Compliance to KDB 594280 D01 and D02 for FCC ID: XOX-Z400

Revision: 1.0

Date: March 16th, 2015

Table of Contents

1 Introduction

This document will provide information pertaining to compliance to KDB 594280 D01 and D02 for the Ziosk Z-400 device FCC ID: XOX-Z400.

2 Definitions, Acronyms & Abbreviations

Android: a mobile OS based on the Linux kernel and currently developed by Google

KDB: Knowledge Database

OS: Operating System

OTA: Over-The-Air

UI: User interface

U-NII: Unlicensed National Information Infrastructure

WLAN: Wireless Local Area Network

3 References

KDB 594280 D01 and D02

4 Compliance to New Rules for U-NII Devices

Authorization to operate the transmitter is being sought under the new rules for U-NII devices operating under Part 15. All testing has been performed in accordance with the requirements for a client device (without radar detection). Additionally, this section describes the software characteristics and procedures followed to ensure compliance under the new rules as set forth in KDB 594280 D01 and D02 relating to software configuration control and device security.

Based on its features and hardware capabilities, the Ziosk is similar to a consumer Android-based tablet. But it has a custom UI that limits the user interaction to only those applications that are enabled on the device, such as infotainment and payment. There are no user configurable controls or screens enabled on the device which would allow a user (or any third party) access to settings that would affect the operation of the radio and cause it to transmit outside the parameters of the authorization. The devices come pre-configured with this UI software from the factory; there are no provisions (and none needed) for professional installers or service personnel to access or configure any of the radio parameters.

Generally speaking, the software that controls the WLAN radio module (and more specifically, the firmware loaded on the module itself) is not expected to be updated after FCC testing and certification has been done. However, the capability to do this does exist and the following

paragraphs describe the procedures and security measures taken to ensure the validity of any updates and prevent any unauthorized changes from taking place.

Operating system, driver, and firmware updates are downloaded from our company server to our local server within the restaurant over an encrypted VPN connection. From there, each Ziosk in the restaurant downloads the software from the local server and installs it using the standard Android authentication mechanism for installing Over-The-Air updates. OTA packages are code signed, with the signature applied over the whole file to prevent any individual file being manipulated by a man-in-the-middle attack. No 3rd-party certificates are allowed.

Code signing must be done with a standard RSA encrypted private key contained in a standard X.509 certificate. This corresponds to a public key built into our device. This key is generally the same for all Ziosks, but it can be changed in case of a breach.

A SHA1 checksum for the Over-The-Air update package is used as a way to detect corruption during the download or storage to the device. Once verified and unpacked, the OTA package is then checked against a known checksum to detect any errors in the decompression.

The private key for an OTA update is kept in secure storage with access limited to two employees specifically designated as secure storage specialists. The key is only given to other employees on an as-needed basis; we track who has this key, and it can be changed during each regular maintenance release of our software as employees leave the company. The public key is stored in source-control with access limited to the operating system team. When an employee leaves the company, this access is revoked immediately, and in the next maintenance release it will be changed.

In each Ziosk restaurant environment, the wireless network is protected by WPA2-PSK encryption to prevent rogue update servers. The password for the wireless network is automatically generated and stored on physical access cards that are used to configure the Ziosk in the store. It is never transmitted electronically. These physical access cards are tracked and are different for each store.

As mentioned previously, the user interface to the device is completely custom and does not provide the ability to change or modify the device configuration in any way, as a normal consumer tablet might. There does not exist (outside of the factory) any mechanism to allow the installation of third party software or drivers – while these abilities do exist in the Android OS, they are not exposed in the Ziosk UI. This is largely necessary due to the level of security needed in order to accept payment on the device, but these same measures serve to protect the operational integrity of the WLAN radio as well.