



## Discussion and Application of WPKI Technology

Lunyong Chen & Chunqing Li

College of Computer Technology and Automation, Tianjin Polytechnic University

Tianjin 300160, China

E-mail: chen Yongtjwd@163.com

### Abstract

With the developments of wireless communication and wireless network technology, the wireless data service will be more widely used in commerce. In order to realize safe electronic commerce, the security of wireless network should be assured. As a rising technology to implement wireless network safety, WPKI (Wireless Public Key Infrastructure) becomes more and more important. This article will discuss structure, implementing principle, security infrastructure, application model and application in wireless network environment of WPKI, analyze the functions of WPKI in WAP security, and probe into the application prospect of WPKI.

**Keywords:** WPKI, WAP, WTLS, PKI, Network safety

### 1. Introduction

With the developments of mobile communication technology and Internet, the application wireless communication technology gradually becomes mature, and its security becomes more and more important. In cable network, one important security guarantee is PKI (Public Key Infrastructure). Keeping to the standards, PKI is the key management platform to pellucidly provide key and certificate management needed by cryptogram services such as encrypting and digital signature for all cable network applications. In wireless network, WPKI (Wireless Public Key Infrastructure) properly complements, optimizes and improves PKI to fulfill the requests including secrecy, integrality, authenticity and undeniable character of wireless network security. WPKI also adopts some management mechanism being differ from PKI to fulfill the needs of wireless network environment.

### 2. Structure of WPKI

For WPKI, the key management system is composed of EE (Entity End), PKI portal, CA (Certification Authority), PKI directory and other parts. In the application mode of WPKI, it also involves data server, WAP gateway and other service equipments. The basic structure and data flow of WPKI are seen in Figure 1.

In Figure 1 these following parts are involved.

(1) EE (wireless user)

EE in WPKI depends on WMLSCrypt API to realize key management and optimization of encrypt computation. Its main functions include producing, storing and allowing visiting user key pair or public key pair, application of original certification, updating request of certification, recalling request of certification, inquiring, recovering and recalling certification information, validating certification, reading certification, producing and validating digital signature.

(2) PKI Portal (RA Registration Authority)

Like WAP gateway, PKI Portal is also the server operating on the cable network. Its function seems to RA in cable PKI, and it is usually used as the joint bridge between cell-phone terminal and present PKI, taking charge of transforming the requests to RA and CA in PKI for WAP users.

(3) CA (Certificate Authority)

It takes charge of signing certification, Authorizing certification, managing authorized organization, constituting policies and concrete approaches to validate and identify users' identities, and signing user certification to insure certification owners' identities and properties to public key.

(4) PKI Directory

The certification sending server such as LDAP (Lightweight Directory Access Protocol) directory server takes charge of sending certification information to CA and content server.

(5) Content Server

It provides content service to users. Taking WEB server as an example, it mainly takes charge of providing service information needed through content server after successful authority.

#### (6) WAP Gateway/Proxy

In WAP 1.X, a WAP gateway is needed to deal with protocol conversions between users and source server. WAP gateway uses WAP protocol to communicate with users and uses standard Internet protocol to communicate with source server. But in WAP 2.0, users and source server can directly use HTTP 1.1 to communicate, which also involves WAP 1.0.

### 3. Implementing principle

In wireless network, the method of security mainly is WPKI. The concept of WPKI is developed from cable PKI, that is to say, in wireless environment WPKI offers security service system similar with cable PKI. WPKI is the proper complement and reasonable optimization of cable PKI in its present mechanism to adapt the characteristics of wireless communication service. The characteristics of wireless communication service are that the calculating ability, frequency width and EMS ability of wireless communication terminal such as cell-phone and PDA are much lower than the computer in cable network. Therefore, WPKI needs adopting some management mechanisms other than cable PKI to adapt these characteristics and offer safe guarantee for applications in wireless network. But for users they can enjoy security service like PKI, just the terminal equipments are different and carriers are wireless. As viewed from this opinion, WPKI is a sort of extension of PKI security service in wireless network.

WPKI adopts optimized ECC encryption and constringent X.509 digital certification. It also adopts certification management public key, validates users' identities through the third party's credible organization, CA (Certificate Authority) to realize safe transport of information. The wireless terminal applies for digital certificate to CA through registration authority, then CA sends digital certificate for users through auditing users' identities, users store certificate and key in UIM card, and the wireless terminal utilizes digital certificate to ensure the security from port to port when implementing electronic business on wireless network. ISP internet confirms users' identities through validating user certificate and offers users corresponding services to realize safe running of wireless network application.

### 4. Security infrastructure

WAP is a collection with language, communication protocol and tools, which aim is to fulfill the requests that people link internet in move and pass contents and super data operations on internet to wireless mobile users. WAP security infrastructure includes WIM (WAP Identity Module), WMLSCrypt (WML Script Crypto API), WTLS (Wireless Transport Layer Security) and WPKI.

#### (1) WIM (WAP Identity Module)

WIM is an embedded chip preventing juggle in WAP equipments (such as cell-phone and PDA) to store key information such as WPKI public key and user key and other relative certificate information. At present, SIM card is usually used to implement the security module. Because WAP terminal equipments such as cell-phone and PDA have limited processing abilities and limited resources, so the SIM card realizing WIM module also can have its own processor, integration code arithmetic assistance unit, RAM and EEPROM, and can realize encrypting arithmetic and other functions.

#### (2) WTLS (Wireless Transport Layer Security)

WTLS evolves from TLS (Transport Layer Security), adapts to be used in narrowband communication channel to validate communication users, encrypted WML data and check their integralities. Based on encrypting technology, WTLS offers services including data integrity, confidentiality, identification and forbidden service protection, and provides safe guarantee for using mobile data communication to implement business operation.

#### (3) WMLSCrypt (WML Script Crypto API)

WMLSCrypt API is an application program interface (API) and it offers WMLSC lib for WML (Wireless Markup Language). This lib gives basic security functions which include producing key pair, storing key, accessing control to stored key and data, producing and validating digital signature, encrypting or encoding data and so on. WML script lib utilizes WIM module to offer supports for bottom code operation.

#### (4) WPKI

Aiming at wireless communication environment, WPKI performs optimized development on the base of cable PKI. It usually uses BER (Basic Encoding Rules) and DER (Distinguished Encoding Rules) to deal with PKI service requests, but the operations of BER/DER request more system resources, so it is not fit for WAP equipments. However, WPKI protocol adopts WML and WMLSCrypt to deal with PKI service request. Comparing with traditional methods, function of Sign-Text in WML and WMLSCrypt can save much system resources when coding and putting in PKI service request.

The above parts have different functions for realizing security of wireless network application, where, as basic establishment platform of security, WPKI is the base to effectively implement security protocol and any applications based on identity validation need supports of WPKI. It can combine with WTLS, TCP/IP and WML Script Sign to implement functions such as identity validation, key signature and so on.

## **5. Application model**

According to different situations of linking among wireless terminal, WAP gateway and content server, WPKI can offer three security models.

- (1) Model WTLS Class2. Its terminal needs validating server.
- (2) Model Sign Text. Both the terminal and server need validating each other and use the mode of application layer signature.
- (3) Model WTLS Class3. Both the terminal and server need validating each other and use the mode of “challenging password”.

### *5.1 Model WTLS Class2*

The security layer in WAP system is called wireless security transport layer that is WTLS, which main aim is to offer secrecy and integrity of validation and data for two communication applications. The functions of WTLS are similar to TLS1.0, but it involves some new characters such as data report support, optimizing handshake negotiation, dynamically updating key, and optimizing longer time-lapse narrow bandwidth network. WTLS Class2 can make users validate identities of commutation gateways with it. Figure 2 is the summarization of necessary steps to start WTLS Class2. As Figure 2 shows, the terminal equipments preinstall some CA root certification information.

WAP gateway produces key pair, the public key and key, and implements the following steps.

- (1) The gateway sends validation request to PKI portal.
- (2) The portal confirms the identity and transfer the request to CA.
- (3) CA sends gateway public key certificate (maybe through portal) to the gateway.
- (4) The mobile terminal and gateway establish WTLS conversation.
- (5) The gateway and server establish SSL/TLS conversation.
- (6) The server sends certificate request to PKI portal, the portal confirms ID and transfers the request to CA.
- (7) CA sends server public key certificate (WTLS certificate) to the server.
- (8) The mobile terminal and server establish WTLS conversation.

### *5.2 Model Sign Text*

The terminal equipments and server in model Sign Text must preinstall (or load) CA root certificate.

The steps to establish security communication are seen in Figure 3. The operation process of model Sign Text includes following steps.

- (1) The mobile terminal applies for certificate to PKI portal.
- (2) The portal confirms the identity and transfer the request to CA.
- (3) CA produces user’s certificate and sends URL of the certificate to user (the other method is that CA sends the whole user’s certificate to the equipment, for example, CA can store it in WIM).
- (4) CA put user’s public key certificate in the database (if necessary).
- (5) User signs affair on client post (Sign Text offers a sort of mechanism which sets up digital signature by the mode of WML Script for user equipments), and sends affair, signature and certificate URL (or certificate) to the server.
- (6) The server takes user’s certificate from the database by certificate URL.
- (7) The certificate database of CA sends user’s certificate to the server.

### *5.3 Model WTLS Class3*

As viewed from PKI, WTLS Class3 (see Figure 4) validation and model Sign Text are almost same, and the difference is in step 5. In this step, model Sign Text uses the mode of application layer signature to complement validation, that is to say, user must confirm the readable message from the server and attach its own digital signature, then sends it to the server for validation, where the using key pair must be the key specially used for digital signature and the message from the server must be readable, however, the model WTLS Class3 validates “challenging password” from WTLS server through user key, which “challenging password” means that the server sends some random numbers to the user and these numbers may not be readable information and need user’s signature to validate user’s identity.

The operation process of model WTLS Class3 includes following steps.

- (1) WAP sends a certificate request to PKI portal through the gateway.
- (2) The PKI portal confirms the identity and transfer the request to CA.
- (3) After CA signs the certificate, it sends the certificate to the WAP terminal through WAP gateway, and at one time, CA

stores the WAP certificate into the certificate database.

- (4) The WAP terminal signs in the dealing affair data, and sends dealing data, signature and certificate to the source server.
- (5) The source server validates the signature, and if the certificate keeps to the URL mode, the following two steps are needed.
- (6) The source server lookups in the certificate database according to the position appointed by URL.
- (7) The certificate database returns the certificate to the source server.

**6. Application example**

The example model is to utilize WPKI technology to simulate cell-phone terminal to offer charging and inquiring services for one card through campus.

The flow of application model is seen in Figure 5. Students input some authorized information such as sequence number or code and bank accounts or code using short message through cell-phone terminal, the cell-phone terminal transports encrypted message to the WAP gateway, when the WAP gateway receives a request, it sends a certificate request to PKI portal for confirming identity and then transfer CA to complete certification signing, where, one certificate is sent to the cell-phone terminal, the other one is sent to the application server, and the WAP gateway also needs send the executive order information to the server of short message, the short message server transports it to the application server through SSL, the application server validates the received information utilizing received digital certificate, then completes needed charging or inquiring services, finally it will send the executive results after encrypting to the cell-phone terminal through the short message server, if the validation is not successful, it will directly return the encrypted wrong information to the cell-phone terminal through WAP gateway.

**7. Application prospect**

The network security is a complicate research domain with application values. With the popularization of computer application, the network security becomes more and more important. And WPKI just adapts these requests for the applications of wireless network security. The network security needs consider many aspects which mainly include security strategy and security technology. With the development of wireless network security, the future development of WPKI technology must be possess more characters including standardization, internationalization, commerce and centralization to fulfill various requests from the developing applications of wireless network.

**References**

Chen, Xiang, Zhuang, Yi & Wu, Xuecheng. (2006). Research on elliptic curves cryptosystems and the application of ECC to wireless public key infrastructure. *Computer Engineering and Applications*. 42(5). p.110-112.

Madge. (2002). White paper: wireless LAN security. [Online] Available: [http://www.madge.com/\\_assets/documents/guides/wlansecurity.pdf](http://www.madge.com/_assets/documents/guides/wlansecurity.pdf).

Wireless Developer Network. (2007). Introduction to the wireless application protocol. [Online] Available: <http://www.wirelessdevnet.com/channels/wap/training/wapoverview.html>.

Huang, Lu. (2004). *The Application of WPKI on M-Commerce Security*. Master Paper of Jiangnan University.

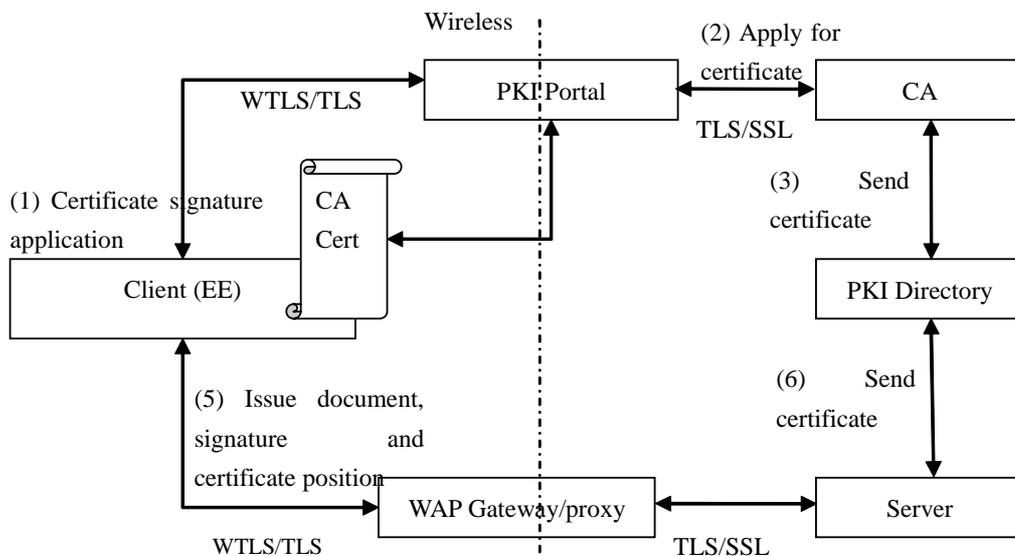


Figure 1. Structure of WPKI

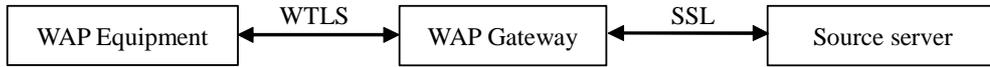


Figure 2. Model WTLS Class2

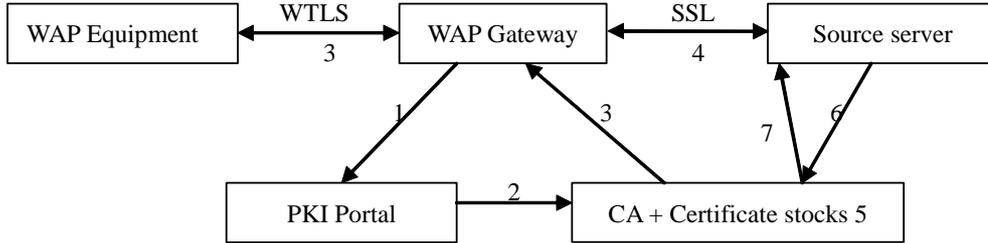


Figure 3. Model Sign Text

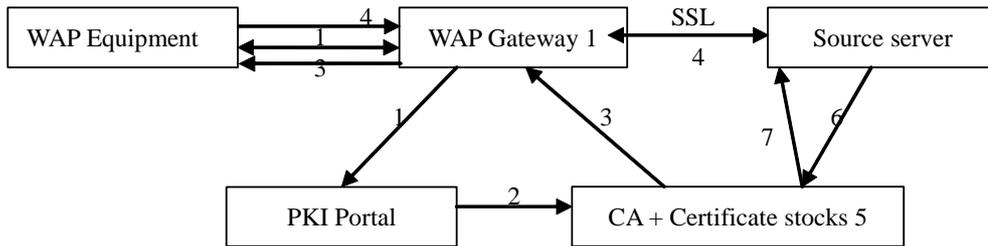


Figure 4. Model WTLS Class3

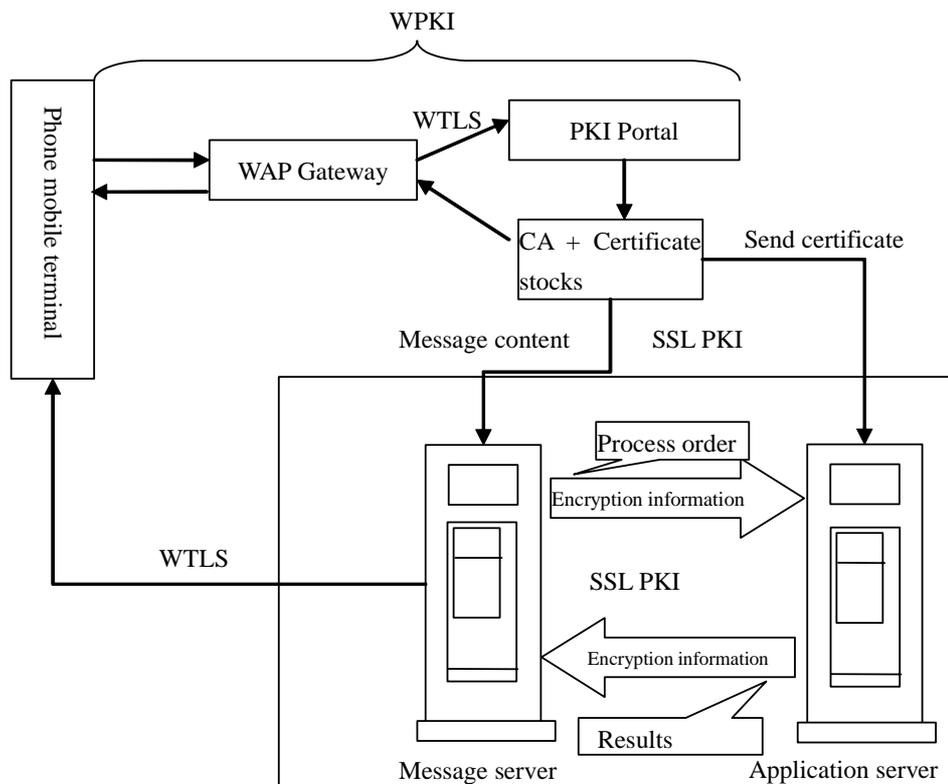


Figure 5. Flow of Application Model