Winter 12-5-2004

The Implementation of Signing e-Document by Using the Wireless Identity Module in Cellular Phone

Chengyuan Ku

Yenfang Ho

Yiwen Chang

The Implementation of Signing e-Document by Using the Wireless Identity Module in Cellular Phone

Chengyuan Ku*, Yenfang Ho, Yiwen Chang

Department of Information Management, National Chung Cheng University,
160, San-Hsing, Min-Hsiung, Chia-Yi, Taiwan, China
Phone：886-5-2720411 ext. 34603, Fax：886-5-2721501
{cooperku, bobo, azure}@mis.ccu.edu.tw

ABSTRACT

Traditionally, the document was recorded on the papers and signed by related personnel to differentiate the responsibility. As the technology of communication is evolved quickly, it makes people connect each other by many different ways. Now, the e-document can be transferred on the network and e-signed with proper tools. However, it still needs people to stay in front of desktop to send and receive e-document. In this paper, we propose a way to send and receive the urgent e-document with cellular phone. For the sake of safety and non-repudiation, the users need to e-sign the document after receiving and before sending our e-document using the embedded wireless identity module (WIM) inside the SIM cards. The use of WIM in the SIM card to sign e-document can make the signing process more secure and reduce the possibility of argument. A prototype of this system was implemented. As can be imagined, the system will provide convenience and security for top managers to handle urgent events and e-document on the move.

Keywords: Smart card, wireless identify module (WIM), electronic document (e-document), mobile office

1. INTRODUCTION

The computers and networks give lots of convenience to us. We can process our e–document very quickly no matter where we are as long as we have the access of Internet. Now, it is convenient to use desktops to get the access of Internet. However, many top managers need to travel very often to handle the remote business. If the notebook is not suitable to be carried with in the long trip and the manager needs to handle the urgent document on the move, the cellular phone or personal digital assistant (PDA) could be a convenient tool to take the initial step. For the consideration of safety and non-repudiation, the proposed system was designed to allow the mobile manager to handle e-document using digital signature through the mechanism of WIM inside the SIM card. The smart card is used to prevent from intrusion by hackers and to show the users' identification to e-document servers. The benefits of using a smart card include [1]：.

- increased security,
- potential user mobility, and
- sequential access to one machine by multiple users.

In 1997, an industry organization named the WAP Forum was founded to develop technical standards to bridge the gap between the mobile and Internet networks. The development of WAP brought the wireless world closer to the Internet through a set of specifications utilizing technologies that enhance the experience of wireless users [14]. The first draft of specifications was published in February 1998. The subsequent release of WAP 2.0 with additional features allows WAP to support improvements in wireless devices and Internet content technologies [14]. WAP can be used to define both communication protocols and application environments. The protocol optimizes the standard Web protocols for use in the low bandwidth, high latency conditions prevalent in wireless networks. Various enhancements to the session, transaction, security, and transport layers make HTTP (Hypertext Transfer Protocol) functionality better suited to the wireless network environment [20]. WAP security functionality includes the Wireless Transport Layer Security (WTLS) and application level security [12]. The WTLS has three classifications of security and provides different functionality as presented in Figure 1.

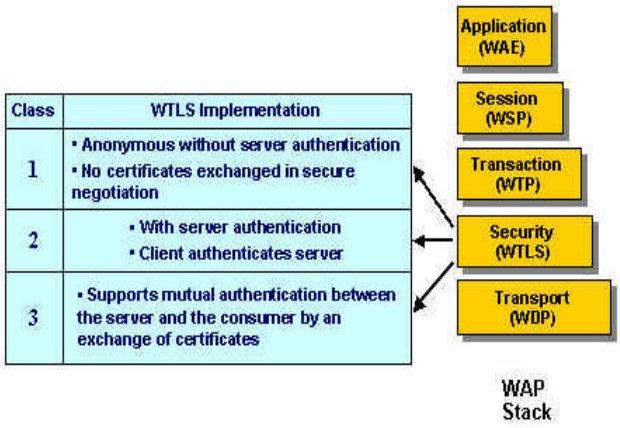

Figure 1. The Security Classification of WTLS [13]

* Corresponding Author

For optimal security, some parts of related functionality need to be performed by a tamper-resistant device [12], especially for level 3 of WTLS. The Wireless Identity Module (WIM) is one of the WAP security function. The WIM is used to perform Wireless Transport Layer Security (WTLS) and application level security functions, and especially to store and process information needed for user identification and authentication [12]. The smart card is the best tamper-resistant equipment. So, our design is to use a cellular phone to provide the better mobility, and the digital signature and mutual authentication will be done by using the WIM embedded in the SIM card. This is the so-called SWIM card. Using the SWIM card to compute the digital signature and authenticate client and server, it can provide the security, mobility and also non-repudiation for e-document transactions.

2. RELATED TECHNOLOGY

2.1 SMART CARD

There are two kinds of smart cards. One is storage card and the other is processor card. People are already accustomed to some applications where a smart card is used just to store data, such as telephone cards and health insurance cards. Currently, the most popular application for processor cards is the SIM card within cellular phone [11]. There are many kinds of applications, which are related to the smart cards. Table 1 presents these applications.

Table 1. The Market Share of the Smart Card [16]

Domain Market	Market Share
Financial Services	16%
Government	13%
Communications	12%
Healthcare	11%
Retail	9%
Transport	8%
Services	7%
Education	7%
Insurance	6%
Utilities	6%
Manufacturing	4%

Because the smart card is a tamper-resistant device, it is widely used for authentication, making payments, or issuing digital signatures. The smart card can protect from physical attack and provide mechanisms against light or abnormal voltage detection, so the security of embedded data is ensured through the use of various coding techniques [11].

To exchange data between the smart card and the terminal, APDUs (Application Protocol Data Units) should be used [9]. The APDU denotes an internationally standardized data unit in the application layer [9]. Table 2 is the format of the command APDU and table 3 is the format of the response APDU.

Table 2. Structure of Command APDU [2, 9, 12]

Mandatory Header				Optional body		
CLA	INS	P1	P2	Lc	Data field	Le

Table 3. Structure of Response APDU [2, 9, 12]

Optional body	Mandatory Trailer	
Data field	SW1	SW2

A command APDU, which is sent by the card reader to the smart card, is composed of a header and a body. The header consists of the four elements [2][9]:

- CLA (class of instruction): the class byte is used to identity applications and their specific command sets.
- INS (instruction code): which encodes the actual command.
- P1、P2 (parameters 1、2): these two bytes are primarily used to provide more information about the command selected by the instruction byte.

The section following the header is the body, which can be dispensed with except for a length specification. The elements of the body are described as follow [2][9]:

- Lc: Lc is the length of the data section sent to the card.
- Data field: contains the data associated with the command that are sent to the card.
- Le: it specifies the length of the data section to be sent back from the card.

The response APDU, which is sent by the smart card in reply to a command APDU, consists of an optional body and a mandatory trailer, as shown in Table 3. The length of the data field may be zero, regardless of the value specified in the command APDU [9]. SW1 and SW2 are the status words to encode the response to the command [2].

2.2 ELECTRONIC OFFCIAL DOCUMENT

There are many disadvantages of manipulations of traditional official document. It may take much of time to deliver the official document and it may be also difficult to reserve the physical document or retrieve it. So our government planed to computerize the official document system and deliver the official document on the Internet since 1993. The electronic document use XML (eXtensible Markup Language) as the national standards. Through the usage of the XML, electronic official document can be exchanged automatically and it is also very easy to be retrieved and maintained. The following Figure 2 describes the infrastructure of e-document exchange. First, the sender should build the official document via XML standard and then use the

digital certificate to confirm the sender's identification. Finally, the sender should e-sign the official document by smart card and then transmit the electronic document to the receiver. After getting the document, the receiver should check the sender's identification and signature and then process the document.

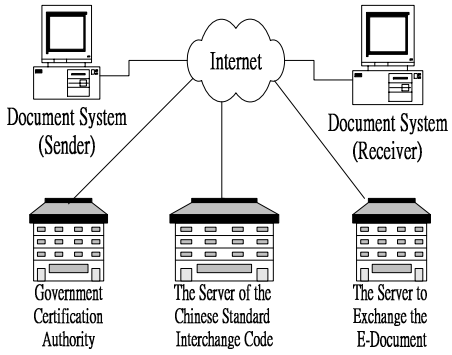

Figure 2. The Integrated Service of the E-Document Exchange

3. SYSTEM ARCHITECTURE

Throughout the usage of the cellular phone, we can utilize the WIM inside the SIM card to verify user's identification and issue digital signature to make the mobile office possible. The Figure 3 presents the system architecture and all functions of WIM are illustrated in Figure 4.

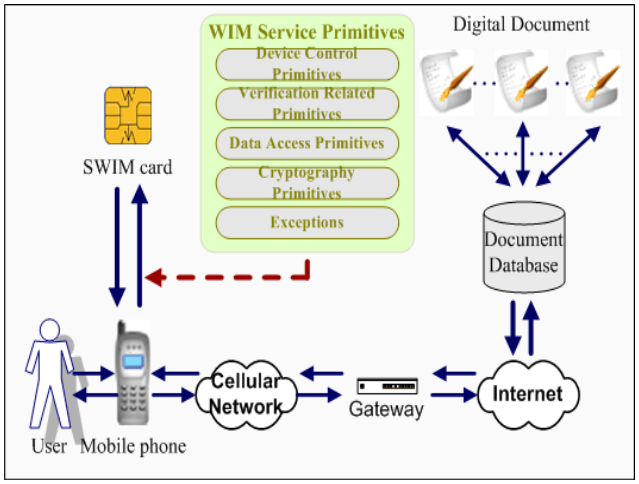

Figure 3. The system Architecture

The WIM contains five categories of service primitives, which are data control primitives, verification related primitives, data access primitives, cryptography primitives and exception [12].

◆ Device Control Primitives

There are two components in the device control primitives, one is WIM-OpenService and the other is WIM-CloseService. The WIM-OpenService can be used to open a logical channel and the WIM-CloseService can be used to close it.

◆ Verification Related Primitives

The verification process is based on a reference data (PIN) stored in the card. A user must be able to verify his/her identity by presenting the verification data.

◆ Data Access Primitives

These primitives can be used to search and access the data in the card.

◆ Cryptography Primitive

These components can be used to compute digital signature, verify signature, derive master secret, etc.

◆ Exception

This primitive is used to warn the user when the system goes wrong.

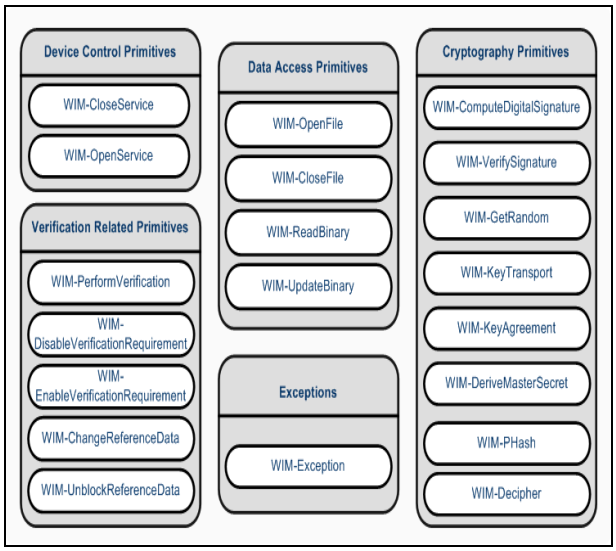

Figure 4. The Service Primitives of WIM [14]

We implement an interface on the mobile phone to communicate with the SWIM card and to access each service primitives. The user can verify his/her identity by entering the Personal Identification Number (PIN) and the SWIM card will return the verification status through the interface as shown in Figure 5. If he/she enters the wrong PIN more than three times, the SWIM card will be blocked and the original PIN will become useless. Only the issuing center can unblock this card [9]. This function can protect the SWIM card against possible unauthorized usage.

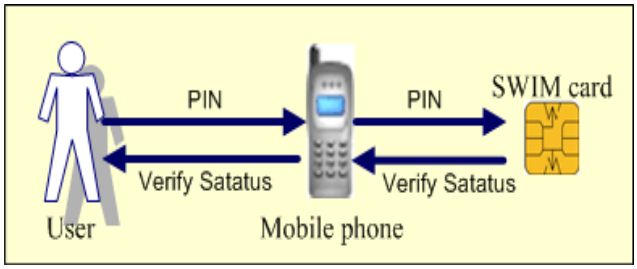

Figure 5. User's Verification

Before computing the digital signature, a Management Security Environment-Restore (MSE-Restore) command should be issued. A Security Environment (SE) is a logical container of a set of fully specified security mechanisms, which are available for reference

in security related commands. Each SE specifies references to the cryptographic algorithms to be executed, the modes of operation, the keys to be used and any additional data needed by a security mechanism [12]. After storing the SE, we should use MSE-SET command to set the location of key of the current SE. Figure 6 illustrates the procedure of computing digital signature.

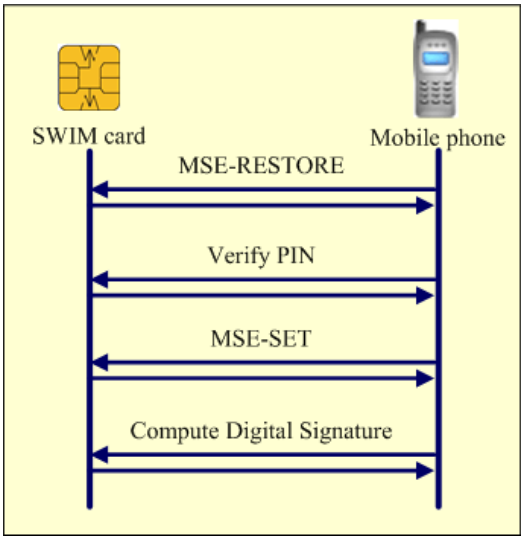

Figure 6. Procedure of Computing Digital Signature [14]

Please set the paper size as A4 (29.7cm*21cm). Leave 2.5cm margins at both the top and the bottom of the page, 2cm on both right and left sides. Please write your paper using MS-Word. The Word of Microsoft's office 97 and 2000 is strongly preferred. If you write the paper by using other versions' Word, please give clear indication of what version of Word you use when you submit the paper by email.

4. PROTOTYPE

The system has two parts, which are the web server and the mobile client. We build the electronic documents with web interface on the server and communicate with SWIM card on mobile client. Therefore we can e-sign the remote digital documents on the web server through the WIM modules in the SWIM card.

Microsoft windows 2000 was chose as the development platform and the JSP (Java Server Pages) and Tomcat 5.0 had been used to implement the website. The development of the mobile client is based on J2ME. First, the user has to login the website of the official document. After the user login, he/she can fill out the electronic form of official document as shown in Figure 7.

Figure 7. Electronic Official Document

Figure 8. Compute Digital Signature

After filling out the form, the user will select the button to compute the digital signature as shown in Figure 8. First, the SHA-1 (Secure Hash Algorithm) is used to compute the digest of official document. Then the web server will transfer this hash value to the mobile client and the mobile phone will invoke the related service primitive to compute the digital signature. If needed, the user can also verify the digital signature through the SWIM card and the card will return the verify status as shown in Figures 9 and 10.

Figure 9. Verify Signature

Figure 10. The Screen of Verify Status

When the user receives the electronic official document, he/she can read and e-sign the receipt as shown in Figures 11 and 12. Therefore the sender of official document knows that his/her document arrives intact.

Figure 11. The letter of receiver

Figure 12. Signing the document while receiving

5. SECURITY ANALYSIS

The security of this system is based on the secure mechanism of the SWIM. We will examine the system security based on the information security standards- ISO/IEC 10181 [4], which are defined by International Organization for Standardization (ISO) and International Electrotechnical Commission. The ISO/IEC 10181 information security standard can be divided into four part, they are Confidentiality, Authentication, Integrity and Non-repudiation. We will ignore the confidentiality because we assume the document is not confidential.

◆ Authentication

Authentication means that the individual is who he or she claims to be. Our system uses SWIM card to authenticate the user. The user should enter his/her PIN code in order to authenticate himself/herself. If the card owner entered the wrong PIN code more than three times, the SWIM card will be blocked and the original PIN code will also be useless.

◆ Integrity

The system should prevent the modification of document when it is transmitted. Our system keeps the digest in the web server. If these digests are not consistent then server will ask the mobile client to send it again.

◆ Non-repudiation

Non-repudiation means that the sender of official document can't deny ever transmitting this document and the receiver can't deny ever getting it. We use the digital signature to prevent the sender or receiver from repudiating their transaction.

6. VARIABLES AND EQUATIONS

In this paper, we propose the system of electronic official document, which can be processed via the cellular phone. In the future, the 3G communication network will provide higher data rate, then the capability of processing multimedia document can be embedded in our system. By adopting the mobility of cellular phones and high data transfer rate, we will go one-step further to the ideal mobile office.

REFERENCES

[1] Chadwick, D.; "Smart cards aren't always the smart choice", *Computer*, Vol. 32, pp. 142-143, 1999.

[2] Chen, Z.; "*Java Card Technology for Smart Cards: architecture and programmer's guide*", Addison Wesley, 1st edition, 2002.

[3] F. P. a. M. R.; Kenneth G. Paterson; "Smart Card and the Associated Infrastructure Problem", *Information Security Technical Report*, Vol.17, pp. 20-29, 2002.

[4] ISO/IEC International Standard, "Information Technology- Open Systems Interconnection- Security Frameworks for Open Systems: 10181", Part1-Part7, 1996.

[5] Mobile Electronic Transaction, "PTD Definition Version 2.0", Oct. 2002.

[6] Nelson, Matthew; "56-bit DES algorithm broken in record time", *Infoworld*, January 25, 1999, p. 8.

[7] Nokia Corporation, "How to utilize Wallet and WIM in mobile transaction services", 2002.
[8] Peyravian, Mohammad; Matyas, Stephen M.; Roginsky, Allen; Zunic, Nevenko; "Generation of RSA Keys That Are Guaranteed to be Unique for Each User", *Computers and Security*, Vol.19, Issue: 3, March 1, 2000, pp. 282-288
[9] Rankl, W.; Effing, W.; "Smart Card Handbook", Wiley, 2nd edition, 2001
[10] Stallings, William; "Cryptography and Network Security Principles and Practices", Pearson Education, 3rd edition, 2003.
[11] Scheuermann, D.; "The smartcard as a mobile security device", *Electronics & Communication Engineering Journal*, Vol.14, Issue: 5, Oct. 2002, Page(s): 205 –210.
[12] WAP Forum, "Wireless Identity Module", Version 12-July-2001.
[13] Douglas A. Kuhlman; "Practical RSA vs. ECC Speed Comparisons", 2002.[14] WAP Forum http://www.wapforum.org
[15] OpenCard http://www.opencard.org
[16] FIND http://www.find.org.tw
[17] International Organization for Standardization http://www.iso.ch
[18] International Electrotechnical Commission http://www.iec.ch
[19] SchlumbergerSema http://www.axalto.com
[20] Shin-Yuan Hung, Cheng-Yuan Ku, and Chia-Ming Chang, "Critical Factors of the Adoption of WAP Services: An Empirical Study," *Electronic Commerce Research and Applications*, vol. 2, no. 1, pp. 42-60, 2003.