E-Blink
Wireless Fronthaul Technology

Software Security Requirements

KDB594280 D02-FCC

Table of contents

REFERENCE DOCUMENTS

Ref[1] : FL58 Product Description 1.1 – FCC.pdf

Ref[2] : 133826-668754-CEN.pdf and 133826-668754-REM.pdf

SOFTWARE SECURITY DESCRIPTION

General Description

1. **Describe how any software/firmware update will be obtained, downloaded, and installed. Software that is accessed through manufacturer's website or device's management system, must describe the different levels of security.**
   It is to be noted that the FL58-45 is not a WIFI device neither a consumer device intended for home nor enterprise usage, but a telecommunication system intended to LTE mobile operators. As such, usage of firmware (FW) on the FL58-45 is fully controlled.

   As a reminder (please refer to [Ref1]), a FL58-45 system is composed of 2 Hardware units (aka WFM modules) making a wireless fronthaul link between a LTE BBU and RRH. FL58-45 shall only be used for that purpose.
   The FL58-45 is controlled by a Local Maintenance terminal (sometimes called craft terminal), named "Local and Remote Maintenance Terminal" (LRMT), since it can be used locally to the radio site or remotely from the radio site.

   The FL58-45 may need new firmware, which would be developed by EBlink. The firmware is not open to external development, i.e. FL58-45 firmware is exclusively developed by EBlink.
   When a new firmware is available (again produced by EBlink), it is provided to the customers who need it, under a controlled way. Again end customers are necessarily restricted to LTE operators. The firmware is provided by file transfer to the customer, via secured methods agreed with customer.

   The firmware is uploaded to a FL58-45 via the LRMT. The LRMT connects to a FL58-45 via TCP-IP, and uploads the new FW to a WFM of a FL58-45 link. The firmware can then be forwarded to the other WFM by the 1st WFM module. Alternatively, the user connects the LRMT to the other WFM module and uploads the new firmware.
   Multiple checks (checksum, header tag) are performed on the FW file before activation.

2. **Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited, such that, it will not exceed the authorized parameters?**

   Any radio parameters modifiable by firmware are ensured to remain within the authorized limits defined by FCC, as depicted in the test report (Ref[2]).

   Indeed, the output power is set automatically by the FL58-45, depending on predefined LTE configurations. A predefined LTE configuration is selected by the customer using the LRMT. In any case, the output power is always below the authorized limits set by the FCC. The tests report provides the FL58-45 behaviour with all possible predefined LTE configurations supported by the FL58-45.

   Finally, the frequency plan might be modified by the customer using the LRMT. The frequency plan can be modified only in the limits of the 5725MHz – 5850MHz frequency band authorized by FCC. The tests report provides the FL58-45 behaviour with all representative possible frequency plans supported by the FL58-45.

3. **Describe in detail the authentication protocols that are in place to ensure that the source of the software/firmware is legitimate. Describe in detail how the software is protected against modification.**

   EBlink provides customers with executable firmware only. Source code is kept secret in EBlink. The FL58-45 hardware is proprietary and cannot accommodate standard WIFI software/firmware. No information is published on the HW or EBlink FW, so that it is almost impossible for non-EBlink personnel to develop a firmware for the FL58-45.
   The firmware is delivered as an encrypted package to customers. The package is protected by a password which is not accessible by customers. The password is only known by the LRMT software, which is provided as executable only.

4. **Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.**

   The firmware is delivered as an encrypted package to customers. The package is protected by a password which is not accessible by customers. The password is only known by the LRMT software, which is provided as executable only.

5. **Describe in detail any encryption methods used to support the use of legitimate software/firmware.**

   Each FW is signed with a specific header tag - kept confidential – containing :
   - File checksum
   - Version stamp
   - File size

6. **For a device that can be configured as a master and client (with active or passive scanning), explain how the device ensures compliance for each mode? In particular if the device acts as master in some band of operation and client in another; how is compliance ensured in each band of operation?**

   Not relevant. FL58-45 is not configured in master / client mode as described above, but as a pair of modules to make a radio link.

Third-Party Access Control

1. **Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification.**

   EBlink provides customers with executable firmware only. Source code is kept secret in EBlink.
   The FL58-45 hardware is proprietary and cannot accommodate non-EBlink software/firmware (unlike some WIFI devices). No information is published on the HW or EBlink FW, so that it is almost impossible for non-EBlink personnel to develop a firmware for the FL58-45.
   No third party Software can be used on FL58-45.

2. **What prevents third parties from loading non-US versions of the software/firmware on the device? Describe in detail how the device is protected from "flashing" and the installation of third-party firmware such as DD-WRT.**

   No third party Software can be used on FL58-45 – please refer to 1) above.

3. **For Certified Transmitter modular devices, describe how the module grantee ensures that hosts manufactures fully comply with these software security requirements for U-NII devices. If the module is controlled through driver software loaded in the host, describe how the drivers are controlled and managed such that the modular transmitter parameters are not modified outside the grant of authorization.**

   Not relevant. FL58-45 is not in the scope of Certified Transmitter modular devices approach.

SOFTWARE CONFIGURATION DESCRIPTION

USER CONFIGURATION GUIDE

1. **To whom is the UI accessible? (Professional installer, end user, other.)**

   The LRMT (UI) is accessible to professional installers and commissioning engineers only. In addition, a support call personal can also access the UI when it is needed.

   a) What parameters are viewable to the professional installer/end-user?

   Parameters viewable by the user are:
   - Inventory information (serial n°, version)
   - Product status
   - Radio link status
   - LTE configuration
   - IP configuration
   - FL58-45 Frequency plan (in the limits set by FCC)

   b) What parameters are accessible or modifiable by the professional installer?

   The following parameters are modifiable by commissioning engineers only:
   - LTE configuration
   - IP configuration
   - FL58-45 Frequency plan (in the limits set by FCC)

   Please refer to question 2 of general description for details.

   (1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

   Yes, the LRMT ensures only valid values are entered

   (2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

   LRMT and FL58 ensure such control.
   Please refer to question 2 – general description for details.

   c) What parameters are accessible or modifiable to by the end-user?
   (1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
   (2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

   The FL58-45 shall be used by LTE operators, with professional installers. End user consumers shall not use FL58-45.

   d) Is the country code factory set? Can it be changed in the UI?
   (1) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?

   There is no country code associated to the FL58-45 firmware.
   Its firmware is unique and complies with FCC regulations

e) What are the default parameters when the device is restarted?

Before product commissioning, if the device is restarted all parameters are set with their default values derived from radio calibration done in factory.
After commissioning, if the device is restarted all parameters are set with values entered during commissioning.
In any case, parameters remain conform to FCC.

2. **Can the radio be configured in bridge or mesh mode? If yes, an attestation may be required. Further information is available in KDB Publication 905462 D02.**

   There is no such mode possible for the FL58-45.

3. **For a device that can be configured as a master and client (with active or passive scanning), if this is user configurable, describe what controls exist, within the UI, to ensure compliance for each mode. If the device acts as a master in some bands and client in others, how is this configured to ensure compliance?**

   Not relevant. FL58-45 is not configured in master / client mode as described above, but as a pair of modules to make a radio link.

4. **For a device that can be configured as different types of access points, such as point-to-point or point-to-multipoint, and use different types of antennas, describe what controls exist to ensure compliance with applicable limits and the proper antenna is used for each mode of operation. (See Section 15.407(a))**

   Not applicable for EBlink FL58-45 device today. FL58-45 works in point to point only with integrated antenna.