DECLARATION OF U-NII INFORMATIONS

Curtis-Straus LLC
One Distribution Center Circle #1
Littleton, MA 01460
USA

December 1, 2016

FCCID:	**XKB-D5000CLWIBT**
IC:	**2586D-D5000CLWIBT**
Model:	**Desk/5000 CL/Eth/Mod/Wifi/BT**

Gentlemen,

We, **INGENICO**, declare following information to provide compliance to:

- ✓ FCC PART 15.407
- ✓ KDB 594280 D02 U-NII Device Security
- ✓ KDB 905462 D03 Client Without DFS New Rules
- ✓ RSS 247

Regards,

Responsible party: **Jean-Baptiste PALISSE**
Title: **HW Norms&Marking Manager**
Signature:

U-NII CLIENT DEVICES WITHOUT RADAR DETECTION CAPABILITY

We, **INGENICO, declare** that the device does not support any non-US channels in all the operational mode(s), like Ad-Hoc…
The client software and associated drivers will not initiate any transmission on DFS frequencies without initiation by a master. This includes restriction on transmissions for beacons and support for Ad-Hoc Peer-to-Peer modes.

PART 15.407 (C) AND RSS-247 SECTION 6.4 (2) REQUIREMENT

We, **INGENICO**, declares that the device automatically discontinue transmission in the 5GHz frequency band in case of either absence of information to transmit or operational failure according to Part 15.407 (c) and RSS-247 section 6.4 (2).

PART 15.407 (g) REQUIREMENT

We, **INGENICO**, declares that the frequency stability is maintained within, the band of operation under all conditions of normal operation according to Part 15.407 (g).

For more details about following points, see KDB 594280 D02 U-NII Device Security v01r03

SOFTWARE SECURITY DESCRIPTION		
General Description	Point 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.
	Response	Software/Firmware can be updated by the secured LLT (Loading Local Tool) 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 terminals. Before diffusing, the driver is controlled (RF performances) and validated internally in Ingenico terminals through a secure program (LLT) or the IngeEstate remote download process
	Point 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?
	Response	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 an end user.
	Point 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.
	Response	RF parameters can be changed with a new binary SIGNED compiled by R&D only. An upload process will use the LLT or IngeEstate Ingenico protocol. Those protocols are fully secured with authentication, traceability and encryption. Protocols are proprietary and confidential.
	Point 4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
	Response	Encryptions are proprietary and confidential.
	Point 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?
	Response	Client only.

SOFTWARE SECURITY DESCRIPTION		
Third-Party Access Control	Point 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.
	Response	A third party cannot operate in violation of the device's authorization if activated in the US
	Point 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.
	Response	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.
	Point 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.*
	Response	Not modular

* Note that Certified Transmitter Modules must have sufficient level of security to ensure that when integrated into a permissible host the device's RF parameters are not modified outside those approved in the grant of authorization. (See, KDB Publication 99639). This requirement includes any driver software related to RF output that may be installed in the host, as well as, any third-party software that may be permitted to control the module. A full description of the process for managing this should be included in the filing.

In addition to the general security consideration, for devices which have “User Interfaces” (UI) to configure the device in a manner that may impact the operational RF parameters, the following questions shall be answered by the applicant and the information included in the operational description.
The description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 Publication D01**.

SOFTWARE CONFIGURATION DESCRIPTION		
USER CONFIGURATION GUIDE	Point 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.
	Response	UI proposes Wi-Fi services.
	Point 1a	What parameters are viewable and configurable by different parties? ***
	Response	Services proposed : - AP scan - Authentication - On/Off - Roaming - IP configuration - Protocol settings - Ping - My Networks (*Profiles recorded*)
	Point 1b	What parameters are accessible or modifiable by the professional installer or system integrators?
	Response	Services proposed : - AP scan - Authentication - On/Off - Roaming - IP configuration - Protocol settings - Ping My Networks (*Profiles recorded*) + Country code can be changed in factory
	Point 1b(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	Response	Authentication protocol settings are controlled as requested by Wi-Fi Alliance.
	Point 1b(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	Response	- Country code control
	Point 1c	What parameters are accessible or modifiable by the end-user?

SOFTWARE CONFIGURATION DESCRIPTION		
	Response	Services proposed : - AP scan - Authentication - On/Off - Roaming - IP configuration - Protocol settings - Ping My Networks (*Profiles recorded*)
	Point 1c (1)	Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
	Response	Authentication protocol settings are controlled as requested by Wi-Fi Alliance.
	Point 1c (2)	What controls exist so that the user cannot operate the device outside its authorization in the U.S.?
	Response	Country code control
	Point 1d	Is the country code factory set? Can it be changed in the UI?
	Response	Yes, it is factory set No it cannot be changed in the UI
	Point 1d (1)	If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
	Response	It does not exist
	Point 1e	What are the default parameters when the device is restarted?
	Response	Last configuration saved
	Point 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.

SOFTWARE CONFIGURATION DESCRIPTION		
	Response	No Bridge, no mesh
	Point 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?
	Response	Client only.
	Point 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))
	Response	Not applicable. The terminal cannot be configured inn access point.

** See KDB Publication 594280 D01Software Configuration Control for Devices. The document provides guidance for devices permitting device configurations and limitations on configuration parameters accessible to the third-parties in which the software is designed or expected to be modified by a party other than the manufacturer and would affect the RF parameters of the Software Defined Radio (SDR).
*** The specific parameters of interest for this purpose are those that may impact the compliance of the device (which would be those parameters determining the RF output of the device). These typically include frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings which indirectly programs the operational parameters.