Aeris® Device Certification Process

Version 1.11
April 11, 2014

Document Support

Questions or comments regarding this document should be directed to

Aeris Communications, Inc.
2350 College Mission Blvd, Suite #600
Santa Clara, CA 95054

Tel. 888-GO-AERIS (1-888-462-3747)
www.aeris.com

Table of Contents

1. Introduction

1.1. Company Background

Aeris® Communications, Inc. is the leading wireless communications service provider dedicated exclusively to the Machine-to-Machine ("M2M") and telematics marketplace globally. Aeris has assembled and seamlessly integrated top tier carrier partner networks through AerCore™ to provide customers with simplified, unified, reliable, and customized network services for M2M and telematics applications. Since 1992, Aeris has provided superior reliability, higher quality coverage, lower latency, and unsurpassed customer support and managed services.

To support the deployment of M2M applications ("Application"), Aeris' customers ("Customer") require cellular radio cards for transceiver application data—such as telemetry and Global Positioning System ("GPS") data from an Aeris Device ("Device")—over cellular frequencies**.**

The objective of this document is to specify details of the AERIS device certification processes and minimum requirements for verification and validation scenarios to ensure that M2M device can operate on AERIS network safely and efficiently.

The goal of the Aeris certification process is to validate the following:

- The device supports all functions per product specifications.
- The device does not create performance patterns which may be detrimental to Aeris network operation.
- The device does not perform erratically.
- Device manufacturers have technical support processes, infrastructure, and escalation capabilities in place.

1.2. Acronyms, Abbreviations, Conventions

The key words "MUST", "MUST NOT", "SHALL", "SHALL NOT", SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" in this document are to be interpreted as described in *Aeris Key Words to Indicate Requirement Levels Specification*.

1.3. Technology Names and Key Terms Used in this Document

- **"M2M Device"** refers to the hardware built to support customer application (application motherboard, processor, GPS board—if used—power supply, antennas, etc.), but excluding the module.
- **"M2M Application"** refers to the logic built into the device that controls the overall operation of the device and relevant reporting algorithms as well as controlling the serial interface to other components (e.g., GPS board, Module, etc.).
- **"Radio module"** refers to the RF module or radio that is contained in the device. The module also includes all of the firmware associated with the operation of the module on the network.
- **"3GPP M2M Devices"** refers to 3GPP standard GSM, HSPA, and LTE devices.
- **"CDMA M2M Devices"** refers to IS-95 1xRTT and CDMA-2000 EVDO devices

1.4. Types of Requirements

This section of the document lists the types of Aeris certification requirements and their identification when applicable only to a specific cellular technology:

Recommended

All recommended requirements are product capabilities and features that Aeris **strongly** believes the M2M Device should incorporate to be a successful product. This recommendation is based on Aeris market studies and/or directly stated Customer requirements.

Mandatory

All mandatory requirements are capabilities and features that **MUST** be incorporated in the M2M Device design. These are based on Aeris technology operational requirements and/or required network behavior that is expected by Aeris systems—including the cellular network. All requirements are Mandatory unless stated otherwise.

Important: Aeris will deny Approval of a Module that fails to meet any Mandatory requirement and commercial product releases will not be allowed

1.5. Waivers

Temporary Waivers

Customers may request temporary waivers of some certification requirements, provided they specifically inform Aeris of the modified behavior and plans for completion. The final product *must* be completed to meet all Mandatory requirements, and pass Aeris Approval tests, before commercial release is allowed.

Permanent Waivers

Customers /Manufacturers may request permanent waivers of certain Mandatory requirements that are not applicable to their implementation. Aeris will review, and approve or rejects, such permanent waiver requests on a case-by-case basis.

The final product *must* meet all Mandatory requirements, less any permanent waivers granted by Aeris, before commercial release is allowed.

Disallowed Waivers

Important: Aeris will not (temporarily or otherwise) waive a requirement for any purpose if the resulting “on-air” or network performance could impair the Carrier cellular or signaling network, or otherwise adversely impact the Carrier’s cellular operations.

2. Overview of AERIS certification process

2.1. Certification phases

Certification of the end M2M devices submitted to Aeris by customer for approval to deploy the device on the network consists of 2 main phases:

Phase 1: Certification of M2M Device.

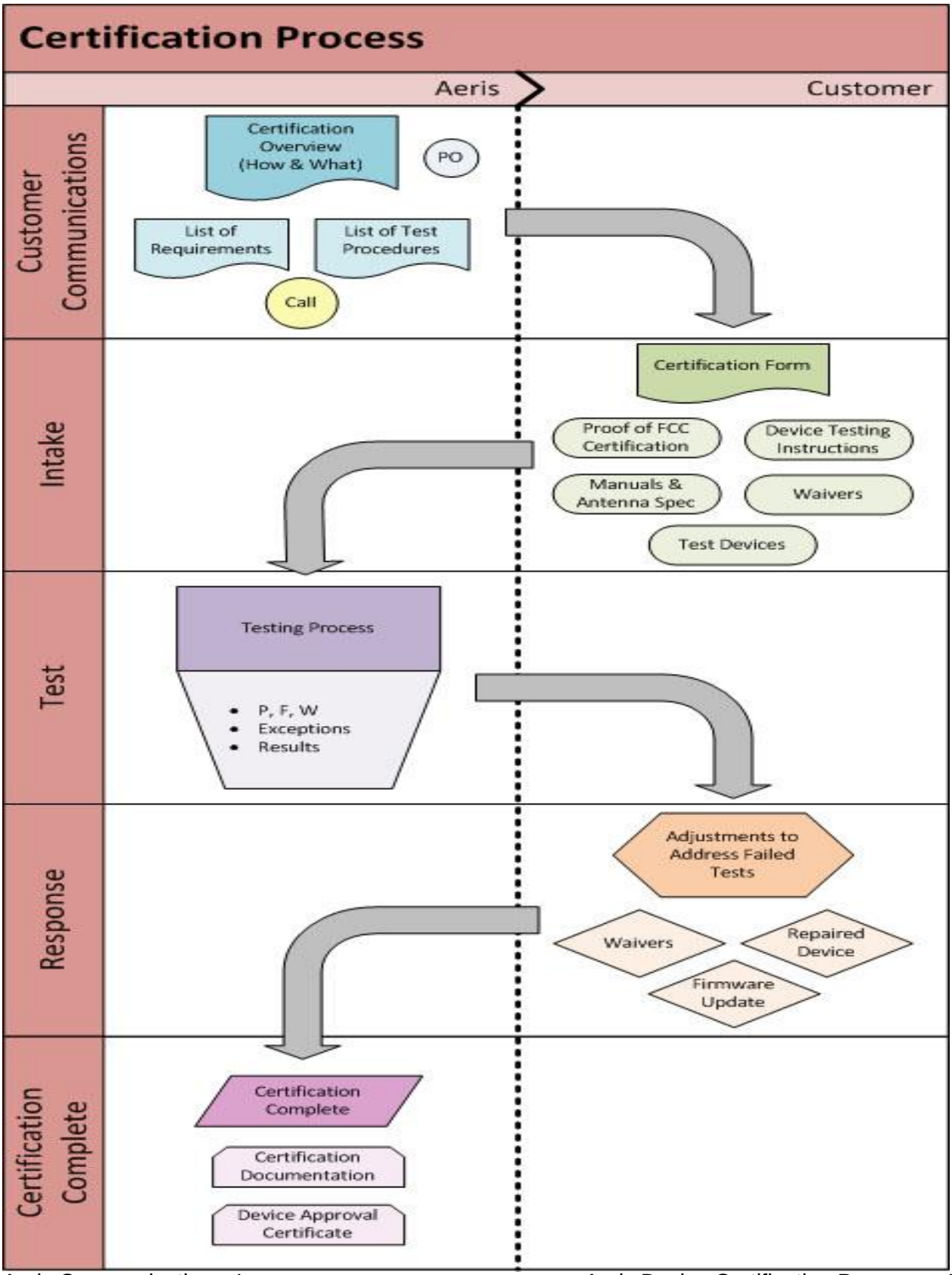
Device certification process checks the performance of the device's radio module in the current physical implementation of the M2M application. In phase 1 the device is tested to verify performance of the following functions:

- MO-SMS/ MT-SMS
- Packet Data
- OTAPA (if applicable)
- MO/MT Voice (if applicable).

Phase 2: Certification of M2M Application.

In phase 2 the M2M application is tested to verify that it does not create operational patterns which might negatively impact the performance of the Aeris network.

The flowchart in Figure 1 below shows the various deliverables during the certification process. The remainder of this document will discuss them in greater detail.


Certification Process
Aeris
Customer
Customer Communications
Certification Overview (How & What)
PO
List of Requirements
List of Test Procedures
Call
Intake
Certification Form
Proof of FCC Certification
Device Testing Instructions
Manuals & Antenna Spec
Waivers
Test Devices
Test
Testing Process
P, F, W
Exceptions
Results
Response
Adjustments to Address Failed Tests
Waivers
Repaired Device
Firmware Update
Certification Complete
Certification Complete
Certification Documentation
Device Approval Certificate

2.2. General requirements for the end M2M devices

M2M Device Regulatory Compliance

It is the Device Manufacturers responsibility to ensure that their device conforms to the regulatory requirements of the country/region in which it will spend the majority of its operational life. It is also the Device Manufacturers responsibility to acquire the necessary certifications required by the regulatory bodies in the host country. Regulatory requirements may include EMC, radio emissions, SAR, and other certifications.

M2M Devices utilizing 3GPP technology must use approved Radio Modules

3GPP M2M Devices may use any Radio Module which has been certified as required by the regulatory authorities in the target deployed country or region.

The table below provides some examples of the regulatory bodies and directives.

Country/Region	Regulatory Body/Directive
USA	FCC
Canada	IC
EU	EMC Directive R&TTE Directive (CE Marking)

Some regulatory bodies will accept regulatory certification from regulatory bodies in other countries (ie the IC in Canada will accept FCC certification) providing it can be shown that the certification meets the minimum requirements of the regulatory body to which it is being applied.

2.3. Specific Requirements for M2M Devices Operating in North America

M2M Devices utilizing IS95/CDMA2000 technologies must use Radio modules with an approved AERIS SKU.

Aeris SKU modules are fully tested and approved for operate on the Aeris Network. They are pre-configured at the factory for Aeris Network Services, and have all the necessary firmware, configuration parameters, PRL and PRI information, etc., in order to *minimize* the effort required by the Customer to develop, manufacture and offer products. A complete list of Aeris SKU module available through Aeris Sales rep.

Any 3GPP radio module or modem which has been approved by Aeris Carrier partners can be deployed on the Aeris 3GPP Network. 3GPP modems are typically ready to use right out of the box. FCC grants may be applied to M2M Devices following specific design guidelines outlined by the module manufacturer.

CDMA and 3GPP M2M Devices must provide proof of FCC Approval

The cellular industry and various governmental regulations require that cellular devices receive appropriate certification and type approval from regulatory bodies. The Module must be put through the process for receiving such type approvals—it is the Manufacturer's responsibility to obtain these certifications and approvals applicable to the country in which the device will primarily operate.

M2M devices submitted for Aeris certification are required to meet the appropriate FCC requirements, which include the following:

- FCC CFR Title 47 Part 15 (Radio Frequency Devices)
- FCC CFR Title 47 Part 22 (Public Mobile Devices)
- FCC CFR Title 47 Part 24 (Personal Communications Systems)

Complete details regarding FCC testing requirements can be found at www.fcc.gov

Wireless communications devices that are using previously approved FCC modules must still obtain FCC certification unless a waiver is obtained from the FCC. M2M Devices may qualify for FCC Grants if an FCC approved Radio Module is used and specific design guidelines provided by the module manufacturer are followed. Typically FCC Parts 22, and 24 qualify for the FCC Grant. Part 15 may qualify for the FCC Grant depending on the final application of the M2M Device.

If the device does not have its own FCC ID number, the supplier must provide a copy of the letter of conformity/waiver from the FCC or an agency on behalf of the FCC.

Certification cannot be completed until the FCC ID or letter of conformity has been provided.

It is not a prerequisite to provide FCC documentation for a device which is using an external modem because the modems should already have the necessary over-the-air certifications.

2.4. Check list of deliverables for Aeris device certification

N	Deliverable
1	Two Test Devices
2	Completed Certification Form
3	Completed Compliance Matrix (checklist form).
4	Certification Papers for the applicable country/region
5	Radiated RF Test Results (if applicable)
6	Device Manuals
7	Waiver Requests

Test Devices

Aeris requires **two (2)** sample devices for certification testing. At customer's request, the test units may be sent back after certification testing has been completed.

Completed Certification Form

Certification form provides information that will be used during testing and in certification documents. This includes general information about your company, contact information, a device summary, required documentation, device details, and device testing instructions:

Device Certification Form

Completed Compliance Matrix (checklist form)

The compliance Matrix check list should be filled by device manufacture and submit before certification.

Cert Submission Check list

Radiated RF Test Results

SAR Testing is required for all devices that have an antenna that operates within 20cm of the human body.

Please note that FCC, PTCRB certification and radiated RF testing reports can be obtained only through accredited testing facilities such as:

CETECOM Inc. Milpitas
411 Dixon Landing Road Milpitas, CA 95035
Phone (408) 586-6200
http://www.cetecomusa.com/company/contact.aspx

PCTEST Engineering Laboratory, Inc.
6660-B Dobbin Road, Columbia, MD 21045 USA
Tel: (410) 290-6652
http://www.pctestlab.com

Device Manuals

Waiver Requests

If customer's M2M application has any limitations or constraints that may prevent you from attaining Aeris approval, customer is requested to submit a waiver request for Aeris review and approval.

3. Certification of the end M2M Device

3.1. Device testing process

Certification testing typically takes about **two (2) weeks**. During this time Aeris cert team will determine whether the submitted device and the M2M application comply with Aeris requirements.

If the device fails any of the tests, Aeris will make recommendations for changes and complete the certification once the issue is corrected. When the device is confirmed to satisfy all requirements, Aeris will issue a formal approval allowing the customer to deploy the device on network.

The table below specifies the certification requirements for the different types of device your application may be using.

Type of Module	Certification Prerequisites			Approval Process		
	FCC Part 15	FCC Part 22, 24	PTCRB	Device Certification	Document Review	Application Certification
CDMA Embedded Modules	X	X		X	X	X
3GPP Embedded Modules	X	X		X	X	X
External Modems						X
X – may qualify for FCC grants if radio module has these certifications. See FCC requirements for more detail (www.fcc.gov)						

Table 1 North America M2M Device Certification Requirements

Type of Module	Certification Prerequisites	Approval Process		
	Local Region Regulatory Certification or Marking	Device Certification	Document Review	Application Certification
3GPP Embedded Modules	X	X	X	X
External Modems				X
X – may qualify for regulatory body grants if radio module has these certifications. See local regulation requirements for more detail.				

Table 2 Rest of World M2M Device Certification Requirements

The process of Document Review will review / verify all required documentation for a commercial launch of the device (User Manuals, Specs, and applicable certification documents).

3.2. Testing an integrated device

The Manufacturer must also provide the ability, including all necessary software and documentation, to test the Integrated Device functionality to the requirements—using external systems that are connected via an externally accessible serial, USB 2.0 or Ethernet port.

In Integrated Devices, the task of Module testing and certification—and to test the requirements of this document—requires access to the Module.

If the Module does not use AT commands, the Manufacturer must provide all necessary software and documentation for external systems to use the actual commands for testing the Module, via an external port in a pass-through mode. Therefore, to test and certify the M2M Device RF performance and the implementation of the requirements of this document, the Manufacturer must provide the ability for an external system to communicate with the Module—in a "pass-through" mode via a serial, USB or Ethernet port—using AT commands.

Requirement	Type
In Integrated Devices, Manufacturers must provide an external port (serial, USB 2.0 or Ethernet) and the ability to test functionality to these requirements.	Mandatory

4. Certification of the M2M Application

4.1. Application testing

The goal of **Application Certification** is to ensure that M2M application to be used with the deployed device does not create behavior patterns which might adversely affect the performance of the Aeris network. These application test cases involve an analysis of how the device connects to the network and how the M2M application communicates with the device.

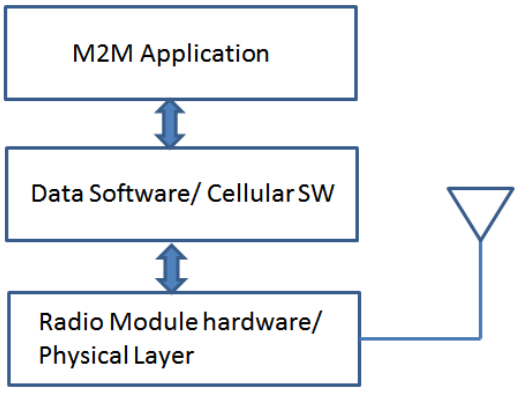
Two Application Certification requirements “Data Retry” and “End of Life” (EOL) are highlighted and explained in more details in the following chapters.

4.2. Data Retry process

The key requirement related to Application Certification which has to be highlighted separately is a **Data Retry** algorithm. This part of the document describes how M2M application is required to behave on the Aeris network when it cannot establish a Packet Data connection or fails to access the Application Server. Aeris does not specify a single universal Data Retry requirement because the data retry algorithm will depend on the specific application. The application may be exempt from such requirements and/or needs to be negotiated between Aeris and the Customer at early stage of product development. For example, the Data Retry algorithm of the devices controlling medical equipment or protecting property may be quite different than the algorithm for devices sending less critical information. However, the general principle which should be followed is that the application retry mechanism should exhibit a random back off.

This section specifies the Data Retry operation for “generic” M2M applications which do not have special retry requirements and exemptions.

Logical Architecture of the Modem



Cellular SW controls the Data connection

Data Software handles Mobile IP data connectivity.

M2M Application operates on top of the Cellular SW/Data Software.

The requirements specified in this section are related to **M2M Application** i.e. the use cases in which the application fully controls all reconnection attempts.

Basic Types of Connection Failures causing Data Retry

A Failed Transmission Attempt (FTA) is a general term used to describe a failed attempt to establish Packet Data connection between the device and the commercial application. The repeated transmission of a previously attempted message or the repeated attempt to establish a connection after an FTA is called a Retry Attempt.

Cause	Description
Application Server is not available (not responding)	Device successfully establishes a packet data connection, obtains IP address but cannot connect to the application server because it's not available (not responding). If the application disconnects the data call and tries to establish it again, this even is considered as one attempt.
User credentials on the Application Server are not valid	Device successfully establishes IP connection to the application server but fails user authentication (if applicable). If the application disconnects the data call and tries to establish it again, this even is considered as one attempt.
Device fails authentication on RADIUS/AuCserver or MIP/PDP context registration on AERIS HA/GGSN.	During data call setup the device goes thorough authentication on AAA Radius server and authentication of Mobile IP registration request (RRQ) on Aeris HA. If any of these authentications fails, the device will fail to establish connection. This event is considered as one attempt.
MIN/IMSI, MEID and/or A/K-Key mismatch	A device fails to establish connection because it is transmitting a MIN/IMSI, MEID or A/K-Key that does not match what is provisioned in the Aeris HLR.

4.3. Data Retry Requirements

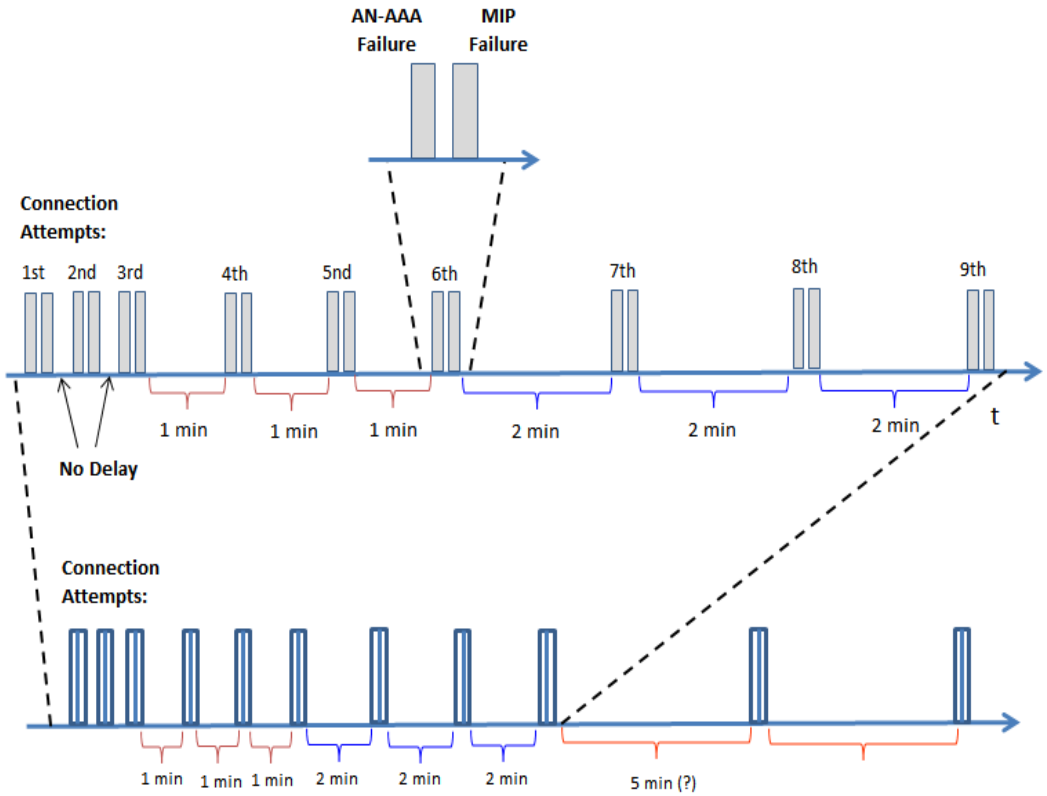
Device **SHALL** follow the algorithm to retry Data connection based on the retry intervals specified in the table below.

(The description below is just an example of possible way to specify this requirement. All variables specified in this table need to be discussed and approved by all stakeholders)

Attempt #	Retry interval (min) after failed attempt
1	0 + X
2	0 + X
3, 4, 5	0 +1
6, 7, 8	0 +2
= > 9	0 + 5 (?)

Where X is a random number of seconds specified for the current application (in the example below the value of X is assumed to be 0).

Example of possible back-off algorithm



In the example of Data Retry algorithm, the mobile device is NOT provisioned on both AN-AAA (for EVDO authentication) and Aeris HA (for MIP authentication). During first attempt to establish packet data connection the device fails EVDO A12 authentication, then falls back to CDMA 1X and fails MIP authentication on Aeris HA (this sequence of events is considered as one connection attempt).

After that the device tries to re-connect again following Data Retry algorithm specified in the table assuming (for this example) that X=0.

Application is not required to keep re-trying indefinitely. After any number to re-establish data connection, the application **MAY** stop the Retry process.

4.4. Reset of Data Retry process

The following events will reset the retry interval and start Data Retry process from the beginning:

1. Successful Packet Data connection.
2. Update of the device parameters using OTAPA, PST or any other methods.
3. Device power-cycle initiated by the user.
4. User-initiated soft reset of the device via AT command.

4.5. Device Recovery:

The Device should have a method of recovery in case of a firmware failure or similar. An example of a recovery method is a Watch Dog timer.

4.6. Graceful shutdown

The device application firmware must adhere to the power-down procedures as specified by the module manufacturer.

4.8 OTAPA Requirement

The device application firmware should allow the device to download the PRL successfully on the device. PRL download usually take 60-90 seconds. In case of PRL download the device should stay on network and don't make any packet data session. PRL download will trigger by Aeris engineer as per demand basis.

In case of battery powered device, device should have way to keep on network for 60-90 seconds as per instruction provided by the server or setting in the firmware.

Aeris uses MT SMS mechanism to download the PRLs.

4.9 Application Modification

If a device fails to comply with any requirements, Aeris will request that customer makes the necessary changes to the hardware or firmware that will bring it up to specification. Aeris will provide recommendations on how to do this and will return the two test devices to you if the problem is related to hardware. Aeris will also work with the customer to determine if a waiver would be appropriate for the M2M application in the case of a particular requirement.

5 Hardware Deliverables

5.8 DUT Quantities

OEM shall provide the following hardware requirements:

Quantity	Functional Area
1	Pass through Mode
1	End finish device

5.9 Device Under Test (DUT) "In Box" items:

To speed up certification efforts, please include the following in each DUT package shipped:

1) Technical point of contact info (business card is sufficient).
2) Printed instructions of how to set up the device, how to turn it on, and how to access the device (typically provided in a Quick Start user guide or similar basic document).
3) Instructions on how to access the pass thru modes or AT command mode.
4) Any other helpful information like GUI passwords, local HTML host IP address or port number, etc.

5.9.1.1.1.1 Accessories

Any additional equipment required to conduct either diagnostics or network testing needs to be included with the device. **One for each device will be required**.

This equipment can include but is not limited to the following:

- Chargers
- Cables
- Monitors
- Adaptors
- Additional Antennas
- Proprietary cables

6 Shipping Guidelines

Each device shipped to Aeris for certification purposes MUST be labeled as required (see below).

6.8 Shipping information (certification samples TO Aeris):

This person will be the primary POC for discussing the scheduling of certification lab entry requirements, product testing and certification status updates and any testing failures that have been observed	Name:	Muhammad Masoom
	Address 1:	2350 Mission College Blvd
	Address 2:	
	City, State, Zip:	Santa Clara, CA 95054
	Email:	Muhammad.masoom@aeris.net
	Phone:	408-457-5115

6.9 Device under Test (DUT) labeling format:

OEM Name:		**DUT Hardware Version:**	
Product Name:		**DUT Software Version:**	
Module Name:		**Antenna Model:**	
Module Firmware Version:			

This labeling is to be affixed to each unit shipped for certification – This label information will be used to identify product for certification and return product once certification is complete. To ensure prompt return of product, please ensure devices submitted for certification are labeled clearly and accurately!