Software Security Declaration

Product: Wireless Lan Module
Model name: NFA455
FCC ID: A3LNFA455

This device is fully compliant with the requirement of KDB 594280D02 version to V01r01.

SOFTWARE SECURITY DESCRIPTION	
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed.
	All Software downloads are supplied and controlled by the host device manufacturer. Download is implemented via a secure server.
	2. Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited, such that, it will not exceed the authorized parameters?
	Centre Frequencies of channels, channel bandwidth, modulations, active or passive scanning and transmit power levels are defined in software. Hardware specific configuration data is stored in non-volatile memory which limits frequency and transmit power levels to U.S. compliant values.
	3. Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details; if not, explain how the software is secured from modification.
	The software image is installed at time of manufacture of the module. The correct embedded software is verified and installed by the module manufacturer. The signature validation procedure in 4) below is used to validate the authenticity of the image using a public key or hash of the public key stored in the module's non-volatile memory.
	4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.
	A hash on the firmware binary is computed at the CASS server using SHA256 hashing algorithm. The hash is then secured using the private key using RSA-PSS algorithm. The secured hash is downloaded from the host to the target along with the firmware binary. After firmware binary download from the host, the target uses the public key to decrypt the hash that is sent & computes the hash on the firmware binary & compares them for authentication. If the hash does not match the firmware binary is discarded from target memory.
	5. Describe, if any, encryption methods used.
	RSA-PSS for encrypting/decrypting the hash.SHA256 for computing the hash.
	6. 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?
	Software limits operation to passive only and No Master modes (WiFi Direct, SoftAP, etc) in radar channels. This configuration cannot be changed by end user or installer.
SOFTWARE SECURITY DESCRIPTION	
Third Party Access Control	1. How are unauthorized software/firmware changes prevented?
	The verification/authentication features described in previous section prevents unauthorized software changes.
	2. Is it possible for third parties to load device drivers that could modify the RF parameters, country of operation or other parameters which impact device
	Embedded software is protected via the measures explained in the previous section. Distributions of host operating software are digitally signed with a private key and matching public key.
	3. Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification

	Country domain is set in non-volatile memory during manufacture. The software and user interface does not provide any option to choose a country of operation.
	4. What prevents third parties from loading non-US versions of the software/firmware on the device?
	Embedded software is protected via the same measures explained in previous section.
	5. For modular devices, describe how authentication is achieved when used with different hosts.
	The module is not available for sale or installation outside of company licensing agreements. Modules are always installed in host systems in a factory by end integrators responsible for loading authorized software.
SOFTWARE CONFIGURATION DESCRIPTION	
User Configuration Guide	1. To whom is the UI accessible? (Professional installer, end user, other.)
	End User.
	a) What parameters are viewable to the professional installer/end-user?
	Misc. device status information is viewable by the end user (channel of operation, connection status, etc).
	b) What parameters are accessible or modifiable to the professional installer?
	General configuration options are available.Regulatory related parameters are not modifiable.
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	Configuration of channel/frequency, modulation type and transmit power are not modifiable by installer or user.
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	The user interface does not allow access to parameters affecting regulatory compliance.
	c) What configuration options are available to the end-user?
	Misc. device configuration options. Regulatory related parameters are not accessible.
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	There are no configuration options available to the installer or end user that can impact regulatory compliance.
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	Regulatory Domain & country code is stored in nonvolatile memory and cannot be changed in the user interface by installer or end user. This is set to U.S.operation.
	d) Is the country code factory set? Can it be changed in the UI?
	Regulatory Domain & country code is stored in nonvolatile memory and cannot be changed in the user interface by installer or end user.
	i) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
	Regulatory Domain & country code is stored in nonvolatile memory and cannot be changed in the user interface by installer or end user. This is set to U.S.operation.
	e) What are the default parameters when the device is restarted?
	Regulatory Domain & country code is stored in nonvolatile memory and cannot be changed in the user interface by installer or end user. This is set to U.S.operation.
	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.
	Not supported.
	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?
	No user controls or user interface option to change master/client operation.

	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))
	The device does not support these modes/features.

<Attachment> “Professional Installation letter”

March 24, 2015

To whom it may concern,

Professional Install Justification:

Samsung electronics, the supplier of the device, declares that the **NFA455** units are not sold or marketed to the general public and are only sold to wireless internet service providers and requires a professional installation.

The professional installers only shall have the account information which let them access to the configuration UI for the device. The account information for the professional installers shall not be revealed to end user.

_____

NAME : ChanHo Youn
TITLE : Manager
E-MAIL: jjano.youn@samsung.com
TEL: +1-973-808-6362
Samsung Electronics Co., Ltd.
19 Chapin Rd. Building D Pine Brook NJ 07058