HARMAN
A SAMSUNG COMPANY

Date: Friday, March 5, 2021

to:	from:
Regulatory Certification Body DEKRA Testing and Certification, S.A.U. Parque Tecnológico de Andalucía C/ Severo Ochoa 2 & 6 29590 Campanillas Málaga, España	**HARMAN BECKER AUTOMOTIVE SYSTEMS GMBH,** Becker-Goering-Str. 16; 76307 Karlsbad, Germany

Related to product:

Type of equipment:	Automotive infotainment System
Brand name:	Audi
Model:	SCON2
FCC ID:	T8GSCON2

Software security description per KDB 594280 D02:

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.	SCON2 will be installed within car by OEM customer. Service (as SW updates) will be executed by car service garages or Over-The-Air from OEM customer server. End customer has no possibility to do SW update. Additionally, all SW update packages are signed and the signature is verified on the system before new SW can be installed.
	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 determined by the binary image. The end user cannot modify RF parameters.
	3. Describe in detail the authentication protocols that are in place to ensure that the source of the RF-related software/firmware is valid.	All software is signed by using public-private key signatures. No software is installed without valid signatures. The installed SW is verified on each

	Describe in detail how the RF-related software is protected against modification.	boot using the Secure Boot mechanism which ensures that the SW has not been altered/changed. No port available/open to install any software or do changes on the existing one.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	The SW is checked on each startup using Secure Boot with digital signatures and a fused public key (not changeable). Further parts are integrity protected using dm-verity. The update/installation data of RF parameters is encrypted and secure by the secure SW update process. Changes in the RF parameters at runtime are only done by SW covered by secure boot
	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?	Device is configured as a client. SCON2 will connect to Wi-Fi HeadUnit only. End Customer has no possibility to change configuration file and connect to SCON in other way.
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.	Not possible for 3rd parties to load any software or drivers. System is bind to car and cannot be used outside its regulatory domain. Option is not provided for any third party usage.
	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	Not possible for 3rd parties to load any software or drivers.

	to ensure the devices' underlying RF parameters are unchanged and how the manufacturer verifies the functionality.	
	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 parameters are adjusted during manufacturing process and cannot be changed at later time.
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.	End Customer has no possibility to change configuration from UI. No posibility to change parameters from other level of access .
	a. What parameters are viewable and configurable by different parties?	Device will connect automatic with HeadUnit. No posibility for end user to change parameters
	b. What parameters are accessible or modifiable by the professional installer or system integrators?	Device will connect automatic with HeadUnit. No posibility for end user to change parameters
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	No posibility to change parameters
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Device is just a client. Will use parameters from HeadUnit Hotspot certified.

	c. What parameters are accessible or modifiable by the end-user?	No posibility to change parameters
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	No posibility to change parameters
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	Device is just a client. Will use parameters from HeadUnit Hotspot certified.
	d. Is the country code factory set? Can it be changed in the UI?	No posibility to change parameters
	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	No posibility to change parameters
	e. What are the default parameters when the device is restarted?	Device is just a client. After restart will reconect to HU.
	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 bridge or mesh mode posible
	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?	Device is operating only as client. No posilibity to connect from UI. Device is connecting automaticly to HeadUnit.
	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	Device is operating only as client.

	applicable limits and the proper antenna is used for each mode of operation. (See Section 15.407(a))	

Sincerely,

By:	Simon Voegele	i.V. Simon Voegele
Title:	Regulatory Compliance Expert	
Company:	Harman Becker Automotive Systems GmbH	
Telephone:	+49 7248 71 3667	
e-mail:	simon.voegele@harman.com	

HARMAN AUTOMOTIVE DIVISION
Harman Becker Automotive Systems GmbH
Becker-Göring-Straße 16
76307 Karlsbad, Germany