Verizon Wireless

4G LTE “Open Access” Application Guidelines

Version 2.0.

Contents

Revision History

Revision	Amendments	Date
1.0	Document creation	09/10/10
2.0	First revision – including GSMA Guidelines reference	12/11/12

1 Introduction

These application guidelines provide a set of recommended practices and technical standards for developers of 4G LTE applications to facilitate access to Verizon's 4G LTE network while protecting against objectionable interference with other users' of the network and ensuring network security. If your application is targeted to be preloaded on a Verizon Wireless device or launched pursuant to an agreement with Verizon Wireless, more specific and stringent requirements may be provided by Verizon Wireless.

Our philosophy with respect to applications that use our 4G LTE network is that we are **open**. We have the best network and we want our customers to leverage it to drive success for their personal and business needs. We also want developers to be able to bring devices and applications to the network that will result in our customers, and their customers, having more and innovative choices.

At this time, Verizon Wireless does not require advance certification for applications that use our 4G LTE network. This is true both in the case of applications that are designed specifically to work on the Verizon Wireless 4G LTE network, or that may be used on that network by consumers but that will be marketed by the developer through a Non-Verizon Marketing Channel (NVMC). By contrast, we currently have a certification program to ensure modules/devices developed by third parties are compliant with our published technical specifications for the 4G LTE network.

While there is no advance certification requirement for 4G LTE applications, Verizon Wireless does monitor its network and work collaboratively with application developers, app stores, and our customers to ensure that applications operating on our network do not interfere with operation of the network of with other users of the network. The guidelines in this document will be implemented as our standards to review the behavior of applications developed for use on our 4G LTE network.

This document provides 4G LTE application developers guidance with respect to **acceptable application behavior**. This document thus complements the existing 4G LTE module/device certification specifications already published.

Verizon Wireless reserves the right to take the appropriate remedial action against applications in the event of the potentially harmful behaviors described in this document. Since the behavior of all potential applications using the 4G LTE network cannot be predicted, the information detailed in this guideline is necessarily not comprehensive of all acceptable or unacceptable application behaviors. Verizon Wireless reserves the right to take appropriate remedial action for applications performing in a harmful manner even if the behavior is not specifically noted herein.

Verizon Wireless reserves the right to change this policy in the future, and to institute a formal application certification program or test plan without regard to marketing channel. We will give interested parties notice of any such change in policy on the Open Development web portal where the 4G LTE device technical specifications are posted.

1.1 Goal

The Verizon Wireless network is a shared resource among all Verizon Wireless customers. It is important that no application has a detrimental effect on the overall operation of the network or on other customers, such as blocking access to the network, causing objectionable interference to other users, and/or threatening the security of users or the network. Applications developed for use on the network should be well behaved when using shared resources, limited resources, or resources required to maintain customer privacy and security.

The application developer is responsible for the user experience, functionality and quality of its applications as well as compliance with all applicable laws. The specifications in this guideline are intended to ensure that applications are safe for the network and do not violate the security or privacy of customers or otherwise harm users of the network. Applications that are found to compromise the LTE Verizon network, user security or privacy, or in general do not adhere to good engineering practices to avoid interference and/or harm to the network or other users are subject to appropriate remedial actions by Verizon Wireless, including, but not limited to, disabling the application from operating on the network. Likewise, Verizon Wireless may take action to address particular applications as needed to comply with applicable law. To the extent any behavior is addressed in the Verizon Wireless device technical specifications, those requirements also will be enforced.

1.2 Feedback

We are always interested in receiving your feedback. Please contact us with your comments and suggestions at http://opennetwork.verizonwireless.com.

2 Application Guidelines

2.1 GSMA Application Guidelines

Verizon Wireless has adopted the GSMA recommended practices for application development published at http://www.gsma.com/technicalprojects/smarter-apps-for-smarter-phones/. These GSMA guidelines are being used by Verizon Wireless as a baseline for recommended practices for applications that use the 4G LTE network, with the addition of Verizon Wireless specific guidelines and requirements. Compliance with the GSMA guidelines is intended to help prevent objectionable interference by applications or their users with other users of Verizon’s 4G LTE network as well as to protect the security of Verizon’s network and its users.

2.2 Network Aware Applications

Network Aware Applications make use of Verizon Wireless’s network resources or features. Examples are applications that explicitly create network connections (sockets), applications that use HTTP services, applications that generate SMS messages, etc. The design and implementation of Network Aware Applications should make efficient and intelligent use of network resources.

The number and frequency of connections to the network should be minimized such that the application only requests what is necessary for the correct and reliable operation of the application. The application should detect error conditions of the network and/or remote servers and act to avoid adding unnecessary congestion to the network. The bandwidth utilized by the applications should be optimized in order to maintain reliable use of the application, maintain a high level of responsiveness for the user, and reduce opportunities for network congestion. Applications that fail to adhere to these best practices may adversely affect the 4G LTE network and/or users of the network, and may be subject to remedial action if necessary to protect the network or users.

2.3 Verizon Wireless Recommended Application Guidelines

The following table outlines a set of recommended industry practices that Verizon Wireless recommends to all application developers. This set of guidelines is based on the GSMA recommendations with the addition of the Security guideline which was only partially addressed by GSMA.

Relevance	**Guideline**	**For more details, see following GSMA document sections**
Usability/ Asynchrony	Techniques such as pipelining and asynchrony should be used to ensure that the client operates smoothly.	Sections 2.2.1, 4.1.1, 4.2.1, 4.3.1
Efficient network connection usage	Use strategies that minimize and optimize data traffic and avoid unnecessary data transfers, especially when roaming.	Section 2.3
Background/ foreground modes	Deactivate background processes when not required.	Section 2.3, 3.6, 4.2.8
Background/ foreground modes, Scheduling	Design polling applications to aggregate their network activities.	Section 2.3, 3.6, 4.2.9
Connection loss and error handling	Applications should be resilient to changing network conditions and errors.	Section 3.2
Compression	Applications using HTTP should support compression.	Section 3.5
Data push	Applications should use push services in preference to polling.	Section 3.6, 4.2.5, 4.3.3
Security	*Applications should protect the customer content on the device and during data exchange with the cloud servers*	Section 3.3

Table 1 – Verizon Wireless Recommended Application Guidelines

3 Applications Compromising Verizon Wireless LTE Network or Users

Applications that are found to compromise the Verizon Wireless 4G LTE network, user security or privacy are, as set out below, inconsistent with applicable technical standards and could be subjected to remedial action by Verizon Wireless, including, but not limited to, disabling the application from operating on the network.

Verizon Wireless will consider taking remedial action:

i. when an application implementation reveals what is considered an industry worst practice resulting in interference and/or a significant adverse impact on the user and/or the network ;
ii. when an application exposes customers of Verizon Wireless directly to a security and/or a privacy risk, including but not limited to sending Spam or malicious code through customer accounts, or potentially giving customers the ability to see communications destined for other customers;
iii. when an application exploits the Verizon Wireless LTE network to enable the unauthorized resale of Verizon Wireless services;
iv. when an application exposes directly and/or indirectly the Verizon Wireless LTE network to harmful events such as denial of service and security attacks;
v. when such action is needed to comply with applicable laws.

3.1 Worst Application Practices

The following application development practices are considered to significantly impact customer use of the device and/or the network:

3.1.1 Application blocks the device transition to sleep mode

- ***Customer Impact***: Battery life of the device significantly degraded.
- ***Prevention and/or Remediation***: Deactivate background processes when not required (see Section 2.3, 3.6, 4.2.8 of GSMA Guidelines).

3.1.2 Application syncs with cloud server on exact same time schedule

- ***Network Impact***: Simultaneous spike of connections triggered by the same application running on multiple devices and resulting potentially in denial of service attack.
- ***Customer Impact***: Response time and sync schedule of the application could be potentially delayed.
- ***Prevention and/or Remediation***: Use strategies that minimize and optimize data traffic and avoid unnecessary data transfers (see Section 2.3 of GSMA Guidelines).

3.1.3 Handling connection errors to cloud server application exhibits high frequency of retries for long period of time

- ***Network Impact***: High frequency of retries sustained for long period of time can result potentially in denial of service attack on cloud server and on network elements.
- ***Customer Impact***: Battery life of the device significantly degraded.
- ***Prevention and/or Remediation***: Applications should be resilient to changing network conditions and errors (see Section 3.2 of GSMA Guidelines).

3.1.4 Attempting to impersonate Verizon Wireless or using the Verizon Wireless name, logo, or other marks without consent

- ***Customer Impact***: Potential confusion over whether applications have been developed or authorized by Verizon Wireless and/or potential privacy and security threats resulting from that confusion.
- ***Prevention and/or Remediation***: Applications should not suggest or imply an association with Verizon Wireless without the consent of Verizon Wireless.

3.2 Customer Security and Privacy Exposure

- ***Customer Impact***: Major security and/or privacy threat to user and device content. This might include malware used to gain control of user’s device without user knowledge, and/or captures confidential user data, such as user IDs, location, contact list, browsing history, without notification to user. This also may include applications that gain access to the account information of Verizon Wireless customers without their knowledge or consent.
- ***Prevention and/or Remediation***: Security (see Section 3.3 of GSMA Guidelines).

3.3 Harmful Events to Verizon Wireless LTE network

- ***Network Impact***: Application events (intentional or not) that can directly or indirectly constitute a denial of service or a security attack on Verizon Wireless LTE network elements.
- ***Customer Impact***: User experience affected due to potential disruption of service.
- ***Prevention and/or Remediation***:
  - Use strategies that minimize and optimize data traffic and avoid unnecessary data transfers (see Section 2.3 of GSMA Guidelines).
  - Design polling applications to aggregate their network activities (see Section 2.3, 3.6, 4.2.9 of GSMA Guidelines)

4 4G LTE Voluntary Application Test Program

4.1 Process

If you are considering the distribution of an application on the Verizon Wireless 4G LTE network through an NVMC and would like it to be tested for use on Verizon Wireless devices, please contact one of our approved testing houses listed below.

Please note that this voluntary 4G LTE application test program is designed to provide assurance that applications will perform well on the Verizon Wireless network and devices. Passing these tests does not guarantee that the applications will always perform well. And, passing these tests does not insulate the application from remedial action if the application, or one of its iterations or revisions, performs in a harmful manner in violation of these guidelines. Verizon Wireless assumes no liability for the application distributed through an NVMC and our Customer Care team will not be able to support customer complaints related to applications distributed through such channels.

4.2 Fees and Contacts

Application certification will be at the expense of the developer.

Please contact the approved test labs below for current pricing and test procedures.

Intertek
Robbie Payne
ICT Sales Manager
Office: (859)226-1000
Fax: (859)226-1050
Email: Robbie.Payne@Intertek.com
Web Site: http://www.intertek.com/wireless-mobile/

P3 Communications
Ron Housenick
VP Operations
Office: (973) 984-6050
Fax: (973) 689-2760
Email: Ron.Housenick@P3-Group.com
Web Site: http://www.p3-group.com/