reboot the affected hardware element and send an alert to the IoT Server Application.

3.13 The IoT Device Application shall always handle situations when communication requests fail in a way that does not harm the mobile network. The mobile network may reject communication requests from the IoT Device with a 3GPPTM error cause code (refer to GSMA TS.34). When the IoT Device Application detects that its requests are rejected, it shall retry connection requests to the mobile network with an increasing back-off period. The IoT Device Application shall not start an application-driven reboot of the communication module/chipset, attempting to ignore or override the mobile network's decision.

3.14 The IoT Device Application shall implement a protection mechanism to prevent frequent "ping-pong" between these different technologies. This is done by limiting the frequency of reselection actions, with appropriate hysteresis mechanisms.

3.15 If the IoT Device supports more than one family of access technology (for example 3GPPTM, WLAN) the IoT Device Application shall employ a randomized delay before switching to a different family of access technology.

3.16 The Device must be programmed to handle and react on messages, error codes and rejects from the mobile network (e.g. Roaming Not Allowed codes),.

4. TRAFFIC AND DATA SESSION BEHAVIOUR

4.1 Zero byte session principle

M2M/IoT applications should only establish data sessions for the purpose of sending and receiving data. An application which establishes a data session and then terminates the session without passing data (a "zero byte session") on a regular basis is not in compliance with Telia's IoT Technical Requirements. However, this requirement is not applicable for NB-IoT or LTE-M Devices.

4.2 Asynchronous Traffic Behaviour

4.2.1 All Devices deployed on Telia's networks must be programmed to strive for asynchronous traffic behaviour. When a Device connects to the network to access a service (data and/or SMS and/or voice), the attempt timing must be randomized between Devices of the same application. In other words, if there are 10.000 Devices which need to upload data to the application server at a fixed interval, shall be randomized within fifteen (15) percent of the transmission frequency. For example, if the report frequency is 60min, the device shall use a approx. a 10-minutes randomized window.

4.2.2 If an application fails to establish a packet data connection to the network or to its application server, then it must introduce a random back-off timer before it attempts to connect again. The purpose of this is to prevent a population of Devices all attempting to establish a data connection at exactly the same time. The re-attempt should be randomized across the group of Devices. An example of where this can occur is if Customer's application server fails. If multiple Devices need to communicate with that server and they all make a repeat attempt to access the data service at the same time, they may all be unsuccessful, as the demand for resources may be exceeded, with the result that they then drop into a retry pattern with an effective self-created Denial Of Service.

4.2.3 The IoT Device Application shall avoid synchronized behaviour with other IoT Devices or events, employing a randomized pattern in time and place (e.g. over a time period ranging from a few seconds to several hours, or days) to request a mobile network connection over the Connectivity Layer.

4.2.4 The triggering of data transmissions, the rebooting of the IoT Device hardware or sub-components (such as the communication module/chipset), or execution of device management commands (including, but not limited to (re-) registrations and firmware updates) shall not be synchronized in time and place. In case of Pull operations, it is extra important to randomise that in time and place and NOT to pull lots of devices in the same cell at the same time.

4.3 Frequent data transmission principles

4.3.1 In the case a Device needs to send data very frequently, it should use an "always-on" connectivity mechanism instead of activating and deactivating network connection. A 'network connection' is the establishment of a radio connection between the Communications Module and the network very frequently.

4.3.2 Devices and applications should be engineered not to exhibit spurious (not-authentic) behaviour on the network. As an example, the Device should not try to establish a data session on the network and acquire a new IP address after a data session is already established for the same Device. If the Device can handle two or more APNs, this applies per APN.

4.3.3 However, if a fixed polling interval is used, the Device should use a time value specified by the Mobile Network Operator. If the preferred value of the Mobile Network Operator is unknown, a default value of 29 minutes is recommended as the polling interval when Devices use TCP protocol. If a fixed polling interval is used, the Device should allow remote and/or local configuration of the interval. *Note: The suggested value of 29 minutes for Devices using TCP protocol is recommended because the routers used by many Mobile Network Operators' will clear the Network Address Translation (NAT) entry for the Devices' data session, 30 minutes after the last communication is sent to/from the Device.*

4.3.4 If the Device uses UDP protocol, the Device must use a timer value appropriate for the target network operator environment.

4.3.5 The frequent data transmission requirement shall not be applicable for NB-IoT Devices.

4.3.6 If the IoT Device Application sends data very frequently (i.e. inactivity periods shorter than two hours), it shall use a persistent PDP/PDN connection with the mobile network instead of activating and deactivating said connectivity.

4.3.7 The IoT Device Application distinguishes between high-priority data requiring instantaneous transmission, versus delay-tolerant or lower-priority data which should be aggregated and sent during non-peak hours.

4.3.8 If allowed by the IoT Service, the IoT Device Application should avoid concentrating communication over the mobile network during periods of high utilization (i.e. transmissions during early morning hours are preferred).

4.3.9 The IoT Device Application shall minimize any geographical network loading problems. There shall be no coordination of all IoT Devices in a given region of the IoT Service to undergo like-operations producing network loading, e.g. firmware updates or software configurations.

4.3.10 Communication requests from the IoT Device Application shall not be retried indefinitely – all requests must eventually time-out and be abandoned by the IoT Device Application.

5. CUSTOMER SYSTEM REQUIREMENTS

5.1.1 If any authentication system resides in Customer’s network and it is out of Telia’s control, Customer must ensure that requests are handled and responded to in a timely manner. This shall apply to systems receiving payload from any Device(s) as well.

5.1.2 Customer must ensure that time-outs due to unacknowledged network requests and/or retransmissions are kept below one (1) percent of the total volume of traffic.

5.1.3 The IoT Device Application should support a “reset to factory settings” via remote and local connection.

5.1.4 The IoT Device Application should support time resynchronization via remote and local connection.

5.1.5 Customer is not entitled to override the preferred roaming list (PLMN) on SIM Cards without Telia's prior written consent

5.1.6 Customer is responsible for restarting any of its own equipment that was powered down or off as contemplated by this Agreement, for instance after a change of Service or troubleshooting.

5.1.7 Customer shall secure the following between the remote Customer Product and Customer Central System:

- appropriate testing (including all future releases) of the Device to comply with the requirements stated above, as well as
- correct communication functionality (voice and/or SMS and/or data).

6. APN CONFIGURATION

Customer is responsible for the configuration of the APN in their Device:

- The APN must be set in the Device by Customer
- Customer must be able to re-set the APN in the Device

7. TESTING OF DEVICES AND APPLICATIONS

Customer shall at any time, upon Telia’s request, provide Telia with a Device and application with the relevant configuration for testing purposes. Once the testing is over, Telia can send the Device back to Customer.

8. SECURITY REQUIREMENTS

8.1 It is the responsibility of Customer to ensure that its Devices conform to industrial security requirements and best practices, e.g. GSMA’s IoT Security Guidelines and the IoT Project recommendations from OWASP. Furthermore it is the responsibility of Customer to continuously monitor industrial security requirements and best practices, and to adapt their Devices’ security settings accordingly in a timely manner.

8.2 Devices must be able to receive software and firmware upgrades in a safe manner as described in the GSMA IoT Security Guidelines.

8.3 Devices and their services must incorporate protection against impersonation attacks and replay attacks. Devices must be able to support mechanisms for protection against misuse, cloning, replacement or theft of their security credentials. Further protection against Denial of Service (DoS) attacks shall be part of the solution.

8.4 Any Device that is directly accessible over the Internet shall be designed with that in mind. Typically this includes reduced exposure to only needed network services/ports and making sure that all access is authenticated. Furthermore, the input received shall be validated to prevent buffer overrun attacks and the like.

8.5 Customer must be able to nominate a point of contact in case of a security related question needs to be addressed by Telia.

8.6 Customer's failure to comply with the Security requirements listed above constitutes ground for suspension of Service.

9. REGULATORY AND LEGAL COMPLIANCE

9.1 Customer must ensure that its Devices at all times conform to current regulatory requirements of the countries in which the Device will be operational and to acquire any necessary certifications required by the regulatory bodies in the host countries, such as EMC, RED, SAR, FCC and other certifications.

9.2 Customer must also ensure that its Devices and applications comply with all applicable laws, including data privacy laws, advertising regulations (such as rules about cookies or "no-spam" laws) and the like.

10. TELIA MOBILE NETWORK FREQUENCIES

The frequencies in which Telia will operate in all Nordic and Baltic countries:

Frequency	LTE Band	Sweden	Finland	Norway	Denmark	Estonia	Lithuania	Latvia
700 Mhz		LTE	LTE					
800 Mhz	20	LTE/ NB-IoT/ LTE-M	LTE/ NB-IoT/ LTE-M	LTE/ NB-IoT/ LTE-M	LTE/ NB-IoT/ LTE-M	LTE/ NB-IoT	LTE/ NB-IoT	LTE
900 Mhz	8	GSM	GSM	GSM	GSM	GSM	GSM	GSM
1800 Mhz	3	GSM/ LTE	GSM/ LTE/ NB-IoT/ LTE-M	GSM/ LTE/ NB-IoT	GSM/ LTE	GSM/ LTE	GSM/ LTE	GSM/ LTE
2600 Mhz		LTE	LTE	LTE	LTE	LTE	LTE	LTE