International Journal of Innovative
Computing, Information and Control
Volume **5**, Number **6**, June **2009**

 ISSN 1349-4198
pp. 1699–1709

CROSS PLATFORM LAYER FOR PUBLIC KEY INFRASTRUCTURE INTEROPERABILITY

Yu Fang Chung[1] and Hui Fang Chen[2]

[1]Electrical Engineering Department
[2]Information Management Department
Tunghai University, Taiwan
{ yfchung; s934957 }@thu.edu.tw

Received December 2007; revised May 2008

Abstract. *This paper explains various security threats on the Internet. A Public Key Infrastructure (PKI) is often employed to promote internet security. PKI is one of the most common security mechanisms. It consists of a trusted third party, Certificate Authority (CA), who provides internet authentication services. Individuals, industries, and the government use PKI to protect the confidentiality, integrity, and non-repudiation of data. This paper explains the PKI structure including the different types of cryptosystem and PKI technology such as digital signature and PKI components, the way of the components operate, and the four main services provided by PKI. The rapid deployment of the Internet over the last fifteen years has caused a number of serious security issues. Also, Internet gave rise to electronic transactions known as "business-to-business e-commerce" or "B2B e-commerce." Security issues of B2B e-commerce are of great concern due to the need for high level of confidentiality in the information that is exchanged between businesses. As we know, different industries may adopt different security rules and standards. This raises the question of interoperability among various platforms. Thus, an interoperable PKI system that offers trust services will be well received and could become a common industry practice. In this paper, we introduce a Cross Platform Layer (CPL) as a communication interface for facilitating secure PKI interoperability. Based on the proposed mechanism and its functionalities, it is evident that cross-enterprise applications can be easily integrated with different PKIs through an efficient and easy way.*
Keywords: Public key infrastructure, Certificate authority, Digital signature, E-commerce, Cross platform layer

1. **Introduction.** Following the emergence and rapid development of the Internet, breakthroughs in computer network and its applications could totally change present and future work environment and learning and living style. Due to the enormous increase in the number of Internet users, businesses and government are looking at the World Wide Web as another channel for marketing, communication, and promotions. To the business world, the World Wide Web is already a virtual market with unlimited business opportunity [6]. It can break through time limitations which exist in classic real market. There was an alarming growth of 200% in e-commerce in the last quarter of 1999.

However, owing to inattention towards security problems at the early stage of development, the basic structure of computer network has a number of security uncertainties. This paper intends to discuss the hidden threats and loopholes of the Internet, and it explains the structure of PKI to help understand how PKI can solve Internet security problems. Besides, security also plays an important role in e-commerce, especially in cross-enterprise transactions [11]. Therefore, public key cryptography, with its ability to implement non-repudiation [7,13,14], is widely accepted as an important mechanism for addressing the security needs of e-commerce transactions. Each industry has its own PKI