White Paper on :
Importance and Issues of Implementing Public Key Infrastructure for Mobile Payments

Shaik Shakeel Ahamad and V.N.Sastry
IDRBT, Road No.1, Castle Hills, Masab Tank, Hyderabad 50057, AP
vnsastry@idrbt.ac.in

Abstract

This paper is prepared for deliberations by the MPFI for enhancing the security aspects of payment systems. It presents the existing set of Public Key Infrastructure (PKI), its functions and challenges. We highlight the difficulties of using the existing PKI in Mobile Payments. We present the issues of securing Private Keys and Certificates in the SIM of the Mobile Phone. The Question of whether a separate Certifying Authority (CA) is needed for Mobile Commerce or the existing CA can be upgraded to adopt the challenges of its implementation for Mobile Payments. We also present what are the issues that may arise if we adopt wireless PKI for enhancing security in Mobile Payments.

1Q) What are the working Principles of PKI System and how it can be implemented?

1A) Public Key Infrastructure (PKI) consists of a set of policies, processes, software, hardware and technologies that use public key cryptography and the certificate management to secure communication. PKI's trusted services enable secure transfer of information and support a wide variety of E-Commerce Applications.

a) PKI ensures Confidentiality, Integrity, Authentication and Non-repudiation.
b) PKI has the following components I) Certificate Authorities (CA), II) Registration Authorities (RA), III) Certificate Holders, IV) Repositories of Certificate Revocation List (CRL).
c) PKI ensures legal sanity of digitally signed agreements. Identities are usually established by issuing Digital Certificates by the Certification Authority (CA) that provide a public key with an end user's terminal or an application server.
d) For the effective implementation of PKI the legal system of the country must support.
e) In India PKI is implemented and managed by Root CA under the control of Central Government of India based on IT ACT 2000.The root CA of a country aligns to the international CA.
f) There are seven CA's operating in India appointed by the Root CA.
g) IDRBT is one of the seven certifying Authorities in the country, which issues certificates to Banks and Financial Institutions.

2Q) What are the issues and difficulties we face if we extend Wired PKI for Mobile Payments?

2A) a) Although PKI does not restrict the medium of communication as wired or wireless a PKI is considered wireless when at least the client devices that are employed by the end users to communicate with other parties are in wireless mode.

b) If Wired PKI is used in Mobile Communications then it has to work in an environment with less powerful CPUs, less memory, restricted power consumption, smaller display and diverse inputs devices. Despite these shortcomings, the wireless equipment must be able to generate and register keys, manage end user mobile identities, encrypt and decrypt messages, and receive, verify, store and send certificates/digital signed data.

c) It is very difficult to implement traditional PKI functionalities such as generate, store and allow access to a user's public key pair and complete, sign and submit first time certificate applications, certificate renewal requests, and certificate revocation requests, and search for and retrieve certificates and revocation information, validate certificates and read the certificate contents and generate and verify digital signatures on Mobile Phones.

e) The method used to handle service requests in Wired PKI relies on the ASN.1 Basic Encoding Rules (BER) and Distinguished Encoding Rules (DER). BER/DER require more processing power, which are scarce in Mobile Phone so Wired PKI in its present form cannot be used for Mobile Commerce.

f) Wired PKI Signature Schemes demand more processing, memory, and storage resources, which are scarce in Mobile devices. Elliptic Curve Cryptography (ECC) techniques are recognized as the most optimized, and therefore the best suited for supporting security in the wireless environment. The keys for elliptic curve are typically of the order of six times smaller than the equivalent keys in other signature schemes, for example 164 bits vs. 1024 bits (RSA).

g) Wired PKI certificates are bigger so it is very difficult to accommodate these certificates on the Mobile device.

h) Certificate Management Protocol (CMP) of wired network is based on Secure Sockets Layer (SSL) which is heavy (92K bytes) so it is not suitable for Resource Constrained devices.

i) Wired CA will be over burdened because they have to maintain short-lived certificates, maintain CRL separately because short-lived certificates expire after crossing their allotted time and they have to work in coordination with Mobile service providers which is very difficult for PKI.

Due to the above reasons it is very difficult to apply Wired PKI for Resource Constrained handheld mobile devices.

3Q) In which part of the SIM (Subscriber's Identity Module) can the Private Key is stored?

3A) **Wireless Identity Module (WIM):** The Wireless Application Protocol (WAP) identity module is a tamper-resistance computer chip that optionally resides in the WAP enabled device such as mobile phones and Personal Trusted Device. It can store key material like the PKI root public key and user's private key. WIMs are most commonly implemented using smart card chips. Smart card chips have memory and storage for data and programs.

a) The WIM is used to protect permanent, typically certified, private keys. The WIM stores these keys and performs operations using these keys. The operations are (i). signing operation (eg, ECDSA or RSA) for client authentication when needed for the selected handshake scheme. (ii) key exchange operation using a fixed client key (eg, ECDH key, in ECDH_ECDSA handshake). So, the private keys never leave the WIM [9].
b) The WIM may store needed certificates: CA and user certificates. Storage of trusted (root) CA certificates has significance also from security point of view: they must not be altered – but they can be exposed without danger. CA certificates may be stored by WIM issuers, or by a user at a later time. If there are many certificates, there may be a need to store them in the phone. Anyway, they are subject to change. So, the phone should be able to download new certificates over the air and store them itself or save them in the WIM [9].
c) From security point of view, there is no requirement of storing user certificates in a tamper resistant place. Storing certificates in the WIM may be useful from logistics and portability view points. It is noted that in Wireless Transport Layer Security (WTLS), the server may retrieve a client's certificate from its own sources. Also, it is possible to store a certificate URL (instead of the certificate itself) in the WIM. The WIM maintains information on algorithms that it certificate itself) in the WIM. The WIM maintains information on algorithms that it supports. The mobile phone retrieves that information from the WIM [9].
d) Permanent key pairs may be generated in the WIM or stored there as a part of the manufacturing or personalization process. However, key generation is not specified in the current version in page no 17 of [9] Specification. It is anticipated that key pairs are generated as a part of the personalization process.

4Q) Do we need a Separate Certifying Authority (CA) for Mobile Communications?

4A) No, we do not need a separate PKI for Mobile Payments because of the following reasons

a) The role of existing CA can be enhanced because according to WAP PKI specification released by OMA (Open Mobile Alliance) in which states that "The goal of the WAP PKI is to reuse existing PKI standards where available, and only develop new standards where necessary to support the specific requirements of WAP" [1].
b) WPKI is not an entirely new set of standards for PKI it is an optimized extension of traditional PKI. WPKI is primarily concerned with the policies that are used in E-Business and security environment by WTLS/TLS and WMLSCrypt in the wireless environment. In

the case of wired networks, IETF PKI standards are the most commonly used, for wireless networks, WAP Forum WPKI standards are most commonly used.

c) Existing CA has to issue Short lived and mini-certificates for WPKI in addition to X.509 for wired PKI.
d) Existing CA has to work in co-ordination with mobile network operators because security keys, certificates etc are stored in SIM, which is usually issued by mobile network operators.
e) Existing CA needs to develop new standards and procedures for mobile devices for their smooth functioning and M-Commerce applications.

5Q) In order to implement Wireless PKI in Mobile Payments what needs to be done for enhancing security?

5A) a) Select optimal digital signature algorithms to be stored and computed in mobile phones.

For digital signature, computation of public key pair generation, digital signature generation and verification in mobile phone are required. RSA based public key cryptographic algorithms may not be suitable with the present commonly available technology for Mobile Phones because public key pair generation based on RSA algorithm in a mobile phone might be time consuming or be impossible due to the lack of sufficient memory and CPU performance. Therefore alternative public key algorithm to make the key generation possible in the mobile phone is required. After a public key pair is generated, the mobile phone must perform computation for digital signature generation and verification, and time limit for digital signature operation must be acceptable to users [3].

b) Minimize data size to be stored in mobile phone and to be transmitted through wireless bandwidth.

The major data storing and processing requirement in a mobile phone are certificate and CRL. Generally, a certificate used in PKI is ITU X.509 certificate defined by ITU. This X.509 certificate has basic fields for certificate verification and many extension fields that are required for certificate path validation. These extension fields increase size of the certificate and make procedures of certificate path validation complex .In order to validate X.509 certificate, CRL verification is also required. To do this, a mobile phone has to download CRL from CA, and check if a certificate is in CRL. This procedure adds cost on the mobile phone and wireless transmission. For this an efficient and reliable method is needed to validate X.509 certificate without direct verification of CRL in mobile phone [3].

c) Optimize Certificate Management Protocol (CMP) to be processed in mobile phone and through wireless bandwidth.

Current wired CMP is based on SSL and certificate request in WAP is based on WTLS. Since security protocol based on WTLS in WAP does not support end-to-end security. In that scheme, information necessary for the certificate request can not be securely transferred to CA. Therefore, new wireless CMP (WCMP) that is based on neither SSL

nor WTLS and is performed by itself is required. The WCMP must guarantee the same functions as wired CMP. This protocol should be more lightweight than wired CMP, and be optimized for processing in mobile phone and feasible for wireless transmission [3].

d) Optimize certificate validation scheme.

To validate X.509 certificate, certificate chain and CRL must be acquired, and verified in mobile phone. Certificate path validation scheme is little complicated and difficult for mobile phone to process. Hence efficient and reliable method for certificate path validation is needed that is possible for mobile phone to process. There are several candidates such as applying the delta CRL scheme to reduce CRL size to download. Also, the certificate validation procedure might be optimized, or certificate validation scheme might be delegated to a trust system [3].

6Q) What is Certificate Validation and how Certificate Validation is achieved in WPKI?

6A) Certificate Validation contains the following steps

a) Verifying the integrity and authenticity of the certificate by verifying the digital signature of CA on the certificate.
b) Verifying the validity period of the certificate.
c) Verifying that the certificate is revoked or not.

There are two methods to validate certificate s in WPKI environment. They are

a) Using OCSP (Online Certificate Status Protocol)
b) Using Short Lived Certificate.

a) Using OCSP (Online Certificate Status Protocol)

Verifying the integrity and authenticity of the certificate involves verifying the digital signature of the CA on the certificate using CA's public key. So for verification of digital signature mobile user delegates this verification process to OCSP server which verifies the digital signature on behalf of the mobile user.

OCSP checks the validity period of the certificate.

OCSP checks the revocation status of the certificate from CRL (Certificate Revocation List).

b) Using Short Lived Certificate

Short Lived Certificates will not have extensions attributes in the certificate. The certificate is lightweight (i.e. it contains important attributes). The validity period of the SLC is less (i.e. 7 or 10 days). Certificate Validation using Short Lived Certificates is done as follows

Mobile phones will verify the digital signature of CA on the certificate using its resources.

Mobile user should check the validity period of certificate from WPKI certificate.

Mobile user need not check the revocation of certificate from CRL because the validity period of WPKI certificate is very less.

7Q) What is the use of Short-Lived WTLS Certificates?

7A) WAP applications require a server certificate revocation capability, to ensure that, in the event a server is compromised or decommissioned, users cannot unwittingly continue to execute what appear to be valid, secured transactions with a rogue server. Wireless devices typically do not have the local resources nor the communication bandwidth to implement revocation methods used in the wired world such as Certificate Revocation Lists (CRLs) or the Online Certificate Status Protocol (OCSP) [1].

To satisfy revocation requirements, WTLS servers may implement the short-lived certificate model, as the means of satisfying revocation requirements. With this approach, a server or gateway is authenticated once in a long-term credentials period – typically one year – with the expectation that the one-server/gateway key pair will be used throughout that period. However, instead of issuing a one-year validity certificate, the certification authority issues a new short-lived certificate for the public key, with a lifetime of, say, 48 hours, every day throughout that year. The server or gateway picks up its short-lived certificate daily and uses that certificate for client sessions established that day. If the certification authority wishes to revoke the server or gateway (e.g., due to compromise of its private key), it simply ceases issuing further short-lived certificates. Clients (in this case, WTLS servers) will no longer be presented with a currently valid certificate; hence will cease to consider the server authenticated [1].

8Q) Differences between Wired PKI and Wireless PKI?

8A)

Wired PKI	Wireless PKI
User needs to store his credentials (private key and Certificate) in hardware token/ smart card.	Credentials are stored in the SIM of the Mobile phone
Storage space is more in the desktop	Storage space is less in mobile phone & SIM, so in order to consume less space in SIM URL of its certificate is stored instead of original certificate along with its private key.
Uses X.509 certificate containing all the fields and extension fields with a reasonable validity period.	Uses Short lived certificates with fewer fields, without extension fields & with less validity period.
RSA (2048 bits) & ECDSA (163 bits) digital signature algorithms can be used to generate & verify digital signatures.	ECDSA is an optimal digital signature algorithm for resource constrained devices like mobile phones because of its key length (163 bits) and it takes less time to generate public key pair in mobile phone than RSA because of its key size. Due to the small size of the key the certificate size is also reduced.
Certificate validation is done by the user using his desktop	User delegates certificate validation function to OCSP thereby avoiding the burden of CRL download and storage as well as the complicated procedure to acquire and verify the certificate chain.
WPKI test environment **For Desktop** CPU Pentium IV 700 MHz Memory 256 Mbytes OS Win2000	**WPKI test environment** **For Mobile phone** CPU ARM7TDMI 13.5 MHz Memory 2 Mbytes OS REX
Comparison of ECDSA processing time in desktop Key generation 3 ms Digital Signature generation 3ms Digital Signature verification 3.6ms	**Comparison of ECDSA processing time in mobile phone** Key generation 1200 ms Digital Signature generation 1200ms Digital Signature verification 2500ms

Abbreviations:

CMP	Certificate Management Protocol
WTLS	Wireless Transport Layer Security
WIM	Wireless Identity Module
WAP	Wireless Application Protocol
OCSP	Online Certificate Status Protocol
CRL	Certificate Revocation List
CA	Certification Authority
PKI	Public Key Infrastructure
WPKI	Wireless Public Key Infrastructure
SIM	Subscriber's Identity Module
BER	Basic Encoding Rules
DER	Distinguished Encoding Rules
ECC	Elliptic Curve Cryptography
SSL	Secure Socket Layer
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
URL	Uniform Resource Locator
RSA Alg	Rivest-Shamir-Adleman Algorithm
SIM	Subscriber's Identity Module
RA	Registration Authority
OMA	Open Mobile Alliance

References:

1) "WAP Public Key Infrastructure Definition," WAP Forum, WAP-217-WPKI, Version 24-Apr-2001. URL:http://www.wapforum.org/

2) OMA, WAP Certificate and CRL, WAP-211-X.509, March 2000. URL:http://www.wapforum.org/

3) Yong Lee, Jeail Lee, JooSeokSong, Design and implementation of wireless PKI technology suitable for Mobile phone in Mobile Commerce in Computer Communications 30 (2007) 893-903.

4) Marko Hassinen, Konstantin Hypponen, Elena Trichina, Utilising national public-key infrastructure in mobile payment system, Electronic Commerce Research and Applications 7 (2008) 214-231.

5) OMA, Wireless Transport Layer Security, WAP-261-WTLS, April 2001

6) OMA, Wireless Application Protocol Architecture Specification, WAP-210-WAPARch, July 2001. URL:http://www.wapforum.org/

7) M.Myers, R.Ankney, A.Malpani, S.Galperm, C.Adams, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP): IETF Network Working Group, June 1999.

8) R.Housley, W.Polk, W.Ford, D.Solo, Internet X.509 public key Infrastructure Certificate and Certificate Revocation List (CRL) Profile: IETF RFC 3280, IETF Network Working Group, April 2002.

9) OMA, Wireless Identity Module, Part: Security, Version 12 July 2001. URL:http://www.wapforum.org/