

Software security for UNII Devices

Digi International
11001 Bren Road East
Minnetonka, MN 55379
USA

To Whom It May Concern:

Product/Model/HVIN: ConnectCore 6UL

FCC ID: MCQ-CCIMX6UL

IC ID: 1846A-CCIMX6UL

In this document the following definitions are used to describe the different level of parties involved:

1. **Module manufacturer**, in this case Digi International, the party selling the embedded module to host product manufacturers
2. **Host product manufacturer** is the third party responsible for integrating the module into the host product
3. **Installer or professional installer** is the party responsible for putting the end product into operation. The end product can either be the host product or a product containing the host product
4. **End user** is the party using the end product

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES acc. to KDB 594280

SOFTWARE CONFIGURATION DESCRIPTION	
<u>General Description</u>	
<u>1</u>	<p>Describe how any software/firmware updates for elements than can affect the device's RF parameters will be obtained, downloaded, validated and installed. For software that is accessed through manufacturer's website or device's management system, describe the different levels of security as appropriate.</p> <p>The device's RF parameters can be affected by the following elements:</p> <ol style="list-style-type: none">1. The firmware running on the radio transceiver chip on the device and its configuration file2. The board data file that contains calibration, regulatory domain, channel limits and power settings3. The device driver and in particular its configuration file(s) <p>The ConnectCore 6UL module is manufactured and sold with none of the above.</p> <p>Digi International distributes the firmware, board data file and device driver that allows to operate the module for the authorized modes of operation in the following way:</p> <ol style="list-style-type: none">1) The firmware image including its configuration is distributed in binary

	<p>form only by the radio transceiver manufacturer, Qualcomm. The source code of this firmware and configuration is not distributed by Qualcomm in any way.</p> <p>2) The board data file that contains the calibration and power settings is distributed by Digi International in binary form only. Only a board data file for the US regulatory domain is provided, with power settings and channel limits for the US region. Digi International only provides the board data file for non US regions to host product manufacturers that sign a contractual agreement which regulates that the device may not be operated outside its authorized region.</p> <p>3) Digi International provides the host product manufacturers with the driver source and configuration files that match the authorized modes of operation.</p>
<p><u>2</u></p>	<p>Describe the RF parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited such that any other software/firmware changes will not allow the device to exceed the authorized RF characteristics?</p> <p>The software interface between the firmware running on the module and the device driver running on the host processor is defined by Qualcomm. Via this software interface, the host configures the operation of the module.</p> <p>The mode selection (client/master) and its configuration parameters can be set by the host, except output power, available channels and modulation settings that are set by the board data file and cannot be modified by the host.</p> <p>Digi International provides the host product manufacturers with default configuration files with operating modes that match the device's authorized modes of operation.</p>
<p><u>3</u></p>	<p>Describe in detail the authentication protocols that are in place to ensure that the source of the RF-related software/firmware is valid. Describe in detail how the RF-related software is protected against modification.</p> <p>At module power-up the RF-related firmware necessary for the module to operate is downloaded from the host to the module. This firmware is provided by Qualcomm, the manufacturer of the radio transceiver on the device. The firmware from Qualcomm is available as a binary image only. The sources for this software are not disclosed by Qualcomm to anyone. Modifications of the firmware require in-depth knowledge of the transceiver chip operation, it is therefore not possible to easily manipulate this firmware by third parties.</p>
<p><u>4</u></p>	<p>Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.</p> <p>As described in the answer to the previous question (3) it is not possible to easily manipulate this firmware by third parties since the firmware from Qualcomm is available as a binary image only and the Sources for this software are not disclosed by Qualcomm to anyone.</p> <p>Similarly and as pointed out in answer (1), the board data files are not part of the firmware and are distributed in binary form only. The tools used to modify this board data file are not distributed by neither Qualcomm nor Digi International and manipulation would require in-</p>

	depth knowledge of the firmware source, which as explained above is also not disclosed by Qualcomm.
<u>5</u>	<p>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?</p> <p>The ConnectCore 6UL module is certified to operate as both client and master in following channels:</p> <ul style="list-style-type: none"> • Channels 1-11 (2412 – 2462MHz) • Channels 36 – 48 (5180 – 5240MHz) • Channels 149 – 165 (5745 – 5825MHz) <p>In all other channels, ConnectCore 6UL can only be used as a client, since the RF chip has no hardware radar detection capability and uses passive scanning in these channels.</p>
<u>Third-Party Access Control</u>	
<u>1</u>	<p>Explain if any third parties have the capability to operate a U.S.-sold device on any other regulatory domain, frequencies, or in any manner that may allow the device to operate in violation of the device’s authorization if activated in the U.S.</p> <p>Third parties do not have the capability to operate the U.S.-sold devices in a manner which would violate the FCC authorization. As explained in point (1) above, only the board data file for the US regulatory domain is provided by Digi International. This board data file mandates what regulatory domain, output power and TX/RX channels are allowed, and cannot be easily modified by third parties. A board data file for other regions is only provided to customers after signing a contractual agreement that regulates that the device may not be operated outside of its authorization.</p>
<u>2</u>	<p>Describe, if the device permits third-party software or firmware installation, what mechanisms are provided by the manufacturer to permit integration of such functions while ensuring that the RF parameters of the device cannot be operated outside its authorization for operation in the U.S. In the description include what controls and/or agreements are in place with providers of third-party functionality to ensure the devices’ underlying RF parameters are unchanged and how the manufacturer verifies the functionality.</p> <p>The device will only operate with a valid board data file. Only the board data file for the US regulatory domain is provided by Digi International. This board data file mandates what regulatory domain, output power and TX/RX channels are allowed, and cannot be easily modified by third parties. A board data file for other regions is only provided to customers after signing a contractual agreement that regulates that the device may not be operated outside of its authorization.</p>
<u>3</u>	For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers fully comply with these

	<p>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 RF parameters are not modified outside the grant of authorization.</p> <p>We refer to our answer in the General description (1). The device is controlled through device driver software running on the host product and in particular by the board data file. Digi International provides the host product manufacturers with a board data file that matches the authorized modes of operation. In particular, regulatory domain, power settings and channel limits are mandated by the board data file and cannot be modified.</p>
	SOFTWARE CONFIGURATION DESCRIPTION
USER CONFIGURATION GUIDE	
<u>1</u>	<p>Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences.</p> <p>The Host Product manufacturer can view and configure the mode of operation (Client/Master) and its configuration, with the exception of regulatory domain, power limits and available channels which are mandated by the board data file. A board data file for non-US regions is only provided to customers after signing a contractual agreement that regulates that the device may not be operated outside of its authorization.</p>
<u>1.a</u>	<p>What parameters are viewable and configurable by different parties?</p> <ul style="list-style-type: none"> i. The Host Product manufacturer can view and configure the mode of operation (Client/Master) and its configuration, with the exception of regulatory domain, power limits and available channels which are mandated by the board data file. ii. If the host product manufacturer does not include further restrictions the installer or professional installer may view and configure the mode of operation (Client/Master) and its configuration, with the exception of regulatory domain, power limits and available channels which are mandated by the board data file. iii. If the host product manufacturer does not include further restrictions, the end-user may be able to view and configure the mode of operation (Client/Master) and its configuration, with the exception of regulatory domain, power limits and available channels which are mandated by the board data file.
<u>1.b</u>	<p>What parameters are accessible or modifiable by the professional installer or system integrators?</p> <p>If the host product manufacturer does not include further restrictions the installer or professional installer may view and configure the mode of operation (Client/Master) and its configuration, with the exception of regulatory domain, power limits and available channels which are mandated by the board data file.</p>
<u>1.b(1)</u>	<p>Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?</p>

	<p>Yes, the parameters are limited and the installer does not have access to configure the parameters in such a way that would violate the FCC authorization. The board data file mandates regulatory domain, power limits and available channels.</p>
<u>1.b(2)</u>	<p>What controls exist that the user cannot operate the device outside its authorization in the U.S.?</p> <p>The user does not have access to configure the parameters in such a way that would violate the FCC authorization.</p>
<u>1.c</u>	<p>What parameters are accessible or modifiable by the end-user?</p> <p>If the host product manufacturer does not include further restrictions, the end-user may be able to view and configure the mode of operation (Client/Master) and its configuration, with the exception of regulatory domain, power limits and available channels which are mandated by the board data file.</p>
<u>1.c(1)</u>	<p>Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?</p> <p>Yes, the parameters are limited and the end-user does not have access to configure the parameters in such a way that would violate the FCC authorization. The board data file mandates regulatory domain, power limits and available channels.</p>
<u>1.c(2)</u>	<p>What controls exist so that the user cannot operate the device outside its authorization in the U.S.?</p> <p>The parameters are limited and the user does not have access to configure the parameters in such a way that would violate the FCC authorization. The board data file mandates the regulatory domain, power limits and available channels which are mandated by the board data file.</p>
<u>1.d</u>	<p>Is the country code factory set? Can it be changed in the UI?</p> <p>The country code is factory set to US and only the board data file for the US regulatory domain is provided. This board data file mandates what output power and TX/RX channels are allowed, and cannot be easily modified by third parties. Board data file for other regions are only provided to customers after signing a contractual agreement that regulates that the device may not be operated outside of its authorization.</p>
<u>1.d(1)</u>	<p>If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?</p> <p>The country code can only be changed by using a different board data file binary which is only provided after signing a contractual agreement that regulates that the device may not be operated outside of its authorization.</p>
<u>1.e</u>	<p>What are the default parameters when the device is restarted?</p> <p>The default parameters are determined by the host product manufacturer except the regulatory domain, output power and channel selections that are mandated by the board data file.</p>
<u>2</u>	<p>Can the radio be configured in bridge or mesh mode? If yes, an attestation may be required. Further information is available in KDB</p>

	<p>Publication 905462 D02.</p> <p>No the device can not be configured in bridge or mesh mode.</p>
<u>3</u>	<p>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?</p> <p>The module is certified to operate as client on all channels and as master on non-DFS channels as it lacks radar detection capabilities.</p>
<u>4</u>	<p>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))</p> <p>The directional gain of the antennas supported does not exceed 6dBi. For this reason, the antennas are not limited to a specific usage (like point-to-point or point-to-multipoint).</p>



McCall, Scott, Manager, Hardware Engineering

Digi International
11001 Bren Road East
55343 Minnetonka
USA
+1 (952) 912-4248