
# Requirements for Mobile Device Software Security Updates

## Version 2.0

## 27 November 2020

*This is a Non-binding Permanent Reference Document of the GSMA*

### Security Classification: Non-confidential



### Copyright Notice



### Disclaimer



### Antitrust Notice

# Table of Contents

# 1 Introduction

## 1.1 Overview

Security vulnerabilities in cellular-connected and other types of internet devices can result in significant harm to users worldwide. In the past, it was not possible to provide remote software/firmware security updates to devices. Today, those updates together with new feature capabilities can be implemented on a regular basis, both preventatively and reactively as vulnerabilities and problems are discovered.

The objective for this document is to enumerate requirements that encourage mobile industry action to improve the security of devices of all types that have cellular network access, thereby enhancing overall global cyber security. It focuses on the most important requirements rather than dealing with the detail of aspects such as process inefficiencies. The rationale and background, including case studies, are well documented elsewhere.

## 1.2 Scope

This document establishes high level requirements for security updates for cellular-connected device software, with a particular focus on critical security updates which need to be deployed widely and quickly due to a major security incident of some kind. The software on devices has historically been, and is often still, referred to as firmware. This includes the baseband software, drivers, operating system, communications stacks and application framework. It also includes manufacturer supplied, pre-installed applications such as browser updates which are also controlled and deployed by the manufacturer, rather than through an “app store.”

Updates for applications which a user has installed are specifically out-of-scope for this document, but the requirements here may lead to future recommendations for such applications. Also specifically out-of-scope at this time are inconsistent software version numbering, updating devices older than the specified end-of-life, or the timeframe for producing and delivering security updates. Some of these elements are covered within the specification ETSI EN 303 645.

The requirements in this recommendation acknowledge changes to the global device landscape and that increasingly varied hardware is making use of cellular connectivity. As a result, many of the principles and methods outlined in this current version will be applicable to internet of Things (IoT) and machine-to-machine (M2M) devices.

The recommendations provided in section 2 complement the GSMA IoT Security Guidelines for IoT Endpoint Ecosystem [2], which explains the best practice for securely deploying updates over-the-air as part of a methodology for developing secure IoT services. The IoT Security Guidelines for IoT Endpoint Ecosystem includes an IoT Security Assessment Checklist [3], which can be used by companies to aid compliance.

Developers of IoT services may find it useful, in addition, to refer to the current document (FS.25) for recommendations on the frequency of security updates, duration of device support or replacement and preferred channels for alerting end-point users to the availabillty and content of patches. Software updates which are provided by other parties which are not Mobile Network Operators or Manufacturers (such as IoT solution providers), are considered beyond the scope of this document.

.

## 1.3 Definitions

| Term | Definition |
|---|---|
| Device | A cellular radio telephone that includes all of the following features:<br>• utilises a mobile operating system;<br>• has cellular network connectivity.<br>A Device may be a handset or an Internet of Things (IoT) device. Examples are primarily smartphones, although today many of these functions can also be performed by other SIM-enabled devices such as tablets with cellular network connectivity and automotive infotainment units deployed in modern vehicles. |
| Device manufacturer | A company that designs and produces a device, including its mobile operating system software (also known as firmware). The mobile operating system may be developed by the device manufacturer or by some other entity, in which case the device manufacturer typically performs some kind of customization and adds device drivers. The device manufacturer is able to develop software updates for his devices (products). |
| End user | A person who is using the device. If security updates are not available for a device, the data of the end user using the device could be at risk. |
| Handset | A device which also possesses a user interface, the capability to utilise mobile software applications, access and browse the Internet, utilise text messaging, utilise digital voice services, and send and receive e-mail. |
| IoT Device | A device which may also be characterised by:<br>• Constrained or ultra-constrained properties – for example, radio, network bandwidth, battery life, processor power, limited memory, etc.;<br>• Safety-related and cyber-physical considerations;<br>• A lack of user interface – so-called “headless” devices;<br>• May be supported by another device such as a companion device and smartphone application, or gateway/hub. |
| Mobile network operator | An entity which offers licensed telecommunications services over an air interface.<br>Mobile network operators may sell devices to end users together with their contracts and promise the availability of certain services, such as telephony, messaging, or internet access. In order to guarantee service availability, mobile network operators usually perform testing to validate devices and software updates before approving them. |
| Security update, software security update | A software update (see below) whose main intention is to fix security vulnerabilities that were identified in the original mobile operating system/firmware, often after the device has been produced and delivered. |
| Smartphone | A device with a large display, predominantly with touch screen technology, a fast processor and memory in the GB range. A fully-featured OS / platform that provides voice and data communications capabilities, enables personalisation of the device by the user and |

| | |
|---|---|
| | additionally supports installation and maintenance of mobile applications (e.g. downloadable from an application store). |
| Software update | An update of the mobile operating system software/firmware controlled and deployed by the device manufacturer, rather than through an app store.<br>Software updates may implement additional features (also called feature update), fix bugs (also called maintenance release), or they may be focused on fixing one or more security vulnerabilities (security update).<br>Although this document does not require any specific delivery method of such updates, updates of certain operating system components may require the installation of a complete firmware update. |

## 1.4 Abbreviations

| Abbreviation | Definition |
|---|---|
| COM | Communication-related requirement |
| CVE | Common Vulnerabilities and Exposures - https://cve.mitre.org/ |
| GSMA | The GSM Association – www.gsma.com |
| IoT | Internet of Things |
| M2M | Machine to Machine |
| MNO | Mobile Network Operator |
| PLMN | Public Land Mobile Network |
| SEC | Security-related requirement |
| SSU | Software Security Updates |
| TES | Testing-related requirement |

## 1.5 Requirements Format

Requirements are denoted using the format XXX-YYY-ZZZZ, where:

- XXX denotes this document: SSU (Software Security Updates),
- YYY denotes the related section: e.g. SEC (Security Only Updates),
- ZZZZ denotes a four digit numbering format which increments by 10 numbers for each requirement, allowing for future updates: e.g. 0020, 0030 etc.

Normative text (i.e. the requirements) is contained within the requirements tables. The remainder of the text is considered to be non-normative and therefore informative and supporting text.

## 1.6 References

| Ref | Doc Number | Title |
|---|---|---|
| [1] | ETSI EN 303 645 | CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements<br>https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf |
| [2] | GSMA CLP.13 | IoT Security Guidelines for IoT Endpoint Ecosystem<br>https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/ |

| Ref | Doc Number | Title |
|---|---|---|
| [3] | GSMA CLP.17 | GSMA IoT Security Assessment https://www.gsma.com/iot/iot-security-assessment/ |
| [4] | RFC 2119 | "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt |

### 1.7 Conventions

The key words "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in RFC2119 [4].

## 2 Device Security Updates Requirements

The following requirements are expected to be implemented by device manufacturers and mobile network operators (MNOs).

### 2.1 Standards Adherence

| Req. Number | Requirement |
|---|---|
| SSU-SEC-0001 | The requirements in ETSI EN 303 645 [1] Section 5.3 SHOULD be followed. |

### 2.2 Security Only Updates

The following requirement is designed to prevent scope and feature creep into streamlined or emergency / prioritised security updates. This is to streamline the process so that operators can deliver high-priority security fixes reliably and in a timely manner.

| Req. Number | Requirement |
|---|---|
| SSU-SEC-0010 | Where an update is issued to specifically fix a particular security vulnerability or set of vulnerabilities, device manufacturers must provide security updates that *only* fix the security problems they are designed to address (as identified by a list of CVEs (Common Vulnerabilities and Exposures), for example) and not other, non-security related fixes. |

Separating urgent security software updates from other types of updates minimises both the development time and the quality assurance overhead for security updates, and allows them to be deployed as quickly as possible. General software updates are not covered by this requirements document.

### 2.3 Regular Security Update Cadence

A regular security update cadence (for example, on a monthly basis) increases cyber security by inoculating devices against security problems they may face, from vulnerabilities to active exploits.

| Req. Number | Requirement |
|---|---|
| SSU-SEC-0020 | For devices capable of being updated, device manufacturers must provide regular security updates (e.g. monthly) throughout the lifetime of the device.<br>Note: For constrained and ultra-constrained devices, manufacturers and |

| | |
|---|---|
| | network operators need to consider practical issues such as network bandwidth, limited processing power and battery life. |
| SSU-SEC-0021 | Device manufacturers, where the device software is under their control, should deploy the security updates across their device range by prioritising the update on the most popular models. |

Historically, device manufacturers have prioritised security updates on device models based on various different business reasons. However, device vendors can significantly reduce the risk of known vulnerability exploitation by deploying security updates starting with the most popular device models.

When a device is a constrained device, manufacturers should consider the use of a companion device such as a hub, if available, to facilitate security updates.

For situations where devices cannot be patched - a replacement plan needs to be in place and be clearly communicated to the user. This plan would typically detail a schedule for when technologies will need to be replaced and, where applicable, when support for hardware and software ends (in accordance with ETSI EN 303 645 Section 5.3-14 and 5.3-15 [1]).

### 2.4 End-of-Life Policy

The following two requirements build upon Provision 5.3-13 in ETSI EN 303 645[1].

| Req. Number | Requirement |
|---|---|
| SSU-SEC-0030 | Device manufacturers, where the device software is under their control, must continue to provide software security updates for at least 36 months from the launch date of the device. |
| SSU-SEC-0040 | Where a device cannot be updated within the period listed in requirement SSU-SEC-0030, the device should be replaceable. |

NOTE: This means that when the last product is sold by the manufacturer it must dedicate engineering resources or “patch teams” to ensure that a product is adequately supported with security updates, where the device software is under its control.

## 3 Communication of Security Updates to End Users

These requirements cover the communication of the availability of security updates to end users. These requirements build upon Provisions 5.3-11 and 5.3-13 in ETSI EN 303 645[1].

| Req. Number | Requirement |
|---|---|
| SSU-COM-0010 | Device manufacturers and mobile network operators must notify end users about the availability of a security update via one or more of the following channels:<br>• Device based notification (strongly preferred)<br>• Website |

| | |
|---|---|
| | • Other communications |
| SSU-COM-0020 | Device manufacturers and mobile network operators must explicitly communicate to users that a security update is a security update. |
| SSU-COM-0030 | Device manufacturers and mobile network operators should make available information to end users about the content of a security update. |
| SSU-COM-0040 | Device manufacturers and mobile network operators should ensure that users can ascertain to what extent a device is patched in a clear and easy-to-understand way - for example, through a user interface menu option that shows the current security release/patch level and the date it was applied to the device.<br>Where a device is a constrained device, manufacturers should make use of a companion device such as a hub and / or companion smartphone application, if available, to assist users in their understanding. |
| SSU-COM-0050 | Users should be able to discover the minimum length of time for which software updates will be available for their device - for example, by means of a website and/or through a user interface menu option. |

NOTE: It is important to consider that security can be undermined by fraudsters and phishing emails/push messages claiming to be updates. Implementers should design notification mechanisms to take these threats into account.

# 4 Device Security Updates Testing & Release Requirements

## 4.1 Device Update Testing, Approval & Release

The following requirements are expected to be implemented by mobile network operators.

| Req. Number | Requirement |
|---|---|
| SSU-TES-0010 | Where software testing needs to be carried out by mobile network operators, they must ensure that device testing of security only updates is completed within one week. |
| SSU-TES-0020 | Where a mobile network operator is using its own software update servers for patch management and the device is unable to be updated by the mobile network operator, the device may revert to the device manufacturer's update servers. |

The following requirement is expected to be implemented by both device manufacturers and mobile network operators.

| Req. Number | Requirement |
|---|---|
| SSU-TES-0030 | Device manufacturers and mobile network operators, as soon as updates are approved for release, must not prevent customers from receiving device software security updates.<br>Unless: the device has been relinquished from the mobile network operator's control temporarily or permanently, by e.g.<br>• User rooting of the device / user-driven software update which modifies the original manufacturer's software/firmware |

| | |
|---|---|
| | • If the subscription has been changed to another network operator<br>Note: for some IoT devices and use cases which may utilise multi-IMSI SIMs and multi-SIM devices, the deployment of software updates may be the responsibility of other parties such as an IoT solution provider. |

NOTE: No implementation details are discussed and the conditions for this requirement to be satisfied are a matter for individual operators and manufacturers to agree bilaterally.

# Annex A Document Management

## A.1 Document History

| Version | Date | Brief Description of Change | Approval Authority | Editor / Company |
|---|---|---|---|---|
| 1.0 | 18 Sep 2017 | First version | TG | David Rogers, Copper Horse Ltd. |
| 2.0 | 27 Nov 2020 | Revised version to extend scope to IoT devices | FASG | James Tyrrell, Copper Horse Ltd. |

## A.2 Other Information

| Type | Description |
|---|---|
| Document Owner | Device Security Group |
| Editor / Company | James Tyrrell, Copper Horse Ltd. |

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.