# An Interoperable Authentication System using ZigBee-enabled Tiny Portable Device and PKI

Ki Woong Park, Hyun Jin Choi, and Kyu Ho Park
*Computer Engineering Research Lab.*
*Department of Electrical Engineering and Computer Science*
*Korea Advanced Institute of Science and Technology*
**woongbak@core.kaist.ac.kr, hjchoi@core.kaist.ac.kr, and kpark@ee.kaist.ac.kr**

## Abstract

*Conventional authentication systems especially in a ubiquitous environment do not consider interoperability among different organizations. Therefore, carrying multiple security cards is inevitable for incompatible authentications. In this paper we propose a flexible, scalable, interoperable and usable authentication system using a ZigBee-enabled tiny portable device. It is specialized for the ubiquitous computing environments. In our authentication system, public key infrastructure (PKI) is used for interoperability and scalability. The noble security mechanism using PKI is also proposed. By applying Single Sign-On concept into our authentication system, possible frequent authentic operations in ubiquitous environment can be reduced. Instead of using the conventional security card, we developed a new low-power tiny terminal which has ability of encryption-related computation. Therefore, authentication operations over many different services are possible with our tiny terminal. We presented three reference application models that use our authentication system in order to show that our proposed system does not sacrifice usability for security.*

**Area: Ubiquitous Computing**
**Keywords: ZigBee, Security, PKI (Public Key Infra-structure), Ubiquitous Computing, Authentication, Embedded System, Z-stack.**

## 1. Introduction

In recent years, network security has received critical attention from both academia and industry. In a ubiquitous environment, terminals would communicate dynamically with multiple devices and this situation causes critical security problems. Therefore, usable authentication system is highly demanded in a ubiquitous computing environment, which involves multiple devices, services, and ambient sensors. While a Radio Frequency Identification (RFID) solution is widely used for an access control in these days, the RFID solution is not extensible and interoperable because of its limited computing power [1].

In this paper, we propose a method for solving these problems. In a ubiquitous environment, careless maintenance of public security can breed bigger problem than conventional environment. In case that private data are misused and abused, overall system can act as a supervisory system. These problems can be obstacles in a ubiquitous computing realization. An advanced system that verifies authorization about several ubiquitous devices with an authentication mechanism for solving these problems should be deployed.

A hierarchical security system is also needed in a ubiquitous computing environment. A hierarchical digital certificate issuance has been proven under real-world conditions to scale smoothly from hundreds to millions of users [2]. A hierarchical security system can be interacted with other security systems of various organizations. Therefore, it can be integrated to a unified security system and has scalability. This system gives us solution for incompatibility among organizations, and users can receive every services using just one security interface.

Services in various forms may be provided in a ubiquitous computing environment. Access controls to public resources are required because several users may share devices in public place. It is essential to achieve authentication, authorization and verification on the reliability of the users.

In this paper, we have designed an advanced authentication system which is called with Tiny-Terminal System. We deployed the Public Key Infrastructure (PKI) to our system to solve previously mentioned problems. A PKI provides an electronic framework for secure communication and transactions among organizations and individuals. A PKI is based on asymmetric encryption and digital signatures technologies. It enables two parties to exchange confidential electronic messages and to enter into legally binding agreements over the network [3]. A

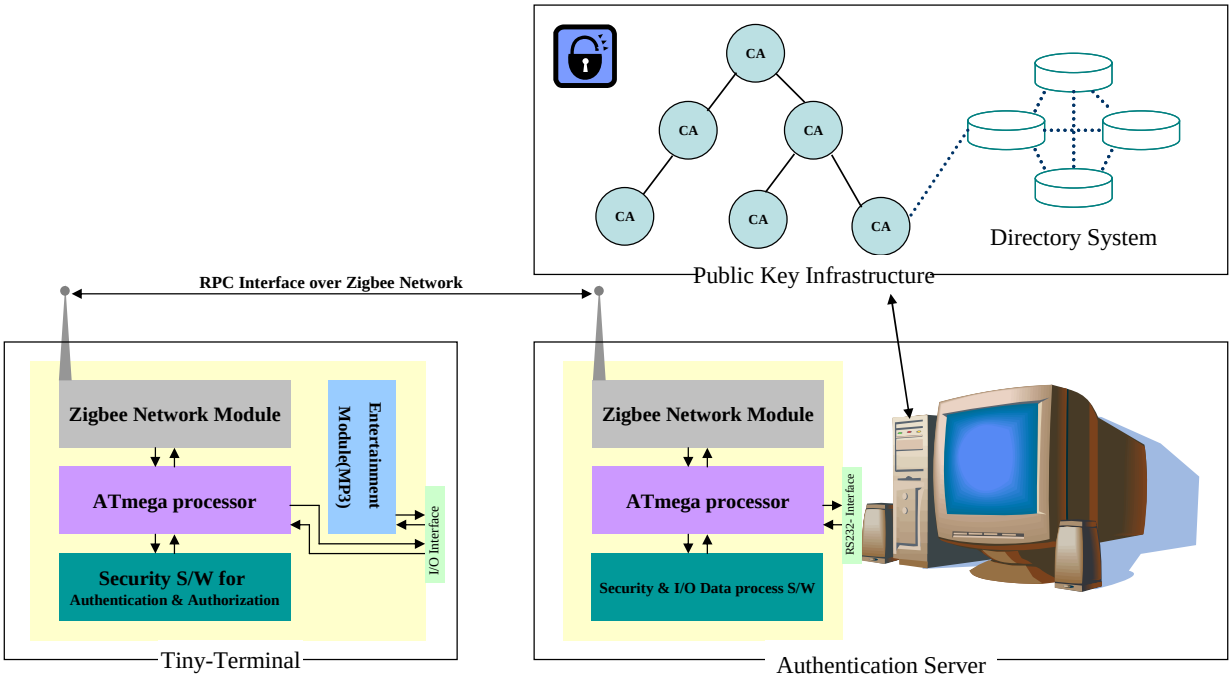


**Figure 2. System Architecture**

PKI is available to its user community around-the-clock. In addition, it is able to scale to millions of users, if necessary, to keep up with organ growth.

We attached ZigBee Communication module for low power communication to our tiny portable terminal whose name is Tiny-Terminal. A low- power wireless technology called ZigBee can be widely applied to the wireless sensor network. ZigBee promises to put wireless sensors in everything from factory automation systems to environmental monitoring. A ZigBee offers battery life of up to several years for common small batteries [4]. The ZigBee module (CC2420) used in implementation of the Tiny-Terminal consumes 20uA on power down mode, 426uA on idle mode, 19.7mA on Tx mode, 8.5mA - 17.4mA on Rx mode [5]. A low power wireless LAN consumes power as 3.5 times, Bluetooth consumes power as 2.75 times than ZigBee module [6, 7]. Therefore, ZigBee module presents possibility that can transmit information with low power, and can develop a tinier terminal by packaging of small size comparing to other modules.

This paper is structured as follows. We begin in Section 2 by describing our system architecture and its components. Section 3 briefly describes a security mechanism using Tiny-Terminal System. Applications using the Tiny-Terminal System are shown in section 4, and conclusions are drawn in section 5.

## 2. System Architecture

In this section we describe overall architecture of our system. The composition of our system is shown in figure 2. The system consists of three major components as Authentication Server part, Tiny-Terminal part that persons carry, and security infrastructure part.

### 2.1 Tiny-Terminal over ZigBee Network

The Tiny-Terminal consists of communication module for ZigBee, processing H/W units for maintenance of security system and S/W that operates the security mechanism and a Z-stack protocol over ZigBee network. The Tiny-terminal communicates with authentication server through the Remote Procedure Call (RPC) interface over the ZigBee network. In addition, we added the MP3 decoder module for the entertainment. It can be utilized as I/O device that can express user's intention and control surrounding devices. ZigBee wireless networks are designed for reliability, scalability (up to 65,000 devices), ease of deployment, long battery life, security and low cost. It uses the license-free, globally available 2.4 GHz frequency. ZigBee devices require microprocessors to run the network stack, which provides the opportunity to put some application code [8]. We deployed the ZigBee stack and developed RPC Interface

and embodied Security System using widely used ATmega128 processor to run ZigBee module on Tiny-Terminal.

A passive Radio Frequency Identification (RFID) has a strong point that does not need electric power. But a RFID tag is an electronic device that holds data, and can not offer scalability [1]. Therefore, it can only just be very limited than authentication using PKI that we deploy. Also, the RFID authentication can not provide users with high level security system. On the other hand, the Tiny-Terminal has ability to process operations and simple I/O interface. It can provide with an interoperable and scalable PKI security mechanism and proactive services like a location based service and personalized services.

### 2.2 Authentication Server

The authentication Server consists of communication module for ZigBee, RPC Interface, processor for maintenance of security system and S/W that operates a Z-stack protocol over ZigBee as shown in figure 2. It takes charge of processing received data from Tiny-Terminal and forwarding to host system using RS-232 interface. Authentication Server is connected to CA that has a hierarchical structure for PKI. CA is a secure third-party organization that verifies the identity and origin of a person or component, which is established using LDAP directory servers. Authentication Server sends the Tiny-Terminal a generated 128-bit random number and verifies the authentication by decoding the received data from the Tiny-Terminal. It can be implemented using SASL (Simple Authentication and Security Layer) protocol. More detailed security mechanisms will be presented in next section.

### 2.3 PKI (Public Key Infrastructure)

There are the symmetric key cryptography and the asymmetric key cryptography in ways that do encipherment for a public security. The symmetric one requires infinite key pairs for maintaining security. It is available when it has a central server structure and there is a key distribution center. However, if the key distribution center got into incapability state, all of system would not operate properly. There is a difficulty of extension, since it is hard to generate infinite symmetric keys. The way to overcome this shortcoming is using an asymmetric one. The asymmetric one is way to use a private key and a public key pairs. The private key is kept individually; the public key is stored in public and stable database. An asymmetric one makes it possible to operate an authentication without a leak of personal information by electric wave and stability of key. So, it can overcome several shortcomings of a symmetric one.

The PKI is a representative security mechanism applied asymmetric one. PKI issues and provides access to public key certificate to preserve the integrity of a public key. It is fundamental for authorization services across the network [ 9 ]. It can be also applied for extensibility on a ubiquitous environment that is required for dynamic connections to surrounding devices.

We gain following advantages by applying infrastructure such as PKI to our Tiny-Terminal System. First, PKI can be utilized very effectively using hierarchical Certification Authority (CA). In the case of conventional security system such as RFID, users should use a different security interface to be authorized for each organization, because there is no compatibility among them. This problem can be solved by using PKI. It can keep maintenance of security through hierarchical CA. Second, Authentic operations can be verified securely without outpouring user’s security information by using internal processor in Tiny-Terminal [10]. Specially, if it has stability like generalized infrastructure, the connection to the infrastructure happens within units that interact with each other physically and the secret information such as password may no longer be transmitted along network. If we should sign-on for each object every time, it drops overall stability, efficiency and user's convenience. This can be solved as applying Single Sign-On concept in infrastructure. Single sign-on is a mechanism whereby a single action of user authentication and authorization can permit a user to access all devices where he has access permission, without the need to enter multiple passwords [11]. Single sign-on reduces human error, a major component of systems failure. So that, Single Sign-On is service that can be deployed to all devices in security infrastructure.

In this paper, we developed the Tiny-Terminal that has ability to verify the authentication over non-TCP/IP network but ZigBee network using PKI. The proposed methods provide a safe connection, a Single Sign-On, end user's pellucid and comprehensive stability.

## 3. Security Mechanism using Tiny-Terminal

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks, authentication is commonly done through the use of logon passwords. In this paper, we proposed Challenge-/Response Authentication Protocol for more secure authentication whose mechanism is operated by one time authentication. Because the Tiny-Terminal can process operations for authentication using the internal processor, the implementation of such protocol is possible. This authentication protocol is a Simple Authentication and Security Layer (SASL) protocol as specified in RFC 2222

[12] whose ideas and concepts are from FIPS 196 [13] and ISO/IEC standard 9798 [14].

As we described in the previous section, an asymmetric authentication algorithm that do not need to exchange key pairs can provide a more secure interface than a symmetric one. We applied an asymmetric authentication mechanism on our system.

Figure 3 describes detailed view of the protocol. In case that the Tiny-Terminal connects to the authentication system, a 128-bit random number is generated at the authentication server and send to Tiny-Terminal within a request frame. (Challenge) The Tiny-Terminal encrypts this random number using own private key and sends encrypted data and ID back to the authentication server within a response frame.(Challenge) Then the authentication server decrypts the received data using public key of it and compares it with the data. If they are equal, the authentication server can believe the authenticity of the Tiny-Terminal. (Response)

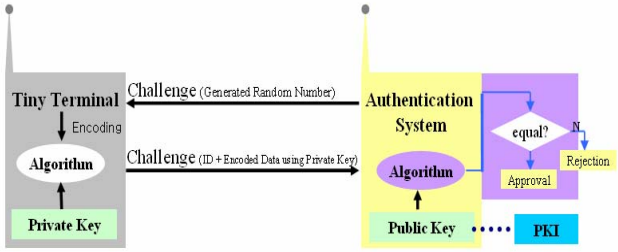


**Figure 3. Authentication Mechanism**

## 4. Applications using the Tiny-Terminal System

We have implemented a prototype of the Tiny-Terminal. Figure 4.1 shows a physical appearance of it whose size is about a half of a credit card. The ultimate goal of our Tiny-Terminal is to intensify portability of it as well as to provide secure valuable services and entertaining services. It has very small form-factor equipped with minimal in/out interface so that a user can wear the terminal as a form of necklace or carry it in one's pocket. The prototype is composed of three functional parts, which are a computational part for authentication using PKI, a communication part using ZigBee module and entertainment part for listening to mp3 music. Our proposed system is applicable to various applications such as examples below making the best use of it.

**Figure 4.1 Tiny-Terminal**

### 4.1 Personalization of a Device

In a ubiquitous environment, several devices and several log-in are required to receive services. Authentication server can detect identification information of users through ZigBee communications. Using this mechanism, we can develop an application that can establish each user's own environment according to the user's location. In case that a user enters within detection region, a binding operation is performed between Tiny-Terminal and authentication server and load the user's authority information and set the personalized device environment by security mechanism.

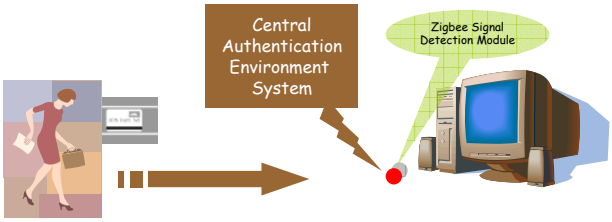


**Figure 4.2 Scenario on Personalized Device**

### 4.2 Shopping in a Mall

Our Tiny-Terminal System can be used in an off-line shopping mall. The system in the mall manages secure information of a client by using PKI and it increases the convenience of a client by providing virtual shopping features. In this application, the terminal is used for a virtual shopping cart where a client does not need to carry a physical shopping cart. Each shop in the mall provides detail information for each good and asks the terminal whether a client buy the product or not through the decision display prepared in the shop. Choices for purchasing goods are transferred to DB system in the mall. When a client walks out of the mall after finishing the

shopping, distribution part in the mall delivers the purchased goods to the client's home.

### 4.3 Services in Campus Life

In this application, Tiny-Terminal is used to authenticate insiders and outsiders of a campus using PKI. It may be possible that only insiders and exchange students in the campus are permitted to enter a specified building such as a dormitory. Exchange student can be authenticated without changing security card. A student having a tiny terminal can be also provided with the location-based services (LBS) such as attendance check and the classroom information about one's schedule. The student serviced from the tiny terminal can experience much easier campus life. A staff or an outsider of a campus can be also provided with personalized service. For example, when a professor wearing a tiny terminal enters a class room for a lecture, a ubiquitous environment may detect the entrance of the professor to the room, taking lecture files from a server, and then projects them to the screen.

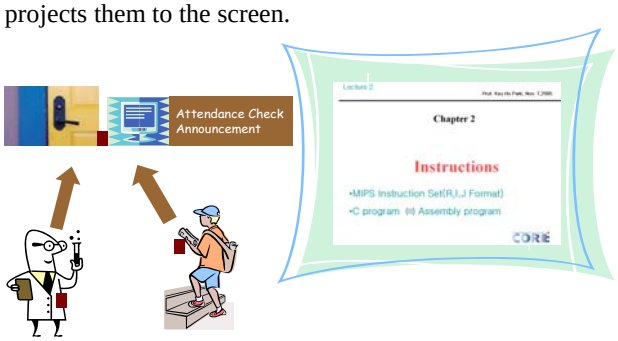


**Figure 4.4 Scenario on Campus Life**

## 5. Conclusion

Our research was motivated by following main factors: (a) In a mobile or ubiquitous environment, terminals should communicate with several devices dynamically and this situation causes critical security problems. (b) Conventional security systems such as a system applying RFID do not provide interoperability and scalability. (c) Such a ubiquitous authentication system which supporting these features is highly required.

In this paper, we propose Tiny-Terminal System with noble security mechanism using PKI especially in a ubiquitous environment. The system consists of three major components. A Tiny-Terminal is a mobile device equipped with a processor and a ZigBee communication module for deploying PKI. The Authentication Server authenticates a Tiny-Terminal by interacting with a security infrastructure which has hierarchical structures for PKI. We described our proposed Challenge/Response Authentication Protocol which is used for more secure authentication. Its mechanism is operated by One-Time Authentication. We also described several scenarios based on the system which enables proactive services like a location based services and personalized services. The proposed Tiny-Terminal System provides more flexible, scalable, interoperable and usable authentication environment than conventional authentication systems.

## 6. Reference


[1] David Molnar, David Wagner "Privacy and Security in Library RFID Issues, Practices, and Architectures" In Proceedings of the ACM 11th Conference on Computer and Communications Security, October 25, 2004

[2] "HHS IRM Policy for Public Key Infrastructure (PKI) Certification Authority (CA)"Office of Information Resource Management Office of the Assistant Secretary for Management and Budget Department of Health and Human Services

[3] S. Chokhani, W. Ford "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework." RFC2527 www.letf.org

[4] Gary Legg "ZigBee: Wireless Technology for Low-Power Sensor Networks " TechOnLine 2004

[5] "CC2420 Datasheet 2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver " Chipcon 2004

[6] "Performance and Power Consumption for Mobile Platform Components Under Common Usage Models" www.Intel.com 2005

[7] Joel Linsky "Bluetooth and power consumption: issues and answers" www.RFDesign.com 2001

[8] David Egan. "The emergence of ZigBee in building automation and industrial control" In Proceedings of the IEEE Computing & Control Engineering Journel, 2005

[9] Qi He, Katia P. Sycara, Timothy W. Finin "Personal security agent: KQML-based PKI" In Proceedings of the ACM 2nd international conference on Autonomous agents 1998

[10] Adams Carlisle, Lloyd Steve "Understanding PKI: Concepts, Standards, and Deployment Considerations" Addison Wesley

[11] Gary Ellison, Jeff Hodges, and Susan Landau " Risks Presented by Single Sign-On Architectures" RPSSOA 2002

[12] J. Myers. RFC 2222: Simple Authentication and Security Layer(SASL), October 1997. Status: proposed standard. Updated by RFC2444.

[13] National Institute of Standards and Technology (NIST). Entity Authentication Using Public Key Cryptography. FIPS PUB 196, 1997.

[14] ISO/IEC 9798-3. Information Technology − Security Techniques − Entity authentication mechanisms − Part 3: Entity authentication using a public key algorithm. ISO, 1993.