Software security for UNII Devices

INGENICO

9 av de la Gare Rovaltain, Alixan, FRANCE

To Whom It May Concern:

Product/Model/HVIN: ISMP4 CL/WIFI/BT

FCC ID: XKB-ISMP4CLWIBT

IC ID: 2586D-ISMP4CLWIBT

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

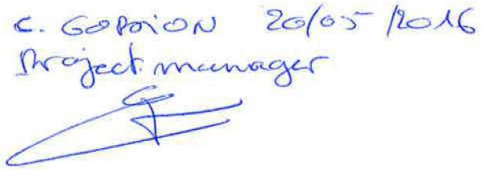
SOFTWARE CONFIGURATION DESCRIPTION	
General Description	
1	Describe how any software/firmware updates for elements than can affect the device's RF parameters will be obtained, downloaded, validated and installed. For software that is accessed through manufacturer's website or device's management system, describe the different levels of security as appropriate. Software/Firmware can be updated by the secured LLT or IngeEstate Ingenico process by qualified professional people only. The software/Firmware, i.e. driver for INGENICO, can only be generated by INGENICO. That driver is encrypted (banking secure process) and can only be downloaded on INGENICO's terminals. Before diffusion, the driver is controlled (RF performances) and validated internally in INGENICO's radio laboratories. The driver is downloaded into INGENICO terminals through a secure program (LLT) or the IngeEstate remote download process

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 can be changed by a SW/FW change. The SW/FW are SIGNED and fully secured and control by Ingenico. RF parameters cannot be changed by end user.
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. RF parameters can be change with a new binary SIGNED compiled by R&D only. An upload process will use the LLT or IngeEstate Ingenico protocol. These protocols are fully secured with authentication, traceability and encryption. Protocols are proprietary and confidential.
4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. Encryptions are proprietary and confidential.
5	For a device that can be configured as a master and client (with active orpassive 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? Client only
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. A third party cannot operate in violation 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. A third party cannot change software or firmware. The only way to update SW or FW is to use LLT or IngeEstate Ingenico process authorized and controlled by Ingenico company.
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. Not modular device
	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. Only one WIFI UI.
1.a	What parameters are viewable and configurable by different parties? WIFI Menu allow : - AP Scan - Authentication protocol setting (with user/password, certificate, ip setting) - ON/OFF General menu - Download
1.b	What parameters are accessible or modifiable by the professional installer or system integrators? WIFI Menu - AP Scan - Authentication protocol setting (with user/password, certificate, ip setting) - ON/OFF General menu - Download
1.b(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Authentication protocol setting are controlled as requested by Wifi alliance. Download menu allow to download SIGNED component control by Ingenico secure process
1.b(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.? None

1.c	What parameters are accessible or modifiable by the end-user? Wi WIFI Menu - AP Scan - Authentication protocol setting (with user/password, certificate, ip setting) - ON/OFF General menu - Download
1.c(1)	Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? Authentication protocol setting are controlled as requested by Wifi alliance. Download menu allow to download SIGNED components control by Ingenico secure process.
1.c(2)	What controls exist so that the user cannot operate the device outside its authorization in the U.S.? None
1.d	Is the country code factory set? Can it be changed in the UI? Automatic setting from the AP country code. No UI for country code
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.? does not exist
1.e	What are the default parameters when the device is restarted? Last configuration
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, no mesh
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? Client only
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)) one antenna only check on manufacturing site.



INGENICO

9 av de la Gare Rovaltain, Alixan, FRANCE