To whom it may concern

Robert Bosch GmbH
Postfach 10 02 61
31102 Hildesheim
Visitor:
Robert-Bosch-Straße 200
31139 Hildesheim
Phone +49 5121 49-0
www.bosch.com

Thomas Dargel, XC/QMM-VR2.1
Phone +49 5121 49-5599
Thomas.Dargel@de.bosch.com

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES 2024-11-20

SOFTWARE CONFIGURATION DESCRIPTION

FCC ID	2AUXS-MMCSBXNAR
ISED ID	25847-MMCSBXNAR

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. **Answer:** The SW update functionality per USB stick or firmware update over the air (FOTA) is protected according to the Android standard security mechanisms which are checksum & signature checks. This prevents that no unauthorized/manipulated SW will be installed on the device. The SW update functionality per USB stick or firmware update over the air (FOTA) is protected with verification mechanisms based on SHA256 which are checksum & signature checks. This prevents that no unauthorized/manipulated SW will be installed on the device.
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? **Answer:** All Bluetooth and WLAN parameter could be modified with module firmware. It is not possible to install any other software than the production software. Any software change will be assessed according to FCC change police (additional testing of parameters will be carried out when necessary).
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. **Answer:** The SW update packages are verified by SHA256/RSA. Secure Boot signatures checks (SHA256/RSA) are also applied to some executables. Different sets of keys are used for the SW update signing during development and production. The production keys are given access only to specific people who are authorized to have. Linux dm-verity boot mechanism performs a checksum verification during runtime to prevent the execution of unauthorized/manipulated SW.

4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware **Answer:** Linux standard security mechanisms based on SHA/RSA are used to secure SW update functionality.
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? **Answer:** The system does not allow the client and master modes to co-exist i.e., the user is allowed to start either the client or master and this is restricted from UI. In client mode, the system scans and lists the external access points which are available in the legal channels of the current regulatory domain and thereby also restricting the Wi-Fi operations in the channels which are not allowed. When the user starts the master mode, the system picks a legal channel of the current regulatory domain.

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. **Answer:** System starts in World Safe Mode (Channels 1-11 only) or starts with the country code from last power cycle ("last mode"). The system then uses its onboard navigation services or mobile country code (MCC) from telematics control unit (if available) to determine the current location and reconfigures the regulatory domain. Channels 12 to 14 are disabled in any case. The system does not trust the 802.11D information broadcasted from the external access point even during an active connection with it. The end user does not have the possibility of configuring the regulatory domain. By this way it is ensured that the

	system does not violate the regulatory rules of the current geographical location that the system is located.
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. **Answer:** The head unit doesn't support the capability to install third party software. The firmware itself is secured as described above.
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. **Answer:** N/A (Head unit is not a modular device.

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. **Answer:** The possibility for the end user and others is only limited to settings in the HMI i.e., HMI does not allow any configurations which directly affect the FCC approval. Specialists of the OEM can use the vehicle diagnosis interface to set the region.
1.a	What parameters are viewable and configurable by different parties? **Answer:** Region setting by authorized personnel from OEM
1.b	What parameters are accessible or modifiable by the professional installer or system integrators? **Answer:** Region setting by authorized personnel from OEM

1.b(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? **Answer:** Yes
1.b(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.? **Answer:** Head unit maintains country based regulatory settings and changes its current regulatory domain when it detects the device is operated in another country. To ensure that the regulatory settings do not exceed the U.S. settings, all country settings are intersected with U.S. settings in the regulatory database.
1.c	What parameters are accessible or modifiable by the end-user? **Answer:** The end user has no access to any parameters.
1.c(1)	Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? **Answer:** Yes.
1.c(2)	What controls exist so that the user cannot operate the device outside its authorization in the U.S.? **Answer:** Head unit maintains country based regulatory settings and changes its current regulatory domain when it detects the device is operated in another country. To ensure that the regulatory settings do not exceed the U.S. settings, all country settings are intersected with U.S. settings in the regulatory database.
1.d	Is the country code factory set? Can it be changed in the UI? **Answer:** The factory defaults is world safe mode. UI does not provide an option to change the country code. Also there exists a vehicle diagnosis interface for OEM authorized personnel to change the country code. The country code 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.? **Answer:** N/A (see above)
1.e	What are the default parameters when the device is restarted? **Answer:** System starts in World Safe Mode (Channels 1-11 only) or starts with the country code from last power cycle ("last mode"). Channels 12 to 14 are disabled in any case. In case of "last mode", world safe mode will be set after 60 minutes if no geo-location is received from navigation services or from telematics control unit (TCU).
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. **Answer:** N/A no bridge or mesh mode supported by the headunit.
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? **Answer:** The system does not allow the client and master modes to co-exist i.e., the user is allowed to start either the client or master and this is restricted from UI. In client mode, the system scans and lists the external access points which are available in the legal channels of the current regulatory domain and thereby also restricting the Wi-Fi operations in the channels which are not allowed in the current regulatory domain. When the user starts the master mode, the user is allowed to configure SSID, passphrase and the frequency band. The system picks a legal channel from the selected band in the current regulatory domain.
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)) **Answer:** The head unit has only a build in antenna system for Wi-Fi which is used for 2.4 and 5GHz. There is no possibility to exchange the antenna or to plug a different antenna. Power limit settings are identical for station and access point modes.

Yours sincerely

pki, BOSCH, DE, M, A, Markus.Maier

Digital unterschrieben von pki, BOSCH, DE, M, A, Markus.Maier
Datum: 2024.11.20 12:13:05 +01'00'

_____

i.V. Markus Maier
Head of EMC Laboratory