

Authentication Methods for USIM-based Mobile Banking Service

Jonghyun Baek¹, Young-Jun Kim¹, Yoojae Won¹, HeungYoul Youm²

Korea Information Security Agency, Seoul, Korea¹
Soon Chun Hyang University, Asan, Korea²
{jhbaek, dream, yjwon}@kisa.or.kr¹
hyyoum@sch.ac.kr²

Abstract. In current advanced internet and electronic commerce environments, the use of accredited certificates first used in PCs has now been expanded to mobile phones and other mobile devices. Due to the lack of computing power and memory in earlier mobile devices, the use of certificates was limited, but recently this limit has been overcome to the point where we have enough processing power to issue, manage, and use certificates freely. As mobile phone technology advances from 2G to 3G, more devices are being equipped with USIMs(Universal Subscriber Identity Modules). This paper presents the current status of authentication methods for mobile banking services in South Korea and proposes an authentication scheme based on the use of USIM-based certificates.

Keywords: PKI, Mobile, Banking, USIM

1 Introduction

We have quickly moved away from internet banking in front of computers, and through our mobile devices it has become possible to conduct balance inquiries, transfer money, and make payments anytime, anywhere. More recently, as mobile technology quickly advances to 3G, USIMs have been brought to the spotlight as a new storage medium. Accordingly, there is also an increased need for secure and reliable self-authentication. As a result, at this critical time before USIM-based mobile banking operates full-scale, and to prepare for the upcoming mobile banking age, we believe it is needed to take actions to spread the use of accredited certificates for mobile banking authentication services, and prepare a standardized format for certificate usage[1]. Since the USIM has security functions that are similar to the HSM(Hardware Security Module)[2], mobile banking security will be strengthened when the certificate is adopted in the USIM and will be considered as being more convenient and secure when compared with internet banking.

In this paper, we look at the concepts of mobile banking and its security requirements, compare current chip-based and VM mobile banking methods and derive its security vulnerabilities, and propose the authentication method using certificates for USIM-based mobile banking services.

2 Current Status of Mobile Banking

2.1 Mobile Banking Concepts

Mobile banking is a financial service where one can conduct bank transactions via an internet enabled mobile phone[3]. In South Korea, this service has been operating since 2003. It differs from telephone banking in that security measures are enabled, and differs from internet banking in that it can be used during movement and travel. Mobile banking services can be divided into the chip-based method which use IC chips, and the VM(Virtual Machine) method, which do not require separate IC chips.

2.2 USIM Overview and Current Status

USIM(Universal Subscriber Identity Module) is a smart card that stores users' personal information(service provider, user password, roaming information, telephone numbers, etc.) for user authentication in WCDMA-type mobile phones. Based on statistics in February 2009, 17.9 million mobile phone subscribers out of 45 million, or about 40% have converted to 3G in South Korea, a sharp increase in just 2 years[4].

2.3 Security Requirements for Mobile Banking

Mobile banking has its symbolic meaning as a financial service where rapidly growing telecommunications technology and financial service converge, but it also has its problems. First of all, mobile banking at its initial stage was less secure because it authenticates the user only by a simple password or PIN number. There was also a threat of key theft as the bank possesses the symmetric keys used in mobile banking. More importantly, accredited certificates could not be used because of the lack of processing power in mobile devices, and therefore mobile banking could not provide the non-repudiation function; an important factor in electronic commerce.

Table 1. Security comparisons between mobile and internet banking

	Mobile Banking	Internet Banking	Comparison
Initial Identification	Face to Face	Face to Face	Identical
Key Creation Place (Key type)	Bank (Symmetric Key)	Terminal (Asymmetric Key)	Mobile banking has a threat of key theft
Key Management	Multiple keys from each bank	Single key management regardless of bank	User needs to maintain multiple keys in mobile banking
Communications Channel	Secure channel	Secure Channel	Identical

Cryptographic Functions Provided	Authentication, Confidentiality, Integrity	Authentication, Confidentiality, Integrity, Non-repudiation	Mobile banking does not provide non-repudiation
---	--	---	---

3 Current Mobile Banking Service Methods

Current mobile banking services can be largely divided into two types; chip-based mobile banking service, which uses an embedded IC chip, and VM-based mobile banking service, which runs on software without the need an independent chip.

3.1 Chip-based Mobile Banking Service

The IC chip-based mobile banking service started in September 2003 through collaboration between Kookmin Bank[5] and LG Telecom[6]. A special embedded IC chip issued by the bank is used as a security enhanced storage device, and this chip stores essential financial information for bank transactions such as account information. A PIN is needed to access information inside the chip.

Currently in South Korea there are three mobile communication companies (SKT[7]: M-Bank, KTF[8]: K-Bank, LGT: BankON) that provide this service. As of March 2009, 4.68 million registered mobile banking users out of a total of 9.15 million use the IC chip-based mobile banking service.

3.2 VM-based Mobile Banking Service

In April 2007, Woori Bank[9] first introduced the VM mobile banking service, which allows banking on a mobile phone without a separate IC chip. VM differs from the IC-based banking service in that it only uses software to enable the financial transactions such as balance inquiry, and transfer of funds on the mobile device. It uses middleware programs (e.g. WIPI) that are created specifically for mobile banking[10].

The VM mobile banking service not only authenticates the user through accredited certificates and secure cards, but also conducts mobile phone self-authentication through SMS, and downloads and installs VM mobile banking software via call back URLs.

When a VM mobile banking subscriber uses the service, he or she first confirms the server by retrieving the mobile banking server's public key certificate, and then creates a secure channel using the public key included in the server's public key certificate.

Initial VM mobile banking services simply used passwords and secure cards for authentication, but as the performance of mobile devices improved, it became possible to transfer the certificate on the PC to the mobile device or even issue and digitally sign using only the mobile device.

There are 4.47 million using the VM-based mobile banking service out of a total of 9.15 million registered mobile banking users as of March 2009.

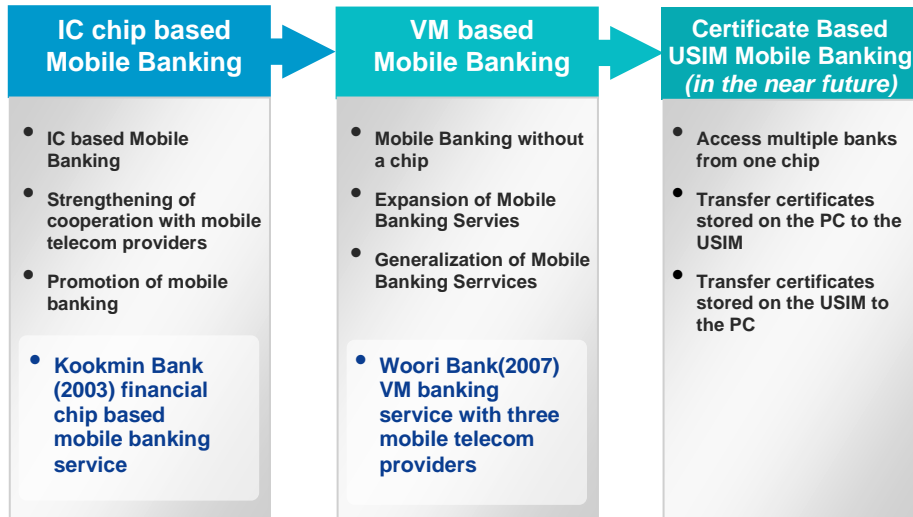


Fig 1. Development of Mobile Banking Services

4 Proposal for a USIM-based Mobile Banking Service using Accredited Certificates

In this chapter we propose a scheme for authentication and certificate management in USIMs, a new common storage media in the 3G environment, for secure mobile banking.

The memory of a USIM can be divided into a general storage area and a secure area which takes the role of a HSM(Hardware Security Module)[11]. Extraction of the accredited certificate and private key is possible in the general storage area, but not in the secure area. This results in a different authentication method depending on the storage location of the accredited certificate.

4.1 Authentication Method Using the General Storage Area of the USIM

This method is used when the user transfers the accredited certificate from the PC to the general storage area of the USIM inside the mobile device, and then downloads the certificate stored in the USIM to another computer to use for digital signature and authentication.

When a 3rd party relay server is used, the software must confirm the credibility of the relay server through a relay server certificate.

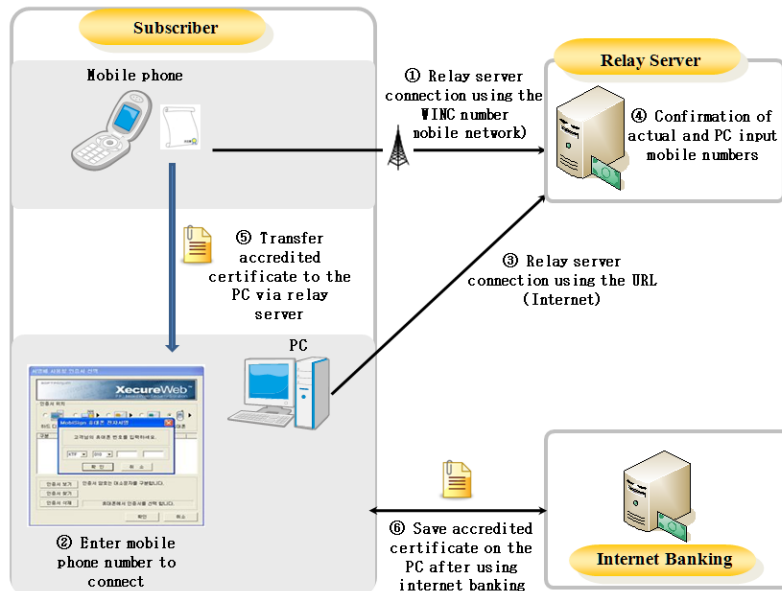


Fig 2. An example of transferring a certificate stored on the USIM to the PC

4.2 Authentication Method Using the Secure Area of the USIM

Authentication using the USIM's secure area can be divided into two methods depending on the issuing location. The first method transfers the certificate issued on the PC to the USIM and signs on the USIM. The second conducts certificate issuance and signing directly on the USIM.

4.2.1 Issuance of the Certificate on the PC

This method first transfers the certificate to the USIM's secure area after it has been issued on the PC, and during authentication, uses the certificate stored in the USIM for digital signing.

The certificate must use an encrypted channel during transfer from the PC to the mobile device. In this case, the transfer channel must have security of at least 1024 bits RSA. Also, the channel must use newly generated keys for each transfer, and when using an internet connection, ensure integrity of the message by conforming to PKCS#12[12].

The private key should be encrypted according to PKCS#5[13], and stored safely according to PKCS#8[14].

4.2.2 Issuance of the Certificate on the USIM

This method issues and stores the certificate on the USIM's secure area, and uses the certificate stored in the USIM for digital signatures.

When invoking the digital signature functions to use the private key stored in the USIM, the standard interface functions of PKCS#11[15][16] must be used.

PKCS#11 is a standardized interface for HSMs with cryptographic processors. It defines a consistent interface defining functional requirements while also providing security for private key and accredited certificates. As defined in PKCS#11, USIM functions such as C_Initialize, C_Finalize, C_GetInfo, and C_GetFunctionList must be supported for initialization, freeing of resources, and general information queries. Key pair generation functions C_GenerateKeyPair, C_SeedRandom, and C_GenerateRandom must be supported. In addition, C_SignInit and C_Sign must be supported for electronic signatures using private keys.

4.3 Comparison of Current Mobile Banking Methods and the Proposed Method

When comparing chip-based and VM-based mobile banking methods, the chip-based mobile banking method is fast since financial information is stored directly inside the chip. It can be used in offline environments such as ATM machines and transportation cards. However, these IC chips cannot be used across multiple banks; therefore a separate chip is needed for each individual bank.

The VM-based mobile banking method enables the user to access the online banking system directly without interaction via a third-party portal. It also reduces processing time when compared with chip-based mobile banking as it only sends and receives relevant data directly related to banking. Another major advantage is that there is no need for additional hardware such as a smart card. On the other hand, this method is more vulnerable to hacking since the users' financial information is processed directly in the memory of the mobile device. Currently, there is no code signing for VM programs downloaded through open networks, creating a potential issue[17] of personal information leakage via malicious VMs, and cell phone hacks.

The proposed method can solve the weaknesses of both chip-based and VM-based authentication methods. It solves weaknesses of VM-based mobile device hacking through hardware protection, and weaknesses of chip-based compatibility issues through a common storage space. Moreover it provides the non-repudiation, an important factor in mobile banking authentication, through accredited certificates.

Table 2. Comparison of Current Mobile Banking Methods and Proposed Method

	Chip-based Authentication	VM-based Authentication	USIM-based Authentication
Authentication Methods	- Internal to chip, PIN	- Accredited certificates, Secure cards, SMS authentication, etc.	- Accredited Certificates

Pros	<ul style="list-style-type: none"> - Fast processing time - Offline usage - Enhanced security 	<ul style="list-style-type: none"> - Shorter processing time than chip-based methods - No need for separate hardware 	<ul style="list-style-type: none"> - Provides hardware-based security which includes protection against mobile device hacking such as key theft - Provides non-repudiation through digital signatures - Compatible between banks
Cons	<ul style="list-style-type: none"> - Separate IC chips need to be issued for each bank - Vulnerable to PIN guessing attacks due to short PIN lengths 	<ul style="list-style-type: none"> - Vulnerable to hacking the customer's financial information - Personal information leakage due to malicious VM, mobile phone hacking, and excess fees due to authentication systems not being established 	<ul style="list-style-type: none"> - Can only be used in 3G type mobile devices

4.4 Security characteristics for proposed authentication scheme for USIM-based Mobile Banking Service

The proposed authentication scheme has the following security characteristic;

- Mutual authentication between the mobile banking subscriber and mobile banking system
- Protect against all potential threats: eavesdropping, modification/insertion of transaction message, replay attacks
- Simple key management
- Prevention of accredited certificate and private key theft
- Storage device with enhanced mobility and security
- Hardware-based memory protection

5 Conclusion and Future Work

In this paper we have presented the status of mobile banking services in South Korea from its start to present time, and have proposed an authentication method for USIM-based mobile banking services as a next generation PKI-based mobile banking technology.

Hardware performance of the USIM is constantly improving, and performance is currently sufficient enough to load and utilize a digital certificate. By using accredited certificates in the USIM for mobile banking services, it will be possible to overcome problems that the chip-based mobile banking method held regarding incompatibilities among different banks on a single chip, and major problems of VM banking services such as mobile phone hacking can be solved. Also, by using HSM functions in the

mobile device private key theft can also be prevented, and through certificates non-repudiation can be provided.

In the future, more research on accredited certificate usage schemes will be needed to prepare for new mobile communication technology with the advent of 4G.

References

1. Korea Financial Telecommunications and Clearings Institute, "The Status and Outlook of Self-authentication Methods in Non-confrontation Payment Services", April 2009 (Written in Korean)
2. Korea Information Security Agency, KCAC.TS.HSMU v1.80, "Accredited Certificate Usage Specification for Hardware Security Module", Oct 2008
3. Mobile Banking, <http://100.naver.com/100.nhn?docid=784608> (Written in Korean)
4. Bank of Korea, "2009 First Quarter Korea Internet Banking Service Usage Status", April 2009 (Written in Korean)
5. Kookmin Bank, <http://www.kbstar.com>
6. LG Telecom, <http://www.lgtelecom.com>
7. SK Telecom, <http://www.sktelecom.com>
8. KTF, <http://www.ktf.com>
9. Woori Bank, <http://www.wooribank.com>
10. WIPI Forum, <http://wipi.or.kr/> (Written in Korean)
11. KISA, KCAC.TS.HSMS v1.10, "HSM Storage Format Specification for Accredited Certificate", Oct 2008
12. RSA Laboratories, PKCS#12, "Personal Information Exchange Syntax Standard", v1.0, 1999
13. RSA Laboratories, PKCS#5, "Password-based Encryption Standard", v2.0, 1999
14. RSA Laboratories, PKCS#8, "Private Key Information Syntax Standard", v1.2, 1993
15. RSA Laboratories, PKCS#11, "Cryptographic Token Interface Standard", v2.11, 2001
16. RSA Laboratories, PKCS#11 Profile, "Conformance Profile Specification", 2001
17. Korea Financial Telecommunications and Clearings Institute, "Trends and Issues of National and International Mobile Payment Services", April 2009 (Written in Korean)
18. Hyung-Jin Lim, Hee-Won Shim, Seung-Hyun Seo, Woo-Jin Kang, "Authentication Technology Trends in Electronic Financial Transactions", Korea Institute of Information Security and Cryptology Review, Book 18. Vol 5. October 2008 (Written in Korean)
19. Steffen Hallsteinsen, Ivar Jorstad, Do Van Thanh, "Using the Mobile Phone as a Security Token for Unified Authentication", Proceedings of the Second International Conference on Systems and Networks Communications, Page 68, August 2007
20. Hassinen, M. , Hypponen, K., "Strong mobile authentication", Wireless Communication Systems, 2005, 2005
21. Jang-Mi Baek, In-Sik Hong, "Secure Payment Protocol for Healthcare Using USIM in Ubiquitous", ICCSA 2005, 2005
22. Hyeyeon Kwon, Kyung-yul Cheon, Kwang-hyun Roh, Aesoon Park, "USIM based Authentication Test-bed For UMTS-WLAN Handover", IEEE Infocom 2006, 2006
23. Yuh-Min Tseng, "USIM-based EAP-TLS authentication protocol for wireless local area networks", Computer Standards & Interfaces, Vol 31, Issue 1, Jan 2009
24. Rachna Dhamija, Adrian Perrig, "DejaVu: A User Study Using Images for Authentication", Proc. 9th Usenix Security Symp., Usenix, page 45-58, August 2000