Ztronicx Microsystem Inc.
Simon Fraser Univeristy
Burnaby, BC V5A 1S6
ensc440-whizkids@sfu.ca

October 18th, 2006

Dr. Andrew Rawicz
School of Engineering Science
Simon Fraser University
Burnaby, BC
V5A 1S6

Re: ENSC440 Functional Specification for VirtualKey
(Bluetooth Access Control System)

Dear Dr. Rawicz,

The following attached document contains Ztronicx Microsystems' Functional Specification for VirtualKey (a Bluetooth Access Control System). The purpose of VirtualKey is to lock / disable any home appliances while parents / guardians are out of sight and to give temporary access to guests visiting the house via Bluetooth wireless link by a cell phone.

The attached functional specification includes the following information:

- Introduction to the VirtualKey product
- System Overview
- System Software on Cellular Phones
- System Hardware on Appliances
- System Test Plans
- Conclusion
- Glossary

This Functional Specification states what VirtualKey will be able to do when the first version is completed in December 2006. This report attempts to cover these issues without going into comprehensive details about how it is to be implemented. If you have any questions or concerns about VirtualKey, you are welcomed to contact Ztronicx Microsystem by emails at ensc440-whizkids@sfu.ca.

Sincerely,

Shahin Teymouri

Shahin Teymouri
President and CEO
Ztronicx Microsystem

Enclosure: Functional Specification for VirtualKey

Virtual Key

Ztronicx Microsystems

Functional Specification for *VirtualKey*

Bluetooth Access Control System for Home Appliances

Project Team: Halim Soetanto
May (Mei-Yi) Liu
Rick Liu
Shahin Teymouri

Contact Person: Shahin Teymouri
ensc440-whizkids@sfu.ca

Submitted to: Andrew Rawicz – ENSC 440
Steve Whitmore – ENSC 305
School of Engineering Science
Simon Fraser University

Issued Date: October 19, 2006

Revision: 1.0

Ztronicx Microsystem Inc.
Simon Fraser Univeristy
Burnaby, BC V5A 1S6
ensc440-whizkids@sfu.ca

Executive Summary

There have been lots of cases where problems occur at home while an individual is away such as theft and fire or gas explosion accidents. VirtualKey wireless access control system targets on any unattended or invalid access of home appliances and doors. Adults, especially parents, can prevent their kids from playing with hazardous machines or devices and also if they have caregiver or guests, they could easily give them the access to any door or appliance. The elderly, small children and dementia patients will be safe at home by not triggering any unintentional accidents. VirtualKey allows users to fully control lock/unlock and enabling/disabling features over wireless communication. It achieves these goals by a small plug and play module that can be connected to the electrical outlet.

Development process of VirtualKey, a wireless access control over home appliances, is divided into two phases. During the first phase, we will be concentrating on proof of concept together with a working prototype which includes the following features:

1. Enable/Disable of home appliances which is determined by detecting the presence of cellphone within range.
2. Provide interface for user to arrange a list of individuals that have access permission.
3. Encryption and pass-code protection.

Upon the successful completion of conceptual working prototype in November, we will extend the functionality of VirtualKey to control lock and unlock behaviour of house doors.

Ztronicx Microsystem Inc.
Simon Fraser Univeristy
Burnaby, BC V5A 1S6
ensc440-whizkids@sfu.ca

Table of Contents

Ztronicx Microsystem Inc.
Simon Fraser Univeristy
Burnaby, BC V5A 1S6
ensc440-whizkids@sfu.ca

List Of Figures

1. Introduction

VirtualKey is a system that eliminates carrying many keys or access cards around to open for instance your house, office, or your car door. VirtualKey also does another function: to disable dangerous appliances in your house when you are not around so that your children will not be able to use them. These two functions of VirtualKey system, acting as a key to all your doors and enabling-disabling the appliances, are all integrated into one simple device which you can easy install around your house.

VirtualKey has two parts: Java-based software installed on your cellular phone and a hardware module installed behind your appliances or inside your doors. The software installed on your cellular phone will have a user interface that can send different pass codes to the hardware module over a short range wireless system that comes with the cellular phone. The wireless system can use Infrared, Wi-Fi, WiMAX or Bluetooth technology. In this current VirtualKey System, we are concentrating on Bluetooth wireless for the phone-to-module communication. The pass code will travel from the cell phone to the VirtualKey hardware module over a wireless signal. The VirtualKey hardware module can then verify the pass code and activate the door or the appliances.

A working model of VirtualKey system will be ready by December 15, 2006 for demo purpose.

1.2 Scope

This document describes the functional requirements that must be met for the VirtualKey access control system. This is the current functional specification we are planning to implement for our first release. As we develop the VirtualKey system for the demo model in December, we might change some minor aspects of this functional specification for further improvement. However the foundation of this functional specification will not change.

1.3 Intended Audience

Design engineers will use this document as the foundation for building the Virtual Key system.

Project managers will use this document to measure the performance, development objectives and to see if this project is following the required design.

Marketing team will use this document to create the initial advertisement and promotional content.

2. System Overview

In this section we will explain the system overview of VirtualKey System. Figure 1 shows the high level or basic overview on how the VirtualKey works. Bluetooth is shown as an example for the wireless connection.

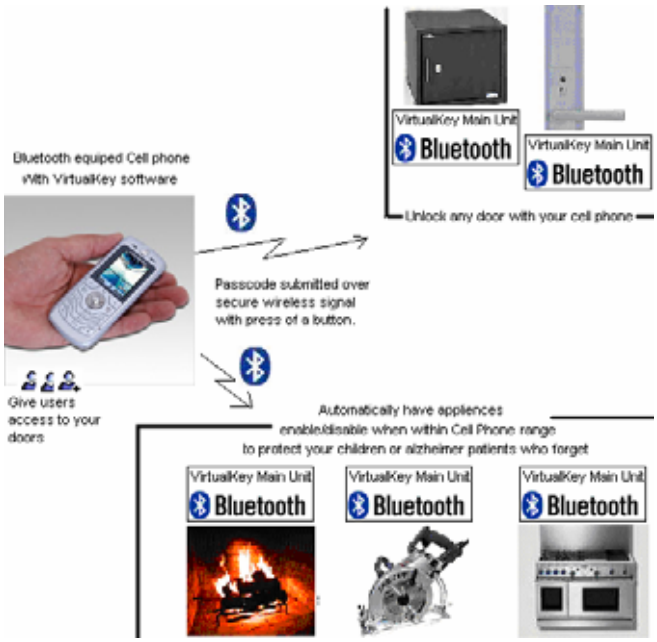

Figure1: Basic diagram for VirtualKey System

Figure 2 shows a more detailed overview of the VirtualKey system. This diagram shows that the list of the pass codes is stored on the cellular phone and another fixed code is stored on the VirtualKey hardware modules. If the pass code transmitted from the phone to the VirtualKey hardware module matches the one on the hardware module, the VirtualKey hardware module will activate the device it is connected to. The device can be an appliance or a door lock actuator.

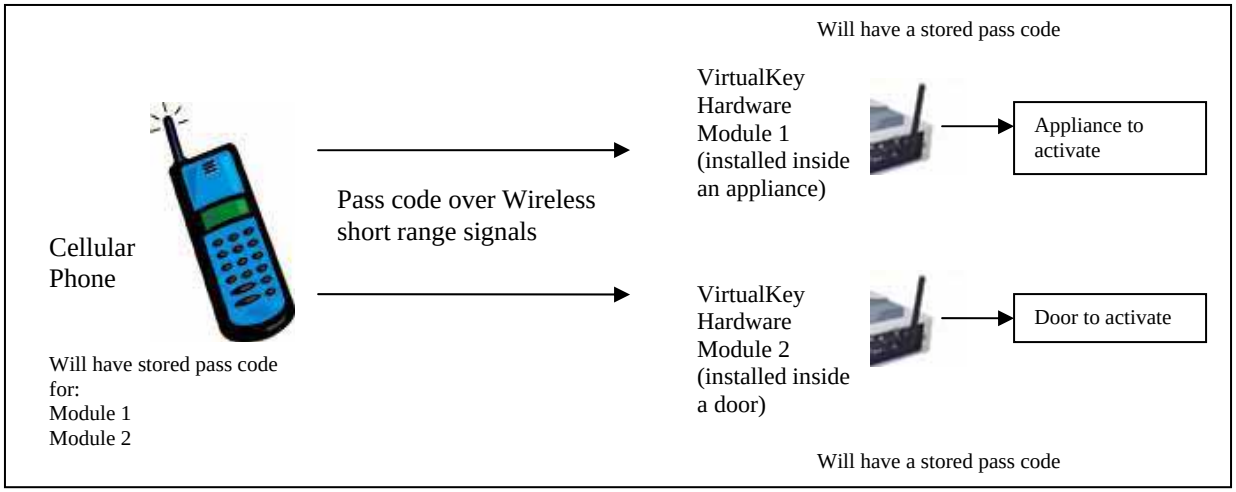

Figure 2: A Detailed Diagram for VirtualKey System

3. VirtualKey Software Application

Figure 3 shows a basic flowchart for the VirtualKey software residing on the cell phone.

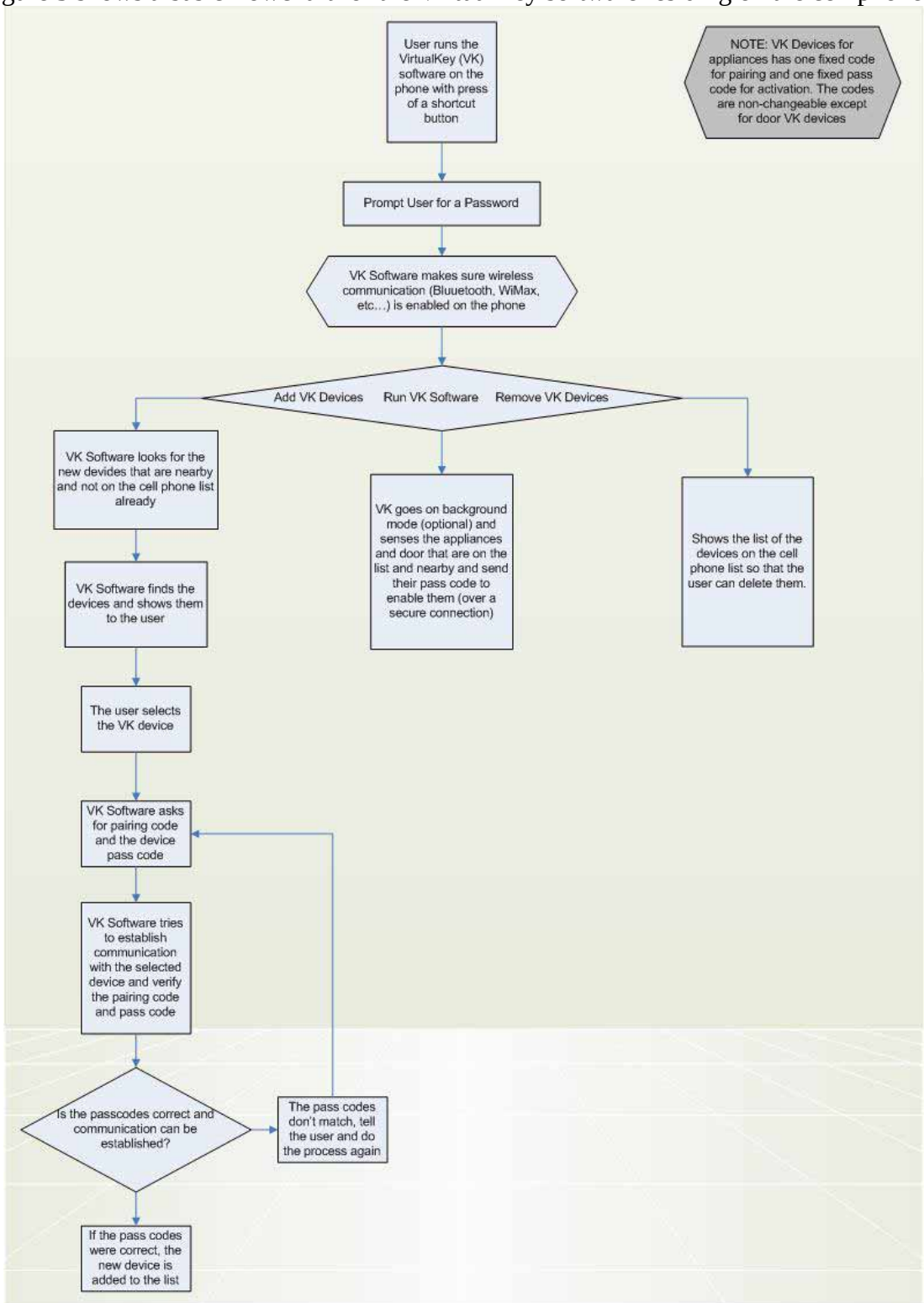

Figure 3: VirtualKey Software Flowchart

4. Functional Specifications for VirtualKey Software

Functional requirements for VirtualKey cellular phone software application are as follow:

1. VirtualKey software application can be downloaded from internet and compatible for all supported cell phone.
2. VirtualKey software encrypts the file that contains the pass code (Nice-to-have feature).
3. VirtualKey software application communicates wirelessly with hardware modules.
4. When VirtualKey software application is launched, it activates wireless connection automatically.
5. VirtualKey software application can pair-up with hardware modules after user enters a password.
6. VirtualKey software application can add/delete list of paired hardware modules.
7. VirtualKey software application can run in the background.
8. Wireless communication between VirtualKey software application and the hardware modules are done over a secured connection (Nice-to-have feature).
9. VirtualKey software application supports on-device user manual for a guide on how to use VirtualKey application.

System Security
The system should provide a secured wireless data link between cell phones and devices. On Physical layer, connection should define random number generation, key management, encryption, authentication, and algorithm for authentication and key generation. On Data Link layer, the system should define the link setup and control between devices, including the security procedures. On Application layer, the system should define how devices are connected to each other and access services for basic interoperability, as well as security models and user interface. [1]

On the software side, the language should strictly define that all primitive data types are of a specific size, and independent of the machine architecture. Second, pointer arithmetic and forging access to objects cannot be done. Third, the language provides array-bound checking and also ensures that casting one object to another is a legal operation. Therefore, an attempt to index an out-of-bound item of an array will throw an exception. During runtime, the software should provide the necessary features to ensure that the system is not subverted by invalid code. Finally, the language could guarantee that the software could be run securely in a closed environment achieved by eliminating features which would pose security. [2]

5. VirtualKey Hardware Modules

Figure 4 shows a detail view of the VirtualKey hardware module, and how the components are connected.

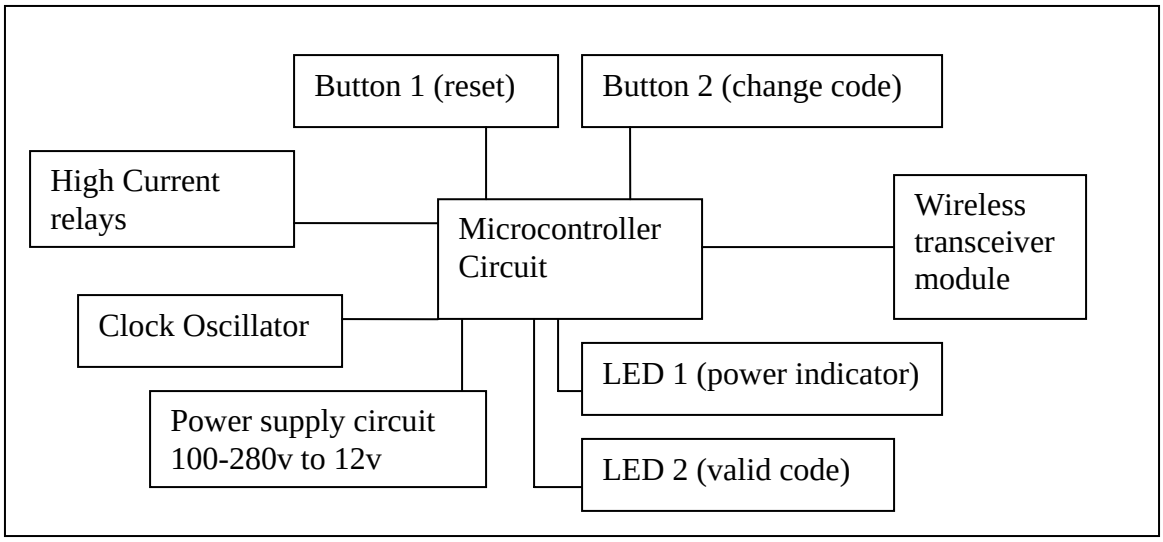

Figure 4: A Detailed Circuit Diagram for VirtualKey Hardware Module

6. Functional Specifications for VirtualKey Hardware Modules

The following is the full specification of the VirtualKey Hardware:

1. VirtualKey hardware modules must be able to fully operate in room temperature and outdoor temperature for the country they have been designed for.
2. VirtualKey hardware modules must tolerate the humidity and pressure of room temperature as well as outdoor environment.
3. VirtualKey hardware modules operate without emitting extra RFI radiation and are sealed inside a metal box.
4. VirtualKey hardware module's antenna is outside of the box.
5. The size of VirtualKey hardware module should be ultra compact, fully integrated inside doors and fit into regular electrical plug.
6. VirtualKey must not give any output voltages that are accessible by the user.
7. For security purposes, if a user enters wrong password for a certain number of times to access a hardware module, then the hardware will disable the wireless transceiver for a period of 15 minutes.
8. VirtualKey hardware will have an adjustable knob that can specify the amount of time a device should deactivate itself after the wireless connection is undetected (Nice-to-have feature).

7. Door and Appliance Module Difference

The hardware door modules of VirtualKey system will be similar to the appliances module except one minor difference: the door modules will have changeable pass codes and they can store up to 10 pass codes for difference people. The pass code on the appliance modules will be fixed.

8. Test Plan

The VirtualKey system can be fully tested with a wireless capable cell phone. The VirtualKey software application will be uploaded-able into a cellular phone. It can then add the hardware modules that are in near proximity to its internal list. After the hardware modules have been added to the list, the cellular phone can send the pass codes to the right module to activate them. This system can be fully demonstrated. There is no need to have an appliance ready. A desk lamp can be used as an appliance. As for the door unlocking, a door actuator can be installed in a nearby door for demonstration. Both can be done in any room or environment.

We are also planning to test the appliance module in an environment where kids as well as Dementia patients are available to see how our module will disable the dangerous appliances when a caregiver is not around.

9. Conclusion

This document dictates the functional specification for both a VirtualKey hardware and software. We are planning to have a very basic working model by beginning of November and the remaining functionality fully integrated by beginning of December. A demo model will be available by middle of December and we will follow the test plan for demonstration.

10. Glossary

RFI: Radio Frequency Interference

Physical Layer:
The services in the OSI protocol stack (layer 1) that provide the transmission of bits over the network medium. This level refers to network hardware, physical cabling or a wireless electromagnetic connection. It also deals with electrical specifications, collision control and other low-level functions.

Data Link layer:
The data link layer is responsible for encoding bits into packets prior to transmission and then decoding the packets back into bits at the destination. Bits are the most basic unit of information in computing and communications. The data link layer is also responsible for logical link control, media access control, hardware addressing, error detection and handling and defining physical layer standards. It provides reliable data transfer by transmitting packets with the necessary synchronization, error control and flow control.

Application layer:
This layer interfaces directly to and performs common application services for the application processes; it also issues requests to the Presentation Layer. The common application services provide semantic conversion between associated application processes.

Encryption:
Encryption means the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

Authentication:
The process of identifying an individual usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

11. Reference

[1] Bluetooth Security http://www.niksula.hut.fi/~jiitv/bluesec.html
2000-05-25
Juha T. Vainio
Department of Computer Science and Engineering
Helsinki University of Technology

[2] Bluetooth SIG http://www.bluetooth.com/
WWW page of the Bluetooth Special Interest Group

[3] Bluetooth.net http://www.bluetooth.net/
More general information about Bluetooth

[4] Java Security http://developers.sun.com/techtopics/mobility/midp/articles/security/
Wireless Security Implementation provided by Java Language