Software security for UNII Devices

ACTIA Nordic AB

Hammarbacken 41, 19149 Sollentuna, Sweden

To Whom It May Concern:

Product/Model/HVIN: ACUII-06

FCC ID: 2AGKKACUII-06

IC ID: 2 0839-ACUII06

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 product uses embedded WLAN module and LTE module. These embedded modules are tuned in supplier's manufacturing before shipped to ACTIA. It is not possible to change RF parameters by ACTIA's application software. ACTIA makes RF validation testing to check that RF parameters have not been modified during manufacturing (e.g. by mounting wrong components). ACUII-06 is factory fitted in vehicles and is not accessible for an end user. In the vehicles there is a configuration file which controls following WLAN parameters: - WLAN output power. Can be set to maximum power used in module's certification, or lower. - WLAN channels to be used. Only ACTIA can make this configuration file. File can only be downloaded with specific workshop tools in car workshops. Authentication and security access is used to check that only approved

	files can be downloaded.
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? In the vehicles there is a configuration file which controls following WLAN parameters: - WLAN output power. Can be set to maximum power used in module's certification, or lower. - WLAN channels to be used (same or fewer channels than used in module manufacturer's certification).
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. Only ACTIA can make new software packages. Authentication and security access is used to check that only approved files can be downloaded
4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. The software/firmware can only be changed through software download protected behind Security Access (service 0x27) of the UDS (ISO-14229) standard using an ECU unique key. On top of this the ACUII-06 also has a proprietary security mechanism to only accept binary software packages signed and encrypted by ACTIA.
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 can be master or client, but the parameters/bands can not be controlled by end user. Device can act as Master, using WLAN channels specified in configuration file which only allows compliant channels. Device can act in Client mode. Using passive scanning. Channels are limited to only allowed channels.
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.
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. Third party SW not possible.
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. Authentication of SW and security access is used to check that only approved files can be downloaded.
	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. There is no UI available for RF parameters.
1.a	What parameters are viewable and configurable by different parties? Only ACTIA can provide a new configuration file. This file can only be downloaded with specific workshop tools in car workshop. Authentication and security access is used to check that only approved files can be downloaded.
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? N/A.
1.b(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.?

	User can not control/modify any parameters.
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? N/A.
1.c(2)	What controls exist so that the user cannot operate the device outside its authorization in the U.S.? User can not control/modify any parameters.
1.d	Is the country code factory set? Can it be changed in the UI? The product variant is specific for USA and Canada.
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.? N/A.
1.e	What are the default parameters when the device is restarted? Modem will use “automatic operator selection”. WLAN will use the last select mode (AP/STA), Radio parameters can not be changed from the default.
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? Device can be master or client, but the parameters/bands can not be controlled by end user. Device can act as Master, using WLAN channels specified in configuration file which only allows compliant channels. Device can act in Client mode. Using passive scanning. Channels are limited to only allowed channels.
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)) Not possible.

<SIGNATURE>

Nicklas Andersson

System Engineer

ACTIA Nordic AB

Hammarbacken 4a

191 49 Sollentuna

Sweden

+46 8 4747200