Design of A Micro SD Card based Security Middleware for M-Commerce

Guifen Zhao, Ying Li, Liping Du, Fei Duan
Beijing Key Laboratory of Network Cryptography Authentication
Beijing Municipal Institute of Science & Technology Information
Beijing, China
gfzh@hotmail.com

***Abstract*—M-commerce security middleware is one of methods to achieve secure application. A micro SD card based security middleware is designed for new generation mobile commerce system constructed on the basis of SOA and using Web Service, smart mobile terminal, combining the commercial flow with technical flow. The security components are developed on the basis of cipher service provide by micro SD card, encryption cards and combined secret key method, and provide security service interfaces based on J2EE. The middleware is proved valid and protect the secrecy and integrity of order information for m-commerce and achieve secure mobile payment.**

Keywords- security middleware; m-commerce security; micro SD card; encryption card; combined secret key algorithm

I. INTRODUCTION

With the increasing prevalence of smartphone, there are more and more mobile internet users, and many users among them prefer to mobile shopping, booking tickets, mobile check-ins, mobile banking, payment for transport and purchases via smartphone, etc. [1-4]

The new generation mobile commerce system is constructed on the bases of SOA and use Web Service [5], smart mobile terminal, mobile VPN and other new technologies. Except for Web Service, CORBA is another method to achieve SOA, therefore there is Message-Oriented Middleware system [6, 7]. Combine the commercial flow with technical flow and map the relationship between each other, so that functional mobile commerce system is achieved. It is in advantage of the first and second generation m-commerce system. The first generation m-commerce system is based on SMS with limited interactivity and poor real time response. The second generation m-commerce system adopts WAP and then mobile users access the WAP pages via browser, which can query information online. However the security is an important problem to be solved.

Till now powerful end devices with easy mobility and large storage space confront more risks than personal computer, such as financial data, location, SMS, MMS, etc. [8] Security is a key point to achieve secure mobile application. And the mobile management is becoming less about devices and more of the application security [9, 10].

Mobile application security commonly consists of several mode including no security, basic security and hardened security. For hardened security mode, there is encryption, many security levels and storage in secure element including removable or non-removable elements, e.g. UICC (SIM), SD card or embedded hardware secure element using a non-removable SIM-type element, and secure element features in the mobile device as part of the baseband processor [11].

Secure elements develop gradually and provide more secure computation function. Different cryptography and key management methods are presented. For convenience and high efficiency, a micro SD card based security middleware scheme using micro SD card and combined secret key is proposed and implemented.

II. SYSTEM STRUCTURE OF SECURITY MIDDLEWARE

The security middleware consists of five layers and four-level interfaces including component interface, security service programming interface, commonality security service interface and basic interface [6, 7]. The architecture of the mobile security middleware is shown in Fig. 1.

Security service providers are taken charge of micro SD card manufacturer and encryption card manufacturer, and provide cipher service, data storage, extensible resources and other service by basic security service interfaces.

Commonality security service management is provided by middleware platform manufacturer, which provide unified interfaces, security task management, independence from platform, high-efficiency and shield the complexity of basic algorithm.

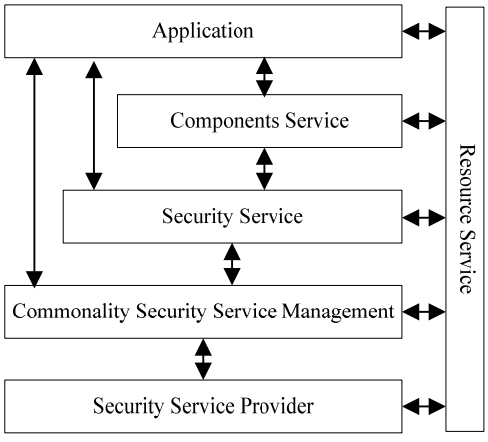

Figure 1. Architecture of Security Middleware.

Security service is taken charge of security service provider and consists of TLS, SET, CORBA and J2EE,

which extend the available security middleware function and provide cooperation among security modules under distributed environment.

Component service provides security service interfaces on the basis of CORBA and J2EE [12]. The middleware based on micro SD card provides J2EE based component interfaces.

Application layer is developed on the basis of components service without consideration about the detail of cipher module, network distribution and other particular environment. The extensible application interfaces include message encryption and decryption, authentication, key distribution, digital signature and signature verification.

III. DESIGN OF SECURITY MIDDLEWARE

A. *Network Topology of M-commerce System*

According to common business flow, there are end users, retailers, payment organization and authority centre, etc. The mobile shopping is achieved via the cooperation among consumers at smart end, retailers, retail servers, payment gateway, payment servers and authentication servers. The network topology of the m-commerce application system is shown in Fig. 2.

The security middleware for m-commerce is designed for mobile internet users own a smartphone which can equip a micro SD card providing cipher service including encryption and decryption in chipsets. Combined with mobile security middleware, micro SD card can realize identity authentication for mobile end user and data protection for business information.

At retail servers, retailers provide online products list and detailed products introduction to mobile internet users for browsing and placing orders.

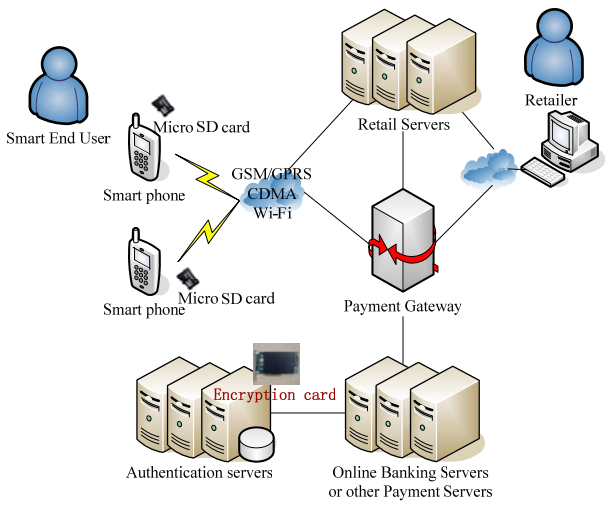

Figure 2. Topological Graph of M-commerce Application System.

All payment requests are collected at payment gateway and then transferred to online banking servers or other payment servers.

Online banking servers or other payment servers take charge of transferring remittance after authentication and verification performed by authentication servers to enhance the security level.

According to the tasks transferred by payment servers, authentication servers perform specific remitter's identity authentication, decryption and integrity verification of payment information to guarantee the security of mobile payment. Authentication servers are equipped with several encryption cards to provide cipher service at server including encryption and decryption in chipsets.

B. *Mobile Payment Flow*

After placing orders, consumers start payment. The mobile payment includes payment at smart end by consumers, collection and transfers of payment requests by payment gateway, authentication and verification by authentication servers, remittance by payment servers, and remittee confirm by retailers. The order and payment flow is shown as follow.

- At smart end, consumers browse products list provided by retail servers. Consumers need log in the m-commerce system when ordering, and then place an order. Meanwhile smart end sends out a payment request to payment server.
- Payment gateway transfers all relative payment information to payment servers.
- Payment servers deal with the remittance process if the users and order is verified. And then retailer, i.e. remittee gets the payment for products.

C. *Main Module of Security middleware*

The security components, including ActiveX content and Dynamic Link Library, are developed on the basis of micro SD card, encryption cards and combined secret key method and provide J2EE based service interfaces. The extensible application interfaces include message encryption and decryption, authentication, key management, digital signature and signature verification.

1) Key management: Each user is assigned a set of secret key seeds amount to about 1.4KB. These key seeds are generated by random number generator of micro SD card, and directly stored into the E2PROM/flash of micro SD card. After generating user's secret key seeds and assigning mobile user's ID and other application information, the micro SD card is distributed to appointed m-commerce user, viz. the user gets its own key seeds. Only the encrypted secret key seeds are output for key exchange. The encrypted secret key seeds output from micro SD card are transferred to authentication server. Users' key seeds are stored in database of authentication server after encryption performed by encryption cards. Authentication servers connect the database for acquiring user's key seeds when encryption or decryption. According to combined secret key

generation algorithm, micro SD card key selects 16 bytes of key seeds according to random numbers and time stamp to combine and generate a one-time secret key for encryption or decryption.

2) Authenticaiton: Smart end users need generate an authentication value by micro SD card equipped on smartphone when logging in. Firstly, micro SD card generates a secret key according to combined secret key algorithm. The authentication value is created by encryption using the secret key mentioned above, and sent to authentication server for identity verification. Authentication server sends the received authentication value, user identity number, time-stamp and random numbers to certain encryption card for regenerating secret key according to time-stamp, random numbers and users' encrypted key seeds stored in database of authentication server. And then regenerates user's authentication value in encryption card, and compare these two values generated by client and server to gain authentication result at last. The authentic user can login the m-commerce system.

3) Message encryption and decryption: When placing an order, the detailed business data about order form are encrypted by micro SD card equipped on smartphone to keep the secrecy of the order data. Firstly, micro SD card generates a secret key according to combined secret key algorithm. The encrypted data are sent to servers. Finally, authentication server decrypts detailed business data by encryption card equipped on authentication servers for normal payment and storage of order data. The decryption key, corresponding with the encryption key, is generated by encryption card equipped on authentication server according to time-stamp, random numbers and users' encrypted key seeds stored in database of authentication server.

4) Digital signature and Signature verification: When submitting and paying for mobile order, the detailed business data about order form are generated an integrity value. The integrity value is calculated via HASH, i.e. digital fingerprint. And then encrypt the integrity value by micro SD card equipped on smartphone to achieve digital signature. The encryption key is generated as mention above. Authentication server decrypts the received digital signature of order form and regenerates an integrity value at server by encryption card equipped on authentication server, and compares with the received integrity value from smart end to obtain a verification result. Mobile payment system can control the remittance operation according to the digital signature verification result. Consequently the security middleware guarantees the remittance security.

D. Work Flow of Security middleware

The payment flow is presented when using the security middleware. Work flow of security middleware for commerce is started by smart end users during payment. The detailed work flow is shown in Fig. 3:

- While paying via browser, mobile end starts a payment request firstly and get a time-stamp from payment server.
- Smart end call micro SD card equipped on smartphone to generate 16 hexadecimal random numbers and then combines user's key seeds according to the random numbers and received time stamp to generate a secret key in chipsets of micro SD card.
- The detailed payment data are generated an integrity value at mobile end. And then encrypt the integrity value by the secret key in chipsets of micro SD card to obtain digital signature and data ciphertext.
- Smart end encodes mobile end user's identity number, random numbers, time-stamp, digital signature and data ciphertext, and then sends the encoded data to payment server.
- Payment server decodes the received data and then communicates with authentication server for transferring decoded data to make sure whether the payment is sent from the remitter and the data of payment form is integrated or not.
- Authentication server regenerates secret key via certain encryption card equipped on server according to received time-stamp, random numbers, user identity number and user's encrypted key seeds stored in database of authentication server. And then decrypt received data ciphertext using the secret key to obtain plaintext of payment data and integrity values from mobile end, and regenerates integrity value at server. Compare these two integrity values generated by mobile end and authentication server to gain verification result at last and return it to payment server.
- If the order is verified, payment servers deal with the remittance process finally. And then the payment is completed, i.e. the retailer receives the payment for products.

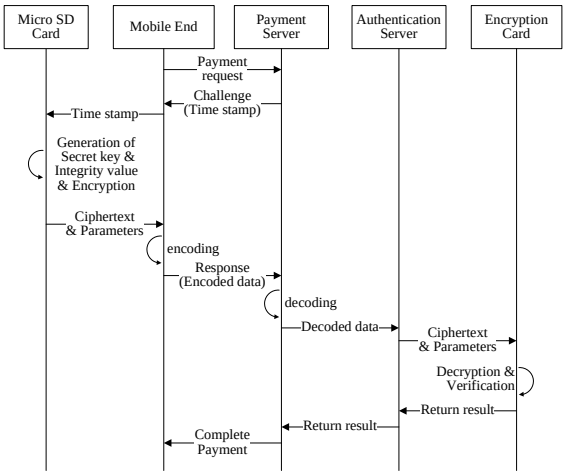

Figure 3. Work Flow of Secure Payment.

IV. IMPLEMENTATION

The components of security middleware are developed under Visual Studio 2008 environment, including ActiveX content and Dynamic Link Library. Regard a smartphone with windows mobile operation system as mobile end. At smart end, all correlative components are packed as a cab file which can be installed at smartphone with windows mobile operation system. Smart end users can perform secure mobile payment normally in m-commerce system integrated with the security middleware after installation. The payment servers install the server components of security middleware and communicate with authentication servers to perform secure authentication and remittances operation. Test environment includes simple interactive pages. Browse test page at smartphone and submit payment request after filling in simulated order information, and then the secure middleware can deal with the authentication for smart end users and data protection for order information. Test results reveal the security middleware run validly and steadily. During the test procedure, the resource usage of authentication server is in reasonable range.

V. CONCLUSIONS

As more and more mobile internet users prefer to m-commerce with the increasing prevalence of smartphone, the m-commerce security is becoming a serious problem to be solved. A micro SD card based security middleware scheme using micro SD card, encryption cards and combined secret key is proposed and implemented under Visual Studio 2008 environment. The security middleware provides message encryption and decryption, authentication, key management, digital signature and signature verification function. Combining the commercial flow with technical flow and map the relationship between each other, the security middleware can protect the secrecy and integrity of payment information. The security components provide J2EE based service interfaces. Test proved that the secure middleware can deal with the identity verification for smart end users, data encryption, decryption, digital signature and integrity verification for order information to perform secure payment.

ACKNOWLEDGMENT

Authors would like to appreciate the support from the Program of Network Authentication Lab affiliated to Beijing Municipal Institute of Science & Technology Information (No. PXM2011_178214_000007). And also thank the helpful suggestions from the director and colleagues in Beijing Key Laboratory of Network Cryptography Authentication.

REFERENCES

[1] Jacob West. Software Security Goes Mobile. RSA2012.

[2] Mobile Payments Appeal to Many in Britain. http://www.emarketer.com/Article.aspx?R=1009322.

[3] Banking Customers Turn to Online, Mobile for Transactions. http://www.emarketer.com/Article.aspx?R=1009375.

[4] Nascent Mcommerce in China Shows Explosive Growth. http://www.emarketer.com/Article.aspx?R=1009367.

[5] ZHENG Jin , WU Wei-min , CHEN Chu-min , DAI Xiao-mian.Advantage of Security Middleware Based on Web Services and Its Design and I mplementation. MODERN COMPUTER. 2009(8). pp. 135-137, 140.

[6] ZENG Linghua, OUYANG Kaicui, ZHOU Mingtian. Design and Implementation of CSPI of Security Middleware. Computer Engineering. 2006, 32(18). pp.178-180, 183.

[7] LI Ke-jin, JIANG Ze-jun. Security Middleware Based on CPK. SCIENCE TECHNOLOGY AND ENGINEERING. 2009,9(7). pp.1761-1765, 1771.

[8] Chris Wysopal. Defending Behind the Device: Mobile Application Risks. RSA2012.

[9] Dan Raywood. The future of mobile managment will be away from the device and more about applications (SC Magazine UK). http://www.scmagazineuk.com/the-future-of-mobile-managment-will-be-away-from-the-device-and-more-about-applications/article/264363/.

[10] Nicko van Someren. Data Loss Prevention: The Evolving Landscape of Mobile Enterprise Threats. RSA2012.

[11] Randy Vanderhoof. Applying the NFC Secure Element in Mobile Identity Apps. RSA2012.

[12] LI Wan-ting. Research and implement of security middleware based on J2EE. COMPUTER ENGINEERING AND DESIGN. 2005,26(6), pp. 1548-1550.