Software security for UNII Devices

Roche Diagnostics GmbH
Sandhofer Strasse 116
D-68305 Mannheim, Germany

To Whom It May Concern:

Product/Model/HVIN: cobas h232 / H232 / H232-HBM 4.5
FCC ID: VO9-H232
IC ID: 3100B-H232

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

SOFTWARE CONFIGURATION DESCRIPTION	
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. The firmware for the RF-module is static and will not be changed (original driver from manufacturer). External (3rd party) applications are not accepted on the device. Any Roche application updates are hash-signed (SHA256).
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? The firmware for the RF-module is static and will not be changed (original driver from manufacturer) and will not be changed by the application.
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. Updates are signed by Roche certificate. Unauthorized update packages will not be accepted by the internal update process. Update software is provided by Roche solely.
4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. The firmware for the RF-module is static and will not be changed (original driver from manufacturer). External (3rd party) applications are not accepted on the device. Any Roche application updates are hash-signed (SHA256).
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? N/A
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 allow the device to operate in violation of the device's authorization if activated in the U.S. N/A
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. External (3rd party) applications are not accepted on the device.
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. N/A
	SOFTWARE CONFIGURATION DESCRIPTION
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.

1.a	What parameters are viewable and configurable by different parties? SSID and Server-IP are read-only visible in the UI for every user. Any RFparameter are controlled by a remote server application within the customer's environment. The remote server application is accessible for the authorized system administrator(s) only.
1.b	What parameters are accessible or modifiable by the professional installer or system integrators? SSID, passphrase, cypher-type and network parameters (such as IP adresses) are configurable by the remote server application, which is accessible for the authorized system administrator(s) only.
1.b(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Put in your text here….
1.b(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.? All input values are checked against its predefined limits. No parameter can exceed its limits.
1.c	What parameters are accessible or modifiable by the end-user? SSID, passphrase, cypher-type and network parameters (such as IP adresses) are configurable by the end-user by using a remote server application, which is accessible for the authorized system administrator(s) only.
1.c(1)	Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? Any transmitted parameter will be validated by the instrument's

	application and will only be accepted if inside of the authorized limits.
1.c(2)	What controls exist so that the user cannot operate the device outside its authorization in the U.S.? Any transmitted parameter will be validated by the instrument's application and will only be accepted if inside of the authorized limits.
1.d	Is the country code factory set? Can it be changed in the UI? The instrument does not have a country code factory set. All parameter ranges per default valid for authorization in US, e.g. only authorized frequency bands are used.
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.? A country code cannot be changed, as it does not exist.
1.e	What are the default parameters when the device is restarted? RF is deactivated. If activating RF only authorized frequency bands are usable.
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. The instrument cannot operate in bridge or mesh mode as it is a passive device.
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?

	n/a (The instrument cannot operate in bridge or mesh mode)
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 device cannot be configured as an access point as it is a passive device.

bnouachc

Digital signiert von bnouachc
DN: cn=bnouachc, c=DE, o=RDS PoC R&D, ou=DV&V, email=charaf.bnouachir@roche.com
Grund: Ich habe dieses Dokument überprüft
Datum: 2023.12.07 14:53:29 +01'00'

Charaf Bnouachir, FPL Design Verification

Roche Diagnostics GmbH

Sandhofer Strasse 1156

D-68305 Mannheim; Telefon +49-621-759-0; Telefax +49-621-759-2890