Open Development Device Certification Process

This document provides initial information related to the Verizon Wireless Open Development. All information herein is subject to change without notice. The information provided was considered technically accurate at the time the documents were developed, but Verizon Wireless disclaims and makes no guaranty or warranty, express or implied, as to the accuracy or completeness of any information contained or referenced herein. VERIZON WIRELESS DISCLAIMS ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE.

The developer of any Device, service or product for use on the Verizon Wireless network assumes all risks related to the development of such Device, service or product. Verizon Wireless does not guarantee or warrant the availability of its network or the compatibility of its network with any Device, service or product. Verizon Wireless disclaims liability for any damages or losses of any nature whatsoever whether direct, indirect, special or consequential resulting from the use of or reliance on any information contained or referenced herein.

Contents

Revision History

Rev.	Revision History	Date
1.0	Initial ODIS Testing Document	March 2008
2.0	Modifications to add process details, LBS/aGPS and ENAP	June 2009
3.0	Modifications after technical review	
4.0	Modifications after legal review	June 2009
5.0	Adding requirements lock down process	June 2009
6.0	Adding language to address export control concerns Section 3.8	August 2009
7.0	Modifications to Device Introduction Process Flow Section	August 2009
8.0	Add MMS, Global and Telematics Device support	September 2009
9.0	RA process modifications and Vendor meeting agenda details	November 2009
10.0	Process updates	January 2010
11.0	Add unit requirements, 3rd party contact name change, edits from review	February 2010
12.0	Add ODPT mailbox to Pre-submission process flow and to Device introduction process flow; Modifications to Unit requirements	March 2010
13.0	Replace Developer Agreement with Certification Agreement. Updated contact list.	April 2010
13.1	Added VzW owns the test reports (Section 3.2.4)	May 2010
13.2	Modifications to Device Introduction Process Flow Section (Section 3.4)	May 2010
13.3	Removed Authors names	May 2010
13.4	Added forecast worksheet to DLD	May 2010
13.5	Legal review additions	May 2010
13.7	Update DLD Agenda	May 2010
13.9	Updated per legal feedback	June 2010
14.0	General updates	June 2010
15.0	Removed section 3.10. Added VPS – Vertical Solutions Provider. Added ppt 1 pager to pre-submission forms. Added sample Device to DLD agenda and reqs. Changed photo in 3.3. Changed available activations w/ approved module to 20.	
16.0	Updated SGS Contact Info to Johee from Dawn. Section 3.2.1 – Added Master Showcase to required docs and DLD agenda, added some clarity on how to register a new Device	

	Section 3.5 – Mentioned new instructions on OD Portal uploads exist on the site.	
17.0	Section 3.3.3 - updated the flow and requirements for the MMSC Server Test. Replaced CPE with NDET	
18.0	Section 3.5 – updated the Device Introduction process	
19.0	Section 3.5 – Updated the Device CSV process	
20.0	Section 3.5 – Updated the wait window with cut off time Section 3.6 – Added sample Device requirements	
21.0	Section 3.7 – Updated the Certification Expiration	
22.0	Section 3.3.1 – Concession Accounts All sections – Changed LBS to LBS/aGPS	
23.0	Section 3.5 Updated IMEI/ICCID pair instructions	January 2013
24.0	Section 3.2 – Updated DLD agenda Section 3.3 – Updated testing process Section 3.4 – Updated time window for ESN upload Section 3.8 (former Section 3.9) – Added new ITL	December 2013
25.0	Section 3.1 – Updated export control link Section 3.2 – Added LTE M2M SIM to DLD agenda Section 3.4 – Removed recommendation for EDI Section 3.8 – Updated test lab information	July 2014
26.0	Section 3.1 – Added Software Update support for 4G devices	November 2014
27.0	Section 3.1 – OTA ID info Section 3.3.2 – Clarification on test results Section 3.2 – Simplified DLD call agenda Section 3.8 – SGS address change and added Wireless Research Center	August 2015
28	Removed reference section, updated lab contact	October 2016
29	Updated acronyms Added overall flow Added new Required Agreement section Added additional testing sub-sections Updated links Updated Lab contacts Clarified other sections throughout the doc	May 2017
30	Removed ECCN link Updated Required Agreements section Clarified FOTA updates Updated EDI upload section, added EID Updated Lab contacts	March 2018

31	• Section 7. Updated Technical contact for Tech Mahindra • Section 7. Updated Test lab name from P3 to Umlaut • Section 7. Updated Contact for Nokia	Feb 2020
32	• Section 3.4.1 Updated conditions for Early Network Access Program devices and Safe for Network devices • Section 7. Updated 7Layers into Bureau Veritas • Section 7. Added Aircom Labs • Section 7. Merged Nokia IOT lab and Motive lab • Section 7. Updated information for Approved Verizon 3rd party labs	July 2020
33	• Section 7. Added Carve Systems, Spirent, Altredis Partners, and Palindrome as approved 3rd party test labs. • Section 3.4.1 Updated conditions for ENAP devices • Section 4.2.2 Added Dual Device ID Upload instructions. • Updated Section 3.1 to include a statement on Verizon FOTA support and IoT device security compliance and testing.	October 2020
34	• Section 3.4.1 Updated conditions for ENAP devices using approved embedded modem • Added section 3.4.3 Auto-Certification Platform Testing Process Flow • Updated Section 3.4.4 for Verizon Services (Verizon Diagnostics, Verizon Baseband FOTA, Verizon Application FOTA) • Updated Bureau Veritas lab information	January 2021
35	• Guidelines for Penetration testing for Parent/Child devices • User Account and login policies management description per Security Audit item 4C • IoT Security Process changes for Chipsets and Modules (Compliance presented and reviewed prior to DLD with approved waivers in place for non-compliance) • Added Private 4G and Private 5G sections	July 2021

	• References provided for Verizon Response Verified (VRV) and Inbound Permanent Roaming processes	
36	• eUICC (reference eUICC process documentation • IoT Security change to “Penetration Testing” for appropriate 3rd party labs • 3rd party lab - Aircom, PC Test and Element Materials Technology	June 2022
37	• Update process for up to 1200 test devices if device is using an approved module and device OEM has PTCRB/GCG/CTIA test reports from approved 3rd party labs for Verizon LTE bands.	Sept 2022
38	• Update Element Material Technology lab information • Update image in section 4.2.1 for IMEI/EID pair for csv to display number (not scientific format) • Update RC Logixx (also known as Arclight Wireless) • Remove Atredis Partners as a test lab • DFIT/GFIT changes requested by NDET	June 2023
39	• Remove references to CDMA • Add TECC length of validity (90 days from ATS) • ITL Lab Updates • DFIT process updates • GFIT process updates • PTCRB updates • Updated 4G and 5G "PWN On-Site" sections • Added section for new "PWN On-Site only" certification process	2024
40	• Updated Pre-FIT information with latest guidelines • Added Fast Track Certification information • Updated ACP self-cert information • Section added for Global IoT Orchestration • Updates to M2M and Consumer eUICC cert process	June 2025

- 3rd party lab info updated; labs DFIT compliance info corrected
- New section started for NTN
- Updated device ‘Inactivity’ conditions
-

41 Dec 2025

- Updated the Fast track process and Section 3.4.2 with DFIT and RF OTA test requirement updates
-

1 Objective

The purpose of this document is to define and describe the Open Development Device Certification process, Device testing and conformance requirements* that Devices must meet before they are certified for use on the Verizon Wireless Network. “Device(s)” means the product, equipment, parts, and components tested for OD Compliance.

This document describes the methods and procedures used to certify voice Devices, voice/data Devices, and data only Devices. This includes, but is not limited to, PDAs/Handhelds, data cards, M2M/IoT Devices, embedded PCs, and more.

*Available from web ODP under ‘Requirement & Test Plan Documentation’ tab (login required).

2 Glossary and Definition of Terms

aGPS	Assisted GPS
AM	Account Manager
B2B	Business to Business
BIS	Bureau of Industry and Security
CCATS	Commodity Classification Automated Tracking System
CA	Certification agreement
CE	*Conformité Européenne*, "European conformity"
COI	Certificate of Insurance
CSV	Comma-Separated Values
DFIT	Domestic Field Interoperability Testing
DLD	Device Lock Down
DMD	Device Management Database
DTO	Device Test Owner
EDI	Electronic Data Interchange
EID	eUICC ID (Embedded Universal Integrated Circuit Card) ID
ENAP	Early Network Access Program
ESN	Electronic Serial Number
ECCN	Export Control Classification Number
ICCID	Integrated Circuit Card Identifier
IMEI	International Mobile Equipment Identifier
FIT	Field Interoperability Testing
FOTA	Firmware Over the Air
GCF	Global Certification Forum
IOT	Interoperability Testing
IoT	Internet of Things
ITL	Independent Test Laboratory
LBS	Location Based Services
M2M	Machine to Machine
MEID	Mobile Equipment Identifier
MDN	Mobile Directory Number
MMS	Multi Media Messaging services
MMSC	Multimedia Messaging Service Center

NDET Lab	Network Device Evaluation Test Laboratory
NDRA	National Direct Revenue Assurance
NRB	Network Repair Bureau
NSA	Non-standalone
NSRA	National Sure Pay Revenue Assurance
NTN	Non-Terrestrial Networks
NWRA	National Wholesale Revenue Assurance
OEM	Original Equipment Manufacturer
OD	Open Development
ODP	Open Development Portal
ODPT	Open Development Product Team (Including Business Development, Certification Owners and Account management.)
ODS	Open Development Specification
OTA	Over The Air
PDI	Product Development and Integration
PM	Product Manager
RA	Revenue Assurance
RF	Radio Frequency
RN	Release Notes
SA	Standalone
SFN	Safe For Network
SUPL	Secure User Plane Location
TECC	Test Entrance Criteria Checklist (Test Campaign)
VSP	Vertical Solutions Provider
WS	Wholesale
VZW	Verizon Wireless

3 Device Compliance Process

3.1 Entrance Criteria and Certification Process

All Devices must be type approved and certified by the United States Federal Communications Commission (FCC) and classified by the Department of Commerce's Bureau of Industry and Security (BIS) before Open Development (OD) Conformance testing can commence.

OEMs or OD Device Developers (collectively, “DEVELOPER,”) requesting Verizon Wireless’ (VZW) certification for LTE capable Devices must receive GCF certification before OD Conformance testing can commence.

All LTE capable Devices must support radio layer Firmware Over the Air (FOTA) updates. All devices using an approved module that supports Verizon FOTA capabilities must be tested to ensure that the Verizon FOTA capability of the module is still functional.

All chipsets and modules brought for approval or devices that are brought to Verizon for certification must provide appropriate security compliance documentation and/or security compliance test results prior to DLD. Any non-compliant security features need to be disclosed to Verizon, and if Verizon agrees to the non-compliant features, a waiver must be submitted and approved prior to the chipset or module DLD.

In order for DEVELOPER to access the OD web portal or OD documents, DEVELOPER must execute a Non-Disclosure Agreement (NDA).
Each DEVELOPER will receive a unique VZW-ID after completing NDA. The VZW-ID will be used in conjunction with the submitted Device to form the Device tracking ID. VZW and OD authorized Independent Test Laboratory (ITL) will identify individual Devices prior to Certification using only this Device tracking ID.

Developer user accounts are created under the company registration to allow access to the Verizon Open Development web portal. Users will be notified after 90 days of user account inactivity that they have 30 days to log in to the OD development web portal to keep their user accounts active. If the user has not logged into their account for 120 days, the account will be made inactive and the user will need to contact the Open Development team to reactivate their user account. If a user account is inactive for 180 days, the account will be deleted, per Verizon Corporate Security requirements, and the user will need to have another user on the company account submit a new user account request.

3.1.1 Device Entrance Criteria

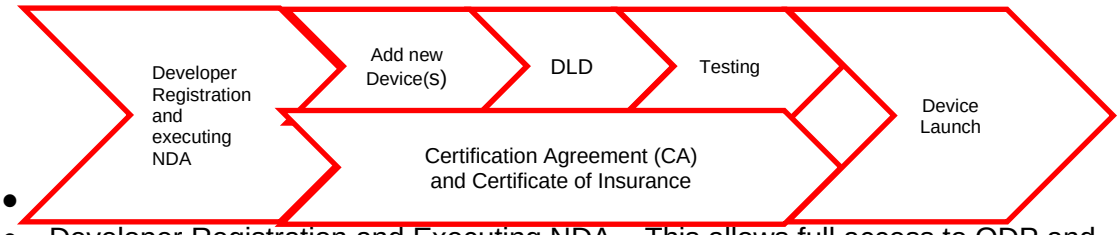
The OD Device Tracking ID

- VZW-ID will be assigned for each DEVELOPER submitting a Device for Conformance
    - Example VZW01000001
- FCC-ID Required Prior to Open Development Conformance

  - FCC Grantee ID (First 3 Characters)
  - FCC Product Code (Remaining up to 14 Characters)
  - https://www.fcc.gov/oet/ea/granteecode#block-menu-block-4
  - Example “A1C0123456789012”
- BIS ECCN and CCATS Required Prior to Open Development Conformance
  - Example " 5A992, G0823456"

3.1.2 Overall Certification Process Flow:

Obtaining Device certification and launching a Certified Device on the VZW network involves fulfilling technical and the contractual requirements of the CA. The CA is a contract issued by Verizon and jointly signed by the DEVELOPER; review can occur in parallel to device registration and testing.



- Developer Registration and Executing NDA – This allows full access to ODP and detailed documents, such as requirements, test plans, etc.
- Add new Device(s) – This involves a five-step process on the ODP
  - New Device Info
  - Marketing Info
  - Forecast
  - Release Notes
  - Attaching all Pre-submission Documents
- DLD - Review and lockdown documents
- Testing - Send device(s) to authorized lab for testing
- FOTA – DEVELOPER to provide FOTA update documentation on a test device.
- Completing Contractual Agreements – Fulfilling CA and COI documents are required prior to device certification.
- Device ID Upload and Launch – Loading Device IDs into Verizon Device Management Database (DMD) system.

3.2 Certification Process

- After the DEVELOPER executes the NDA, accounts will be created to access the ODP at https://opendevelopment.verizonwireless.com/
- DEVELOPER downloads and reviews the OD certification documentation.
- DEVELOPER adds information regarding the new Device and submits all required information on the ODP and notifies their supporting VZW representative. The registered device name/model number should reflect the marketing name/model number as it appears in any FCC filing or approval.

- A DLD review will be held between DEVELOPER and VZW team. The review will cover the following:
    - Submission Overview
    - Device Certification Agreements
    - Documentation Review
    - Review Test Campaign
    - Review Testing & Schedule
    - Review of Developer's Sample Devices - Besides ITL, DEVELOPER is required to send 2 samples to VZW ODPT.
    - Complete required compliance testing in Verizon authorized ITL
- Pending the successful completion of the DLD requirements, VZW will upload the Test Campaign (TECC) to the ODP and notify the DEVELOPER and selected ITL with Approve to Start test (ATS). Testing by the ITL should begin within 90 days of the final TECC release. If testing has not started at the ITL within 90 days, the certification manager will determine whether a new TECC will be needed.
- A host device is certified using an approved module or chipset. A module or chipset is approved through the ODP. For module and chipset approval, refer to Module Guidelines from Requirement & Test Plan Documentation section of the ODP.

3.3 Required Agreements/Documents

All Open Development Agreements must be executed prior to Device Approval.

- **NDA** – Execution required prior to full access to ODP.
- **CA** – Must be executed before device can be fully certified. This will allow use of Verizon mark with a written request per Verizon Branded Guidelines.
- **COI** – Issued by the DEVELOPER and must be provided to Verizon as proof of valid insurance.
  (NOTE: As of January 2018, Verizon Wireless and companies with a current Certification Agreement executed prior to then shall no longer execute an addendum for each newly certified device. Certification of devices will be memorialized in the OD Notice of Certification that contains any device specific requirements and will include the Certification Period for the device).

3.4 OD Compliance Testing

The following figure shows a high-level view of the OD - required testing process known as OD Compliance Testing:

Any Device (including a test Device) must have a FCC ID before activation on the Verizon Network.

3.4.1 Early Testing Process Flow

DEVELOPER may request early testing if development is required prior to certification. The ODPT will review the request and approve it if there is a need for live network testing during development.

Early Network Access Program (ENAP)

- **If the DEVELOPER is using a VZW certified module, up to 20 activations can be allowed for developmental purposes.** Without a VZW certified module, up to 2 activations can be allowed for developmental purposes. Upon uploading of test Device IMEIs to the ODP, VZW will load the test Device(s) MEID/ESN/IMEI in DMD. The DEVELOPER should then work with their VZW sales representative to subscribe and activate lines to connect the test Device(s) with VZW network. The test MDNs must be disconnected no later than 60 days after testing is completed. In order to obtain approval for more than 20 test device IMEI activations, the OEM must have agreed to the terms of the Certification Agreement, and provided the Certification Manager for the device with a detailed business justification detailing: the need for additional test devices; a list of persons/entities who will be using the additional devices; where the additional devices will be used; for what length of time the additional devices be needed; and the current target date for completing device certification. The Verizon Open Development certification team will consider the requests for the additional test devices over the 20-device limit and will approve or deny the request, based on the business justification, at its discretion. If the business case is approved, the device OEM will be allowed to update the additional test device IMEIs for approval by their assigned device certification manager.
- **If the DEVELOPER is using a VZW approved embedded modem**, **up to 20 activations can be allowed for developmental purposes.** Upon the uploading of test Device IMEIs to the ODP, VZW will load the test Device(s) MEID/ESN/IMEI in DMD. The DEVELOPER should then work with their VZW sales representative to subscribe and activate lines to connect the test Device(s) with VZW network. The test MDNs must be disconnected no later than 60 days after testing is completed. In order to obtain approval for more than 20 test device IMEI activations, the OEM must have agreed to the terms of the Certification Agreement, and provided the Certification Manager for the device with a detailed business justification detailing: the need for additional test devices; a list of persons/entities who will be using the additional devices; where the additional devices will be used; for what length of time the additional devices be needed; and the current target date for completing device certification. The Verizon Open Development certification team will consider the

requests for the additional test devices over the 20-device limit and will approve or deny the request, based on the business justification, at its discretion. If the business case is approved, the device OEM will be allowed to update the additional test device IMEIs for approval by their assigned device certification manager.

- DEVELOPER shall not activate or use test devices on the Verizon Wireless network other than for internal testing purposes prior to device certification while such devices are in ENAP testing. ENAP test devices are to be used by the DEVELOPER for development and testing of devices in preparation for certification test activities only. Such test devices should not be activated and used on the Verizon Wireless network in connection with end customer activities.

Safe For Network (SFN) Testing

- **If the DEVELOPER completes SFN testing successfully, up to 500 activations per project can be allowed for further development purposes.** DEVELOPERS must submit the Device information for the ODPT's review and the SFN testing must be conducted at a VZW Authorized ITL.

  DEVELOPERS submit Device information on the ODP and send a test Device request with supportive reasons and test ESNs/MEIDs/IMEIs.

  - RN, TECC, and Device Solution One Pager are required for SFN.
  - ODPT and NDET team review and approve the request.

Upon successful completion of SFN, DEVELOPER can request up to 500 activations of test Devices. All the SFN activated devices must be kept under the device OEM's own mobile account or ECPD (Enterprise Customer Profile Database) ID account and remain in the possession and control of the device OEM. The device OEM must also update the device SW to the final certification version once full certification is complete.

- If the DEVELOPER plans to sell the test devices as commercial products after approval, the DEVELOPER must manage these test devices as commercial products and upload them again (e.g., Note: **Test Devices to be sold as production Devices shall be re-uploaded by DEVELOPER as certified Devices via ODP or EDI).**

Extended test devices for pilots and trials if using a Verizon approved module and the device OEM has successfully completed PTCRB, CTIA or GCF testing on the Verizon bands in a Verizon approved 3rd party lab.

- If the DEVELOPER completes PTCRB, CTIA, or GCF testing successfully on the Verizon frequency bands at a VZW Authorized ITL, up to 1200 activations per project can be allowed for further development purposes. DEVELOPERS must submit the Device information for the ODPT's review and the PTCRB, CTIA, or GCF testing must be conducted at a VZW Authorized ITL and the reports uploaded under the device submission.

  DEVELOPERS submit the Device information on the ODP and send a test Device request with supportive reasons and test ESNs/MEIDs/IMEIs.

  - RN, TECC, and Device Solution One Pager are required for SFN.
  - ODPT and NDET team review and approve the request.

Upon successful completion of PTCRB, CTIA, or GCF testing at a VZW Authorized ITL, DEVELOPER can request up to 1200 activations of test Devices. All the SFN activated devices must be kept under the device OEM's own mobile account or ECPD (Enterprise Customer Profile Database) ID account and remain in the possession and control of the device OEM. The device OEM must also update the device SW to the final certification version once full certification is complete.

- If the DEVELOPER plans to sell the test devices as commercial products after approval, the DEVELOPER must manage these test devices as commercial products and upload them again (e.g., Note: **Test Devices to be sold as production Devices shall be re-uploaded by DEVELOPER as certified Devices via ODP or EDI).**

3.4.2 OD Certification Process Flow

- DEVELOPER should work with ODPT to obtain a TECC.
- DEVELOPER works directly with IOT labs on schedule, payment and complete IOT testing prior to or in parallel with lab conformance testing.
- DEVELOPER chooses and contacts a Verizon authorized ITL from the VZW approved list (see Section 7).
- DEVELOPER submits required Devices and product documentation to the ITL.
- It is responsibility of the DEVELOPER to provide FOTA update documentation (either their own/proprietary solution, from Module vendor, or from Verizon/Motive solution). This can be submitted while the device is in testing, but required with final results.
- The ITL executes VZW approved test campaign based on the TECC.
- The ITL provides test results to ODPT.
- If a module or host device is required to perform Official DFIT testing, then pre-DFIT testing is required and the pre-DFIT test results must be submitted by the OEM. The OEM may choose to conduct the pre-DFIT testing using the a) The OEM's direct employees or b) Any third-party lab or c) Any other individual or organization. Pre-DFIT test results must be submitted in the appropriate pre-DFIT reporting format.
- For the host devices using Verizon approved modules, the Official DFIT is only required for 5GSA VoNR and 5G Redcap
- For 5G SA data only host devices with Verizon approved modules, the 5G SA Pre-DFIT is required and is to be performed at Verizon approved 3rd party lab only. The Official 5G DFIT is no longer required.
- Please note that if a device utilizes an external antenna with a cable lead length over 20cm and no TIS/TRP results are provided, additional RF Supplementary Verizon certification testing will be required for the device.
- CTIA OTA TP Version 10 Release to include Verizon bands as part of PTCRB
- ODPT reviews the test results, along with FOTA solution documentation and either passes, conditionally passes or fails the device.
- After the Device successfully passes testing, ODPT will certify the Device and issue an official notification.

3.4.3 OD Certification through Fast Track Process

If the OEM completes PTCRB or GCF testing successfully on the Verizon 4G/5G frequency bands then Verizon will certify the Host Device through Fast Track process if the following criteria are met:

- The Network Technology supported is 4G LTE and 5G NSA.
- The device utilizes a Verizon-approved module (this applies to Host Device only).
- The device is data-only and does not support voice functionality.
- A final PTCRB or GCF test report and certificate are required, which must include testing results and TIS/TRP RF OTA measurements for all required Verizon bands and EN-DC combinations. Please ensure that these TIS and TRP measurements meet Verizon's RF OTA requirements.
- Please note that if a device utilizes an external antenna with a cable lead length over 20cm and no TIS/TRP results are provided, additional RF Supplementary Verizon certification testing will be required for the device.
- The OEM needs to provide self-test reports for the FOTA Compliance Report and an IoT Security Compliance Report.
- If the device supports eUICC then the eUICC Test Results are also required.
- Any additional feature will require the additional testing prescribed by Verizon.
- Devices classified as ‘Performance Critical’ or ‘Verizon Response Verified (VRV)’ are not eligible for the Fast Track certification.

3.4.4 OD Domestic Field Testing (DFIT)

Refer to section 7.5 Field Testing section of the HOST DEVICE_Certification_Test_Plan_for_all_Technologies_using_Approved_Module.docx process document and the Domestic_FIT_Test_Plan.docx.

3.4.5 OD Global Field Testing (GFIT)

Refer to Global FIT Test Plan.docx

3.4.6 Self-Certification through Auto-Certification Platform (ACP)

The Auto-Certification Platform (ACP) is a simple, cost-effective platform that enables OEM self-testing for supported GCF and Verizon test plans for devices, chipsets and modules. One of the best aspects of the ACP is that it's completely free for OEMs to use and is also portable.

Before the ACP can be shipped to an OEM the following conditions must be met:

- Confirm device readiness by completing Device lockdown (DLD) with Certification manager
- Certificate of Insurance (COI) completed
- Review the ACP Prerequisites document (including Host PC requirements) shared by Certification manager during DLD and confirming that OEM is able to meet them

- Submit account registration at https://acp.verizon.com/acp/login

The ACP can only be shipped to business addresses in the United States, and only to persons directly employed by the OEM. The ACP cannot be sent internationally by the receiving company to locations outside the United States without prior approval of Verizon. Export Regulations mandate that it can only be shipped by OEM to approved countries. Please check with your certification manager on international shipping destinations.

For any issues with ACP setup and testing, there is a ticketing system setup to contact ACP support and details are provided in the Prerequisites document.

3.4.7 Additional Testing for Verizon Services (If features are supported by the device)

OD Standard Lab testing completion is a prerequisite to additional testing. Details for additional testing are available in the Requirement and Test Plan Documentation section of the ODP.

3.4.7.1 LBS/aGPS/SUPL Application Testing Process Flow

After OD Standard Lab Test completion, DEVELOPER may start the LBS/aGPS/SUPL process. Refer to "LBS/aGPS Certification Submission Package" for more information.

3.4.7.2 MMS Device Testing Process Flow

The MMS process must be completed before Device certification for Devices that are MMS capable and require the use of the Verizon MMSC server Refer to the 'VZW OD MMSC Server Test Process' for more information.

3.4.7.3 Private Network Testing

Applicable to Devices using the Verizon Private Network. Refer to Private Network section on ODP.

3.4.7.4 On Site (Private) 4G and 5G Network

Verizon's On-Site LTE is a transformative new wireless networking solution that essentially places a fully contained, private wireless network on the premises of customer facilities/campuses.

On Site 5G adds 5G Ultra-Wideband (UW) small cells and related capabilities to an On-Site LTE deployment. So, enterprises can specify a custom-designed, private network that has the range and scale to match today's needs and adapt quickly to emerging capabilities. On Site LTE/5G is referenced in the industry as a private LTE network, bringing small cell wireless technology to large campuses.

Applicable LTE and 5G devices supporting On Site (Private) network should follow "LTE Data Device requirements" and complete the "On-Site (Private) Network test plan".

This test plan should be performed at Verizon Boston Lab facility by the Verizon testing team. OEMs should select the "Private Wireless Network (On Site)" feature in the Verizon Features and Services section of the device profile and the testing will be assigned in the TECC. OEMs can then work with their Cert Manager to schedule testing and ship devices. If the module has completed this testing, then the device will be credited for it.

3.4.7.5 On Site (Private Wireless Network) Only

For modules and devices that are planned for private network use only and will not be used on the Verizon Macro (public) network, a new distribution channel category, “Private Wireless Network (On-Site),” has been added to the certification process.

This enhancement will streamline the certification process for devices intended for use in private 4G/5G networks. OEMs certifying their module or device 'only' for On-Site private network should select this option and then discuss further with their cert manager

3.4.7.6 Device Management Services

Refer to Verizon OMADM 1.2 Reference Client Package or Verizon light weight M2M (LWM2M) OTADM Reference Client Package on ODP.

3.4.7.7 Verizon Diagnostics

All modules and chip-on-board devices OEMs have to run LWM2M Diagnostics testing. Refer to Reqs-LWM2M document and the ACP support team to utilize ACP box for Verizon LWM2M Diagnostics testing.

3.4.7.8 Verizon Base-band FOTA

Verizon Firmware Over the Air (FOTA) is a Mobile Software Management (MSM) technology in which the module’s (or chipset’s) base-band firmware can be wirelessly upgraded by Verizon. Verizon base-band FOTA uses OMADM or OMA LWM2M industry standards. More information can be found in the “OD FOTA Compliance Instructions and Testing Guidelines" document under ‘Device Management Services’ on the OD Partner Portal.

3.4.7.9 Verizon Application FOTA

Verizon Firmware Over the Air (FOTA) is a Mobile Software Management (MSM) technology in which the application (AP) firmware of a host device can be wirelessly upgraded by Verizon. Verizon Firmware Over the Air (FOTA) uses OMADM or OMA LWM2M industry standards.

3.4.7.10 Verizon Response Verified

Verizon Response Verified offers a standard process for OEMs to verify that their devices are ready for public safety applications. It provides a centrally managed web platform for OEMs to register, test and validate results. Plus, it gives public safety customers a unified place to view all verified devices.

In order to qualify for the Verizon Response Verified program for public safety customers, OEM devices need to achieve these benchmarks:

- National capability
- Available 24/7 customer care
- Dedicated separate web page associated with the device provided by OEMs for public safety customers
- Compliance with latest published open development security requirements
- Testing to validate compliance with Verizon device requirements
- Diagnostics available and included
- Over-the-air upgrades available and included
- Supporting sales and operations resources available
- Installation and maintenance contract either available or included
- Support of Verizon IoT Security Credentialing or equivalent

End customers will be responsible for:

- Keeping devices up to date with over-the-air updates
- Activating and operating the device on Verizon's Public Safety Core for network security
- Using Verizon SIM-Secure (recommended)
- Using Verizon IoT Security Credentialing (recommended)
- Complying with the terms and conditions of the public safety plan under their approved Verizon government contract

More information can be found in the "Verizon Response Verified Certification Process" and "Verizon Response Verified Certification Test Plan" documents under 'Device Management Services' on the OD Partner Portal.

3.4.7.11 Inbound Permanent Roaming

Verizon deems devices to be non-incidentally roaming in its network if any of the following criteria is met:

- Home operator (also referred to herein as "Connectivity Service Provider" or "CSP" deems device to be roaming non-incidentally on the Verizon network
- Device is not in a mobile application and fixed (e.g., alarm panels), or has a limited range (e.g., farming equipment),

- Device is used on the Verizon network for 3 or more consecutive monthly billing cycles and such usage exceeds 60% of the global traffic usage for such Device; or
- Device is activated by CSP with a non-US based profile but device is otherwise registered or licensed in the United States (e.g., an automobile or recreational vehicle with a US-based license plate).

If these criteria are met, then there is a specific certification process to be followed for the device certification. A detailed primer document on the Inbound Permanent Roaming certification process can be found under the Requirements and Test Plan documentation section of the Open Development portal.

3.4.7.12 Global IoT Orchestration (GIO)

Global IoT Orchestration uses a set of ThingSpace APIs to manage both US and global Embedded Subscriber Information Module (eSIM) profiles (provided by Verizon) of IoT devices for multi-national enterprises. You can remotely swap a Verizon US (lead carrier) eSIM profile and a global (local carrier) eSIM profile of the IoT device over the air based on GSMA SGP.02 Remote Provisioning Architecture for Embedded Universal Integrated Circuit Card (eUICC) for M2M.

To qualify for the GIO program the following prerequisites must be met:

- Device is certified for M2M eUICC (SGP.02)
- The Device is Global capable and GFIT certified
    - The device is considered global eligible for GIO if at least one of the following are true:
        - The device is using a Verizon Approved module which completed GFIT testing and certification
        - The device completed the GFIT testing and certification
        - The device has completed the GFIT “LITE” certification testing (see below)

If the device is not planning to roam globally using the Verizon SIM profile, but would like to qualify for the GIO program, then there is the option to complete a GFIT “LITE” certification.

- The device will be required to complete the applicable test case in Section 9 of the Global FIT (GFIT) test plan (Roaming with Bootstrap Subscription), and with each applicable IMSI
    - 9.1 M2M eUICC Bootstrap Connectivity for IMS Capable Devices While Roaming
    - 9.2 M2M eUICC Bootstrap Connectivity for IMS less Devices While Roaming
- This testing would need to be performed in at least one of the applicable global markets that the device will be performing the outbound localization.

3.4.7.13 NTN (Non-Terrestrial Network) Certification

For NTN certification process and test scope, please work with your OD certification manager.

3.4.7.14 Guidelines for Penetration Testing for Parent/Child Devices

Some devices may require evaluation by a Verizon approved 3rd party security evaluation company for penetration testing. Penetration testing is performed by evaluating the device's hardware and software structure, and designing a test methodology to identify and exploit the device hardware and software vulnerabilities to malicious acts. If a family of devices are approved to have a single Parent device and one or more Child devices by the OD certification manager and penetration testing is required, the device OEM will need to provide a separate penetration report for each Parent and Child device.

The penetration report for the Parent device should include the following:

- Device Information (Model #, HW version, OS version, SW version)
- Scope of the penetration test for the Parent device.
- Findings and results of the penetration testing for the Parent device.
    - Note: If there are any findings of device vulnerabilities found during penetration testing and they have not been corrected, a waiver request with a plan/schedule to fix them will need to be submitted for the Parent device.

The penetration report for the Child device should include the following:

- Device Information (Model #, HW version, OS version, SW version)
- A comparison matrix between the Parent and Child devices.
- Scope of the penetration test for the Child device based on an evaluation of the differences between the Parent and Child devices.
    - If it is determined that there is no additional testing needed because the threat scope of the Child device is the same or a subset of the threat scope of the Parent device, the report should document this fact.
- Findings and results of the penetration testing for the Child device if additional penetration testing was needed beyond what was performed for the Parent device.
    - If there are any findings of device vulnerabilities found during penetration testing on the Child device and they have not been corrected, a waiver request with a plan/schedule to fix them will need to be submitted for the Child device.
- Scope of the penetration test for the Parent device. The scope can be copied from the penetration test report of the Parent device, which includes the Device Information of the Parent device.
- Findings and results of the penetration testing for the Parent device. These can be copied from the penetration report of the Parent device.
    - If there are any findings of device vulnerabilities found during penetration testing on the Parent device and they have not been corrected on the Child device, the waiver identifier from the Parent device should be included.

3.4.7.15 Guidelines for Device eUICC Certification

Some device OEMs may choose to utilize an eUICC, which will allow the device to either download a Verizon SIM profile remotely through Remote SIM Provisioning (RSP) or switch between a preloaded Verizon or other MNO profile. The device may support either the Consumer eUICC architecture (using SM-DP+) or the M2M eUICC architecture (using SMSR and SM-DP).

If the device will be utilizing the **M2M eUICC architecture (SPG.02)**, then the below prerequisites must be met ahead of submitting for OD certification:

- Device OEMs shall comply to Verizon Wireless LTE_3GPP_B13_NetworkAccess requirement section 1.3.1.3.15 eUICC (M2M eUICC sections only)
- Device should have the capability to change APNs using AT commands
- Device should be able to handle image configurations when ICCID switches from one MNO to other MNO
- Device should have SIM slot (SIM adapter) and logging capability
- The eUICC should have already completed Verizon Technical Acceptance and approval.
- If the device is using a 3rd party M2M (partner) eUICC, then the eUICC must complete Verizon eUICC Validation, and ensure the following are in place:
    - API available for RSP functionality
    - SMPP Binds – Partner SMSR to both Verizon SMSC and Partner SMSC
    - ES3 Integration – Partner SMSR to Verizon SMDP

A detailed process guide for Device M2M eUICC certification can be found under the Requirements and Test Plan documentation section of the Open Development portal.

If the device will be utilizing the **Consumer eUICC architecture (SPG.22)**, then the below prerequisites must be met ahead of submitting for OD certification:

- Device OEM shall comply with the Consumer eUICC requirements in LTE_3GPP_B13_NetworkAccess requirement section 1.3.1.3.15 eUICC (Consumer eUICC sections only).
- Device OEM is required to provide information regarding the eUICC and LPA (Local Profile Assistant) being used within the RSP Functionality Matrix form which is available on the OD portal.
    - NOTE: If it is determined that the eUICC being used in the device was not previously Technically Approved or Validated to be compatible with a Verizon eUICC profile, then the eUICC will first need to go through the eUICC Validation process with the Verizon SIM profile before any device testing can take place.

The Consumer eUICC Device testing will be determined per the below:

- If the device is using an SGP.22 eUICC (previously validated or Technically Approved), which has the Verizon profile already

preloaded, then no additional device testing is required for device certification

- If the device will be utilizing the RSP functionality to download the Verizon profile, then E2E Device Consumer eUICC testing is required for device certification.
    - Smartphone, Laptop/Tablet, and Rugged Handhelds with user interfaces will undergo the E2E Device Consumer eUICC testing in the Verizon NDET lab.
    - M2M/IoT Devices without a user interface may complete the E2E Consumer eUICC testing remotely following the Consumer eUICC for M2M/IoT Devices test plan.

A detailed process guide for Device Consumer eUICC certification (GSMA_RSP_Consumer_High_level_Onboarding_Process) can be found in the eUICC requirements document within the Open Development requirements package under the Requirements and Test Plan documentation section of the Open Development portal.

Once the device has completed testing and full certification for M2M or Consumer eUICC, the Device OEM may use any eUICC in their commercial deployment without additional VZ testing on the device under the following conditions:

1. The eUICC needs to be already validated or Technically Approved by Verizon
2. The Device OEM or CSP should perform some sanity testing before large scale deployment with the new eUICC
3. Any liability (of M2M or Consumer eUICC features not working) is the responsibility of the device OEM and they will be the first point of contact for the customer in the event there is an issue with M2M or Consumer eUICC functionality on their device.

3.4.8 Inactivity

If the device or module submission status in the OD portal remains inactive for more than 6 months, the status will be changed to INACTIVE. Upon reactivation the Device will be subject to re-evaluation or re-submission for certification and may require complying to most recent VZW Requirements.

4 Post Certification Device ID Upload Procedure

After the Device is approved and before the Device goes to market, the Device must be entered into the VZW DMD to allow future activation of a certified Device. This Process is known as the Device identification upload (ESN/MEID for 3G Devices or IMEI for 4G Devices).

The DEVELOPER can upload the production Device identifications using one of the following approaches:

1. EDI
2. ODP

If one of the above two upload methods is not followed, the VZW' system will prevent activation of the Devices.

4.1 EDI

Electronic Data Interchange (EDI)

- Refer to the "Electronic Data Interchange (EDI) Document" section on the ODP for more information

4.2 OD ODP

4.2.1 Single Device ID Upload

- DEVELOPER captures all of the Device identifications (ESNs/MEIDs/IMEIs) in a CSV file or text file as followed:
    - The ESNs/MEIDs/IMEIs will start on the first line of the first column. For Devices with IMEI & ICCID pairings the IMEIs will be placed in column A and ICCIDs will be placed in column B
    - The name of the file should not contain any special characters (e.g., spaces, dashes, quotation marks, etc.) and must contain the make, model, and total number count of ESNs/MEIDs/IMEIs or IMEI/ICCIDs loaded).
    - Examples of the CSV or .txt file:

  Note: If uploading as *.csv file, ensure that the cells containing the IMEIs are formatted as a number, otherwise if stored in general cell format, it will be in scientific format and digits will be lost.

File Name: CompanyXYZ_ProductABC_5.csv

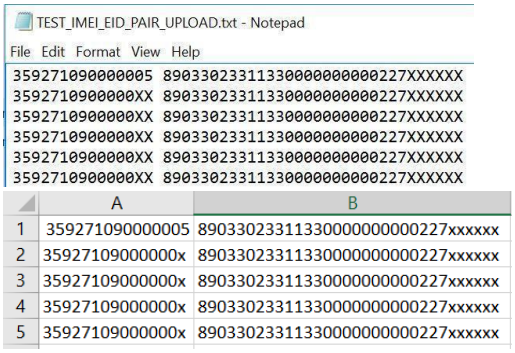
ESN/MEID/IMEI:

	A
1	A00000028BC821
2	A00000028BC822
3	A00000028BC823
4	A00000028BC824
5	A00000028BC825

- IMEI/ICCID pair:

	A	B
1	A1234567890123	1234567890123450
2	B1234567890123	1234567890123451
3	C12345678901234	1234567890123452

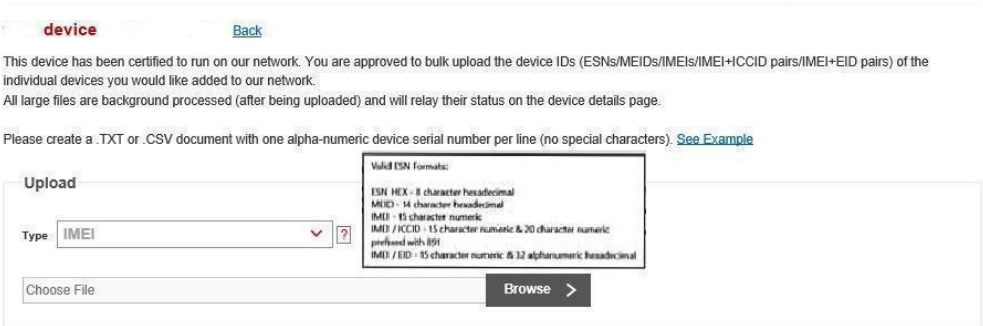
- IMEI/EID pair (txt or csv):



	A	B
1	359271090000005	89033023311330000000000227xxxxxx
2	35927109000000x	89033023311330000000000227xxxxxx
3	35927109000000x	89033023311330000000000227xxxxxx
4	35927109000000x	89033023311330000000000227xxxxxx
5	35927109000000x	89033023311330000000000227xxxxxx

- DEVELOPER logs into ODP, clicks on the “Upload ESN/MEID” link/tab next to the approved Device.
- On the upload screen, select the format of the serial numbers that will be uploaded. The format must be one of the following:

  - IMEI (15) numeric or alpha
  - MEID (14) alpha numeric only
  - ESN HEX (8) alpha numeric only
  - IMEI/ICCID Pair- IMEI (15) numeric or alpha & ICCID (20) alpha only
  - IMEI/EID Pair – IMEI (15) numeric or alpha & 32 alphanumeric hexadecimal

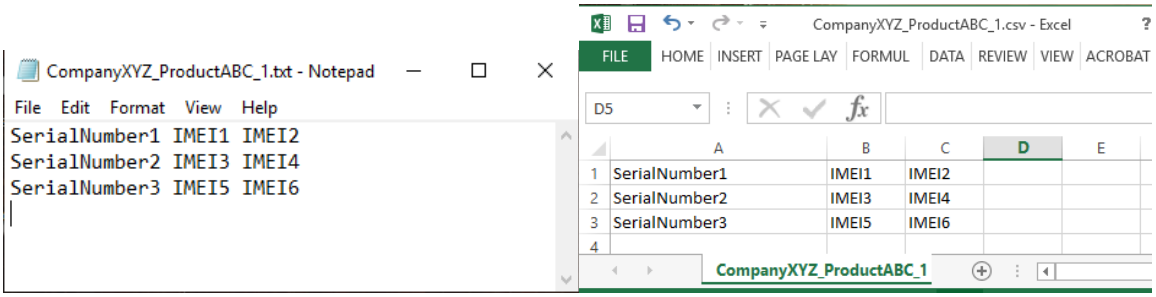


- Once the DEVELOPER uploads the CSV or txt file, an email is automatically sent to the DEVELOPER providing notice that an ESN/MEID/IMEI file has been uploaded and automatically approved.
- The Device identification (ESNs/MEIDs/IMEIs or IMEI/ICCID pairs) provided in the CSV approved file will take up to 15 minutes to load into the VZW DMD system and will be ready for activation then.
- **Test Devices to be sold as production Devices shall be re-uploaded by DEVELOPER as certified Devices via ODP or EDI.**

4.2.2 Dual Device ID Upload

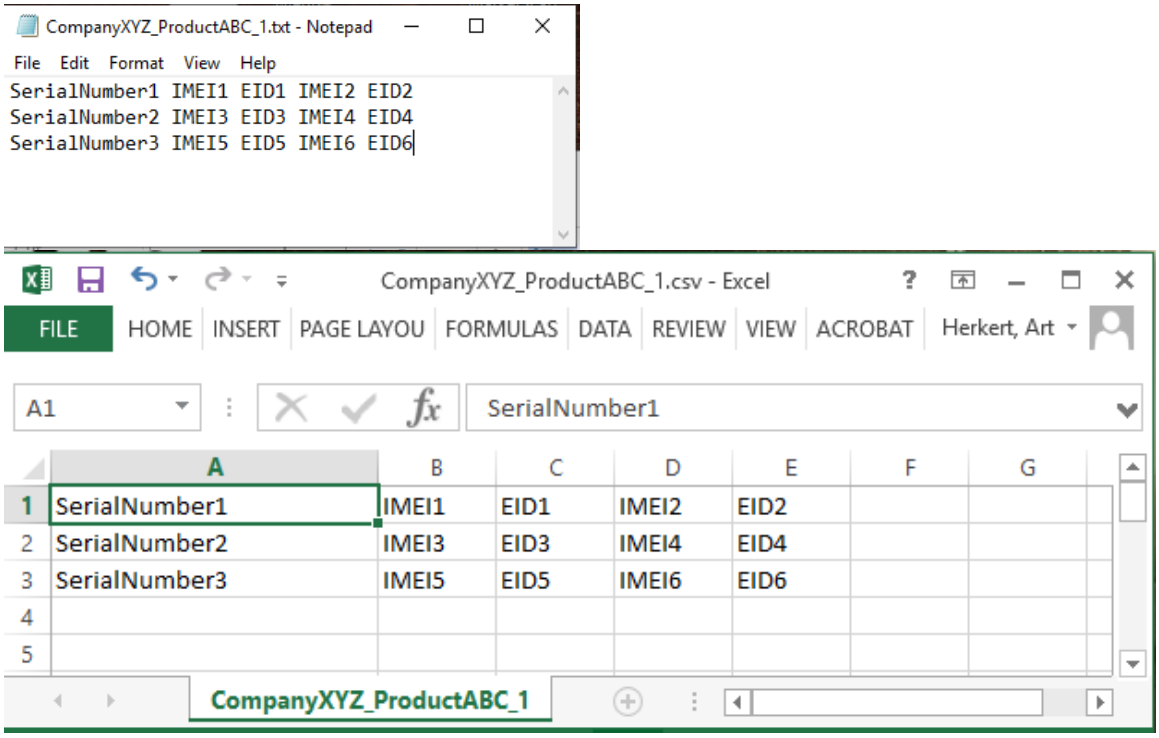
4.2.2.1 2 Physical SIMs mapped to a Single Device SKU

- DEVELOPER captures all of the Device identifications (Serial Number, Device IMEI1, Device IMEI2) in a CSV file or text file as follows:
    - The Serial Numbers will start on the first line of the first column. Device IMEI1 will be stored in the second column, and Device IMEI2 will be stored in the 3rd column.



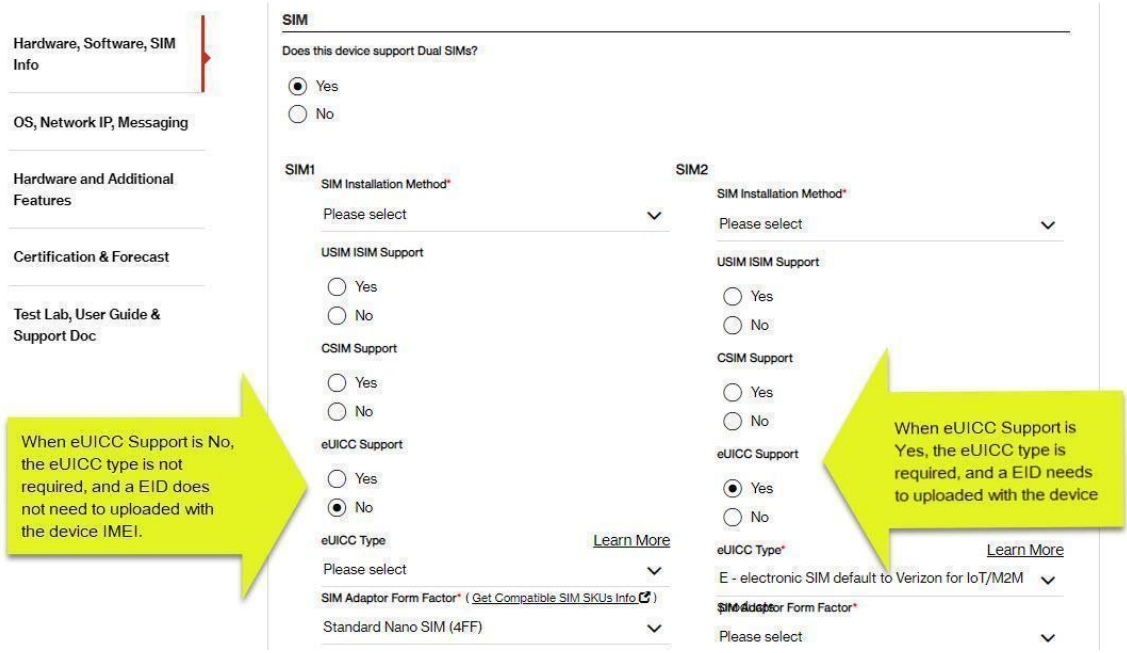
4.2.2.2 2 Electronic SIMS

- DEVELOPER captures all of the Device identifications (Serial Number, Device IMEI1, EID1, Device IMEI2, EID2) in a CSV file or text file as follows:
    - The Serial Numbers will start on the first line of the first column. Device IMEI1 will be stored in the 2nd column, EID1 will be stored in the 3rd column, Device IMEI2 will be stored in the 4th column, and EID2 will be stored in the 5th column.



4.2.2.3 1 Physical SIM and 1 Electronic SIM

- DEVELOPER captures all of the Device identifications in a CSV file or text file.
- The order of the device elements will be dependent on how the device OEM has selected the SIM types in the ODP.



- If the SIM is selected with eUICC support as No, only the device IMEI1 or device IMEI/ICCID pair will required. If the SIM is selected with eUICC support as Yes, the Device IMEI and associated EDI will need to be provided.
- The following table shows the possible combinations of SIM types and required information.

SIM Selection in ODP	**Required Identifiers in uploaded CSV or text file**
Physical SIM, Electronic SIM	Device Serial Number, IMEI1, EMEI2, EID2
Physical SIM/UCCID pair, Electronic SIM	Device Serial Number, IMEI1, UCCID1, IMEI2, EID2
Electronic SIM, Physical SIM	Device Serial Number, IMEI1, EID1, IMEI2

5 OD Certification Agreement Violation Process Flow

Upon knowledge of any Rogue Devices (unapproved Device or approved Device harming the network), Applications or Violations to the CA with VZW the following will take place:

- ODPT notifies DEVELOPER of Device compliance issue (rogue Devices or applications detected, CA violations)
- Developer will ship 2 sample Devices within 48 hours upon receiving the formal request from Verizon for network evaluation.
- VZW retains the right to restrict or deactivate the OD Device if VZW has determined the Device to be harmful to the Network and its end users and de-certify it if necessary.

If a Device fails to comply with the OD Specification, Verizon may de-certify the Device or take any necessary steps to protect the Network and its end-users, including, but not limited to, (a) no provisioning of additional units of the Device on the Network, (b) removal of the Device from the OD website that lists current certified devices, (c) notification to Device end-users of Network issues related to the failure to comply with the OD Specification that impact the Device end-users' service on the Network.

6 Device Evolution, Maintenance & Regression Testing Process Flow

6.1 Device Evolution:

At any time, in case of any updates to the certified software or hardware, DEVELOPER must notify ODPT and provide all submission documentation to the ODPT

- DEVELOPER provides all submission documents with the Device changes in detailed descriptions
- ODPT/NDET determines the level of testing required based on the updated Device.
- DEVELOPER initiates Device Maintenance Release Testing Flow

6.2 Device Maintenance & Regression Testing Process

- DEVELOPER submits updated submission documents to the ODPT/NDET Lab for evaluation, and coordinates with the OD Authorized ITL to execute regression testing (in coordination with VZW NDET Lab).
- After the regression test criteria are completed for the Device, the OD authorized ITL forwards the results to the VZW (ODPT & NDET Lab) to verify that the Device is compliant.
- After the Device successfully passes testing, the ODPT will certify the Device Maintenance Release and issue official notification.

7 Test Lab Contact information

Bureau Veritas (Formerly 7Layers)		Capabilities
APPROVED TESTING LOCATION 1 - MAIN		
Business Contact:	Bureau Veritas Sales	4G Class3 APN, LWM2M (FOTA), OTADM (FOTA), Domestic Field Interoperability Test (DFIT)
Phone:	214-364-3295	
Email:	Jenil.Nathwani@bureauveritas.com	
Technical Contact:	Jenil Nathwani	
Phone:	214-364-3295	
Email:	Jenil.Nathwani@bureauveritas.com	
Business Address:	1293 Anvilwood Ave, Sunnyvale, CA 94089	

Cetecom		Capabilities
Business Contact:	Ray Chung	4G, 5G NR FR1 OTA
Phone:	408-586-6267 (O) / 408-707-7035 (M)	
Email:	ray.chung@cetecom.com	
Technical Contact:	Nicolas Stamber	
Phone:	408-586-6234	
Email:	nicolas.stamber@cetecom.com	
Business Address:	411 Dixon Landing Road, Milpitas CA 95035	

Ericsson		Capabilities
Business Contact:	Omkar Dalal	Interoperability (IOT)
Phone:	972-741-6696	
Email:	omkar.dalal@ericsson.com	
Technical Contact:	Omkar Dalal	
Phone:	972-741-6696	
Email:	omkar.dalal@ericsson.com	
Business Address:	6300 Legacy Dr, Plano, TX 75024	

ATMC Labs (formerly Intertek)		Capabilities
Business Contact:	Lane Linville	LTE, 5G Lab test, RedCap, Live Network test, VoLTE, OTA Radiated Performance, VoWiFi, Domestic Field Interoperability Test (DFIT)
Phone:	859-749-7439	
Email:	lane.linville@atmcl.com	
Technical Contact:	Maurice Abram	
Phone:	765-215-5811	
Email:	maurice.abram@atmcl.com	
Business Address:	721 Enterprise Drive, Lexington, KY 40510	

Motive	Capabilities

Business Contact:	Mahantesh Hiremath	Interoperability (IOT) Motive-bridge (FOTA)
Phone:	+1-972-342-8462	
Email:	mahantesh.hiremath@motive.com	
Technical Contact:	Justin Taylor	
Phone:	+1-512-201-7624	
Email:	justin.taylor@motive.com	
Business Address:	9442 North Capital of Texas Hwy, Building 1, Suite 500, Austin, TX 78759	

Element Materials Technology Washington DC LLC (Formerly PCTEST Engineering Lab)		**Capabilities**
APPROVED TESTING LOCATION 1 - MAIN		
Business Contact:	Dennis Winslow	5G, 4G Lab Conformance, RedCap, Domestic Field Interoperability Test (DFIT)
Phone:	517-898-9429	
Email:	vzw@element.com	
Technical Contact:	Soohee Kwon	
Phone:	410-290-6652	
Email:	vzw@element.com	
Business Address:	7185 Oakland Mills Road, Columbia, MD 20146	
APPROVED TESTING LOCATION 2		
Business Address:	7195-A Oakland Mills Road, Columbia, MD 21046	OTA 5G/4G
APPROVED TESTING LOCATION 3		
Business Address:	382 Piercy Road, San Jose, CA 95138	OTA 5G/4G/RedCap

Arclight Wireless, Inc (Formerly RC Logixx)		**Capabilities**
Business Contact:	Ross Brown	Domestic Field Interoperability Test (DFIT)
Phone:	919.912.9052	
Email:	ross.brown@arclightwireless.com	
Technical Contact:	Brian Tungcab	
Phone:	919.912.9052	
Email:	brian.tungcab@arclightwireless.com	
Business Address:	65 TW Alexander Dr. #12721 Research Triangle Park, NC 27709	

SGS		Capabilities
APPROVED TESTING LOCATION 1 - MAIN		
Business Contact:	James You	LTE, Multi- Mode, VoLTE, VoWiFi, OTA,5G FR2 RF, 5G FR2 Protocol, 5G FR1 (SA/NSA), RedCap, Domestic Field Interoperability Test (DFIT)
Phone:	858-729-8884	
Email:	Jaewon.you@sgs.com	
Technical Contact:	Gerardo Berrelleza	
Phone:	858-775-0712	
Email:	Gerardo.Berrelleza@sgs.com	
Business Address:	15150 Avenue of Science, Suite 300, San Diego, CA 92128	
APPROVED TESTING LOCATION 2		
Business Address:	12310 World Trade Dr, Suite 106/107 San Diego, CA, 92128	OTA, Audio
APPROVED TESTING LOCATION 3		
Business Address:	14 Culnen Dr, Lower Level, Branchburg, NJ 08876	4G & 5G OTA

Tech Mahindra		Capabilities
APPROVED TESTING LOCATION 1 - MAIN		
Business Contact:	Arunav Roy	5G FR1/FR2 VZW Supplemental RF and Protocol, RedCap, VoNR, LTE, VoLTE, Domestic Field Interoperability Test (DFIT)
Phone:	469-600-7846	
Email:	arunav.roy@techmahindra.com	
Technical Contact:	Hiteshkumar Gamdha	
Phone:	908-239-5232	
Email:	Hiteshkumar.Gamdha@techmahindra.com	
Business Address:	Tech Mahindra Americas: 500 Hills Dr, STE 203, Bedminster, NJ 07921	
APPROVED TESTING LOCATION 2		
Business Address:	6092 Stewart Ave, Fremont, CA 94538	5G FR1/FR2 VZW Supplemental RF, OTA 4G/5G

Accenture LLP (Formerly UMLAUT and P3)		Capabilities
Business Contact:	John Pirrello	Domestic Field Interoperability Test (DFIT)
Phone:	973-440-8147	
Email:	john.pirrello@accenture.com	
Technical Contact:	Kranthi Kusuma	
Phone:	949-239-4127	
Email:	kranthi.kusuma@accenture.com	
Business Address:	412 Mount Kemble Ave, Morristown, NJ 07960	

Accenture International Ltd (Formerly UMLAUT and P3)		Capabilities
Business Contact:	Ivan Tucakovic	Global Field Interoperability Test (GFIT)
Phone:	+381628044734	
Email:	ivan.tucakovic@accenture.com	
Technical Contact:	Petar Jandric	
Phone:	+381628044543	
Email:	petar.jandric@accenture.com	

Wireless Research Center		Capabilities
Business Contact:	Jordan Stearns	LTE OTA
Phone:	919-435-1051 ext.102	
Email:	jordan.stearns@wirelesscenter-nc.org	
Technical Contact:	Jordan Stearns	
Phone:	919-435-1051 ext.x102	
Email:	jordan.stearns@wirelesscenter-nc.org	
Business Address:	3331 Heritage Trade Dr. Suite 101, Wake Forest, NC 27587	

IoT Security Penetration Testing Labs

Carve Systems		Capabilities
Business Contact:	Max Sobell	Penetration Testing for IoT Security
Phone:	650-454-0072	
Email:	max.sobell@carvesystems.com	
Technical Contact:	Max Sobell	
Phone:	650-454-0072	
Email:	max.sobell@carvesystems.com	
Business Address:	38 E Ridgewood Ave, #110 Ridgewood, NJ 07450	

Spirent		Capabilities
Business Contact:	Satya Patel	Penetration Testing for IoT Security
Phone:	732-895-9486	
Email:	satya.patel@spirent.com	
Technical Contact:	Satya Patel	
Phone:	732-895-9486	
Email:	satya.patel@spirent.com	
Business Address:	101 Crawfords Corner Road, Suite 4-216 Holmdel, NJ 07733	

Palindrome		Capabilities
Business Contact:	Peter Thermos	Penetration Testing for IoT Security
Phone:	732- 688-0413	
Email:	peter.thermos@palindrometech.com	
Technical Contact:	Peter Thermos	
Phone:	732- 688-0413	
Email:	peter.thermos@palindrometech.com	
Business Address:	100 Village Ct., Suite 300 Hazlet, NJ 07730, USA	