NOKIA

NOKIA INC.
Joensuunkatu 7
FIN-24100 SALO
FINLAND
Tel. +358 7180 08000
Fax. +358 7180 44695
February 11, 2013

Federal Communications Commission,
Authorization & Evaluation Division,
7435 Oakland Mills Road,
Columbia, MD. 21046

Attention: Equipment Authorization Branch

Software upgrade for devices deployed in the field.

With this application we are asking permission to upgrade devices FCC ID:PYAA in the field with a software upgrade. We are upgrading devices with LTE band 2 (UL 1850-1910 MHz; DL 1930-1990 MHz) and band 5 (UL 824-849 MHz; DL 869-894 MHz). These bands are approved for use in the initial FCC application. We are basing this PC2 application to the KDB 1788919.

Brief description of the arrangement between parties:

Nokia owns the product configuration.
Nokia is building the product configuration. Deliveries from hardware and software providers are used. All software is delivered to Nokia. Nokia and Microsoft (OS vendor) are responsible for packaging and delivery of the software.
Nokia delivers the original product configuration, while updates hereto are distributed to the end user by Microsoft, using their software update servers.
Nokia certified Customer support providers can also update the software on a device, but they cannot use any software configuration that has not been created by Nokia.

Software control process used by the parties to ensure that reasonable safeguards are in place to ensure that the device cannot be modified by unauthorized parties:

The software update to enable LTE function for this application will only enable the specific LTE band which is already covered by the original grant. The software change needed to enable the originally approved LTE band does only change one pre-existing setting in non-volatile memory controlled by Nokia.
There are no changes affecting power, emission and designators, SAR or frequency bands outside what the grant already lists.
Third parties do not have any ability to configure or operate transmitters in any way that violates the approved certification.

NOKIA

Software is delivered as part of the manufactured product delivered from the factory. The device is also calibrated against all the bands the hardware supports.
As part of the manufacturing process, RF parameters are tuned and compliancy is verified. This is accomplished by instructing the phone to transmit on specific frequencies and power levels and measuring the results with external equipment. The test is re-run iteratively until the device is verified to be within tolerance. The proper correction values are computed and downloaded to the phone. The calibration values are protected, so they cannot be modified by an unauthorized party.
The protection mechanism relies on the Secure Boot concept and the fact that all software and settings must be digitally signed by secure servers. This will ensure the authenticity and the integrity of all software running on the device. The device will refuse to install or run any package that has not been properly signed.
Signing is a cryptographic process that prevents anyone but the software owner of the package to update it. Packages are tracked by increasing packaging version numbers. There are multiple levels of trust and also OEM software modules cannot execute beyond their granted authority level. All third party software applications must be signed by Microsoft and are only granted the minimal level of access needed and approved by Microsoft.

Software updates are originating from Nokia, hardware/software vendors and Microsoft (OS vendor). Nokia collects internal updates as well as updates from other parties (hardware and software vendors). Any updates are assessed for certification impact and if any further permissive change is applicable. Software is only released to the market after full assessment is completed and new approvals are in place if required. Nokia has an internal process that requires certification approval before software is released to third parties.
Only Nokia can deliver updates that can modify the way the transmitter operates.

The update packages collected by Nokia are digitally signed and delivered to Microsoft. Microsoft will add own updates and verify the update package. When the planned update has been verified, the final update package is created and digitally signed.
The last step is to load the update packages to the update servers, so the end user will get the updates.

Attestation from the grantee:

Nokia declares that all software releases provided to the end user will be fully assessed and compliant with the FCC requirements and will ensure that FCC approvals will be in place before software is released to the market.

NOKIA CORPORATION

Digitally signed by tero.m.lehtinen@nokia.com
Date: 2013.02.11 09:53:30 +02'00'

Tero Lehtinen
Product Certification Officer
Salo