SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES Declaration

For Certification Service in the USA

Federal Communications Commission
Equipment Authorization Division, Application Processing Branch
7435 Oakland Mills Road
Columbia, MD 21048

To whom it may concern

Pursuant to Section III of KDB 594280 D02 Device Security we attest as follows for the product listed below:

FCC ID	Model name
2A9TU-322001	322001

We declare that no third party will have software, or configuration control, to program the device out of compliance of the technical rules under which it has been certified. Details may be found in the annex.

Applicant/Approval Holder

Company Name: AVL DiTEST GmbH
FRN:
Contact Name: Heinz Schaffler-Pichl
Address: Alte Poststrasse 156
8020 Graz
Austria
Phone: +43 316 787 4748
Email: Heinz.Schaffler-Pichl@avl.com

Unterschrieben

Qualifiziert signiert von Heinz Schaffler-Pichl, 13.05.2025 10:04
AVL DiTEST GmbH, Austria

Annex

SOFTWARE SECURITY DESCRIPTION			
		Description	Comments
General Description	1.	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.	Firmware updates are distributed via customer PC software. Updates are encrypted and signed based on private/public keys.
	2.	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?	RF parameters are contained in the Wi-Fi module and cannot be altered, unless an authorized and compliant update is provided by the Wi-Fi module manufacturer, which will be included in the VCI One firmware update.
	3.	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.	Authenticity and validity are enforced by a signed firmware checksum, which is verified during the update process.
	4.	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	The firmware is encrypted with an encryption similar to TLS. A random AES key is created and used to encrypt the firmware. It is encrypted with an RSA public key and appended to the encrypted firmware. The firmware has the RSA private key to decrypt the AES key to be able to decrypt the firmware with it.
	5.	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?	The VCI One acts as a client. The compliance in each band of operation is ensured by the country settings, which come with the Wi-Fi module. The access point mode is operating in the 2.4 GHz band only.
		Description	Comments
Third-Party Access Control	1.	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	No

		allow the device to operate in violation of the device's authorization if activated in the U.S.	
	2.	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.	No
	3.	For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers 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 RF parameters are not modified outside the grant of authorization.	The drivers have been provided by the Wi-Fi module manufacturer. Software updates are encrypted and signed to ensure authenticity of the drivers.
SOFTWARE CONFIGURATION DESCRIPTION			
		Description	Comments
USER CONFIGURATION GUIDE	1.	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.	The user cannot alter any RF-related configurations through the UI.
	1.a.	What parameters are viewable and configurable by different parties	None
	1.b.	What parameters are accessible or modifiable by the professional installer or system integrators?	None
	1.b.(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Not applicable
	1.b.(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Not applicable

	1.c.	What parameters are accessible or modifiable by the end-user?	None
	1.c.(1)	Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	Not applicable
	1.c.(2)	What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	Not applicable
	1.d.	Is the country code factory set? Can it be changed in the UI?	The factory default is a safe world roaming setting. It is changeable by the user software in accordance with the PC's country settings but cannot be changed in the UI.
	1.d.(1)	If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	Not applicable
	1.e.	What are the default parameters when the device is restarted?	The device will use the same parameters as before. Restarting does not change any parameters.
	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.	No
	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?	The device acts as a client only. The access point mode can only be used in the 2.4 GHz band.
	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))	The access point mode can only be used in the 2.4 GHz band. The parameters are contained in the Wi-Fi module and are thereby ensured to comply with the applicable limits.