Proposing a Wireless PKI Model Optimized for M-Commerce Applications

Fariborz Mousavi MADANI, Iran BIMAR

Abstract—**The rapid advances in wireless mobile communication technology and the growth of e-commerce applications have naturally led to the development of e-commercial services on wireless medium through mobile phones. As more mobile devices are developed, security issues of crucial importance to the wired environment are resurfacing and creating a similar degree of impact. PKI which assures security issues in wired networks has difficulties to be implemented in wireless medium due to the limited performance of mobile phone such as less memory and less powerful CPU. Therefore a wireless PKI customized to mobile phone is needed. In this paper we present a wireless PKI for mobile phone based on the work presented in Ref [1].**

Keywords— **Mobile phone, M-Commerce, Wireless Public Key Infrastructure, Digital certificate, SCVP.**

I. Introduction

MOBILE wireless telephones, or cell phones, are those who have shortwave analog or digital transmission capabilities that allow users to establish wireless connections to nearby transmitters. Today's cell phone is rapidly evolving to integrate with PDAs, thus providing users with increased wireless email and Internet access. Mobile phones with information-processing and data networking capabilities make a new field of study named Mobile Commerce. Mobile commerce is an electronic commerce contains some services and applications, brought to mobile users via mobile devices such as palmtops, PDAs. In order to deliver these mobile services and applications over the Internet in a secure, scalable and manageable way, new architectures and protocols customized to wireless internet are essential. Basic Security services defined in the literature [1]-[10] are confidentiality and integrity of data, authentication, and non-repudiation. Architectures and protocols customized to wireless Internet must fulfill these services as those in the wired Internet. Nowadays many security protocols on Internet and most security applications for e-commerce are based on public key cryptography [1]. Public key infrastructure (PKI) is an integrated secure platform based on asymmetric encryption, with a collection of mechanisms for creating, distributing and using public key certificates to transmit user's public key and user's identity in a secure and reliable way. Its combination with wireless network technology leads to the wireless PKI (WPKI).

School of Engineering, Alzahra University, Tehran, Iran.
mosavif@alzahra.ac.ir, iran_bimar@yahoo.com

WPKI optimizes the traditional PKI and applies it to the wireless environment. Mobile phones have many limitations of screen size, input utility, processing power and memory. Especially, the processing power of many mobile terminals is quite limited. This must be taken into account when cryptographic algorithms are chosen. Therefore, the number of cryptographic algorithms must be minimized and small-sized algorithms must be chosen to reduce RAM requirements as low as possible [1], [2]. Wireless data network presents more constrained communication environment such as less bandwidth and has different protocol compared to wired internet protocol. In this paper, we propose a Wireless Public Key Infrastructure (WPKI) model for mobile commerce. For this purpose we will make some enhancements in WPKI model presented in [1]. Section 2 introduces public key infrastructure, its problems and limitations in mobile phone. In Section 3 we describe the reference WPKI model, its limitations and propose an enhanced model to acquit limitations. The performance of the proposed WPKI is analyzed in Section 4. Section 5 concludes this paper.

II. PKI and Its Limitations

Public key infrastructure (PKI) is an integrated secure platform based on asymmetric encryption, with a collection of mechanisms for creating, distributing and using public key certificates to transmit user's public key and user's identity in a secure and reliable way. In the PKI's entities show in Figure 1, Certificate and CRL forms the core of PKI, hence verifying the correctness of certificate is a fundamental building block for public key applications. While digital certificates provide a secure mechanism to identify and authenticate an entity via the verification of a digital signature, there must also be mechanisms in place to validate that certificate and the associated private key. This issue is commonly known as certificate validation and is based on the concept of certificate revocation. Certificates may be revoked for various reasons, including, but not limited to, change of name, change of association between subject and CA and compromise or suspicion of compromise of the corresponding private key. There must be mechanisms in place for a requesting entity to retrieve status information of a certificate that may have been revoked. One method, as defined by [RFC3280] defines the concept of certificate revocation lists (CRLs) that are used to convey information about certificates revoked by a Certification Authority (CA). Although CRL's are in use in many environments, they have some properties that make their

use in mobile environments unattractive [6]. In particular, the use of CRL's requires additional processing by the client that may be difficult to implement in a constrained mobile device. Also, CRL's are often quite large in size and thus raise network latency and bandwidth issues [6].

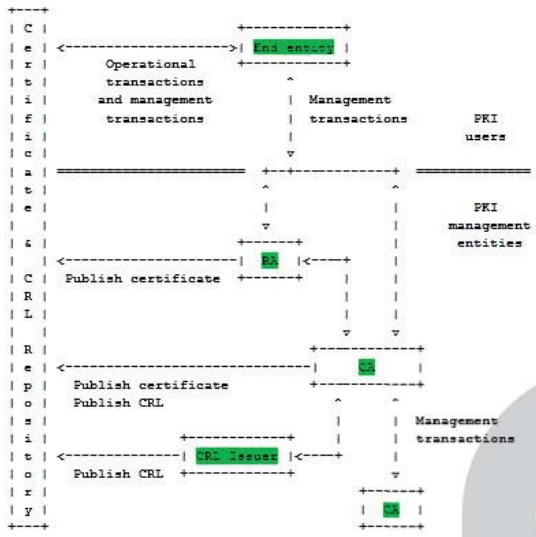

Fig. 1. PKI entities

The explosive growth of the Internet has fuelled the creation of new and exciting information services. Mass-market, hand-held wireless devices present a more constrained computing environment compared to desktop computers. Because of fundamental limitations of power and form-factor, mass-market handheld devices tend to have [7]:

- Less powerful CPUs
- Less memory (ROM and RAM)
- Restricted power consumption
- Smaller displays
- Different input devices (e.g., a phone keypad)

Similarly, wireless data networks present a more constrained communication environment compared to wired networks. Because of fundamental limitations of power, available spectrum, and mobility, wireless data networks tend to have [7]:

- Less bandwidth
- More latency
- Less connection stability
- Less predictable availability

In order to apply wireless PKI to mobile phone through wireless internet with the same level of security as that of wired internet, the following requirements must be satisfied [1]:

- Select optimal digital signature algorithm to be calculated in mobile phone
- Minimize data size to be stored in mobile phone and to be transmitted through wireless bandwidth
- Optimize CMP protocol to be processed in mobile phone and through wireless bandwidth
- Optimize certificate validation scheme

III. WPKI Architecture

In this model, Yong Lee and her co-workers apply X.509 certificate as certificate of mobile phone, because verification of mobile certificate is not difficult in the server with adequate performance. Assumptions of this model are:

- Communication is between mobile phone and server as content provider, and excludes communication between mobile phones
- This model has one CA
- End entity such as a mobile phone or server has only one public key pair and one certificate for one purpose

In this model, as Figure 2 shows, CA issues a certificate, publishes its directory, and sends only URL of the certificate to the mobile phone. When a mobile phone communicates with server, the mobile phone sends URL of the certificate to server, not the certificate itself.

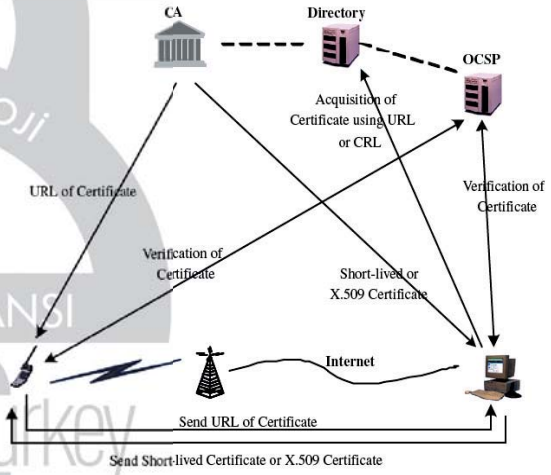

Fig. 2. WPKI model

The server can easily access the directory and acquire the certificate. Authors introduce Online Certificate Status Protocol (OCSP), and the mobile phone delegates OCSP to validate certificates rather than validation in the mobile phone by itself.

For digital signature algorithm, mobile phone cannot measure the generation time of RSA 1024-bit public key pair because it takes so long time. Thus, the alternative digital signature algorithm with same security level was required and they chose ECC-based Elliptic Curve Digital Signature Algorithm (ECDSA) that is recommended by [8] and [9]. For ECDSA 163-bit key size, equivalent to RSA 1024- bit key size; it takes shorter time to generate public key pair in mobile phone than RSA algorithm [1].

For Certificate and CRL profiles they describe Wireless X.509 certificate profile issuing for mobile phone and server, and short-lived certificate profile issuing for server to reduce

verification load of mobile phone. X.509 certificate consists of basic field and extension field. To reduce size of certificate they omitted some extension fields. Their profile defines that names should not be reused for different entities and CAs conforming to this profile should not generate certificates with unique identifiers. Authority key identifier and subject key identifier are used to identify the public key where an issuer and/or subject have multiple signing keys. The private key usage period extension allows the certificate issuer to specify a different validity period for the private key than validity period of the certificate. They also assume that the private key usage period is same as the validity period of the certificate and do not use this extension. For the issuer alternative names extension, because they assume one CA, this extension was omitted. The extended key usage indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension. Since applying OCSP for certificate validation in this model, they use domain information and authority information access extension for specifying how to access of OCSP server. How a mobile phone securely requests a certificate to CA and CA issues it to the mobile phone in this model? They consider that the followings are requirements of certificate request protocol as mentioned in [10]:

- Certificate request message is constructed at mobile phone. This value should include a public key, end-entity's reference number like as ID and password. They assume that other requested certificate fields, and additional control information related to the registration process are made in out-of-band
- A POP (Proof of Possession) of the private key corresponding to the public key for which a certificate is being requested value is included in certificate request massage
- Method that the certificate request message is securely communicated to a CA

To satisfy these requirements, they designed wireless certificate management protocol and developed this protocol on mobile phone. Since a password could be transferred to a CA by hash value, confidentiality of the password could be guaranteed. They use the public key as one time information for prevention of replay attack.

For short-lived certificate, the mobile phone validates the certificate through verifying only signature and valid period in the certificate. The server acquires a certificate from directory using URL of the certificate received from the mobile phone, and sends mobile phone its certificate with CA's certificate and ARL (Authority Revocation List) together.

The assumptions made in this model require us to have just one CA. So if the number of CAs exceeds one, certification path cannot be supported. Moreover, an entity is forced to have just one certificate. So limitations of this model are summarized as:

- No more than one CA
- No more than on certificate for mobile user

Having one CA decreases flexibility of the model. Because lots of organizations have their own rules which rises consistency issues. Also, it is difficult to convince all users to take their certificates from one CA. This model is more suitable for domestic markets due to limitations of one CA and one certificate per user.

A. The Proposed WPKI Architecture

In this section we briefly describe Server-Based Certificate Validation Protocol (SCVP) as an alternate for Certificate Validation Scheme in this model. As Figure 3 shows, we substituted OCSP with SCVP.

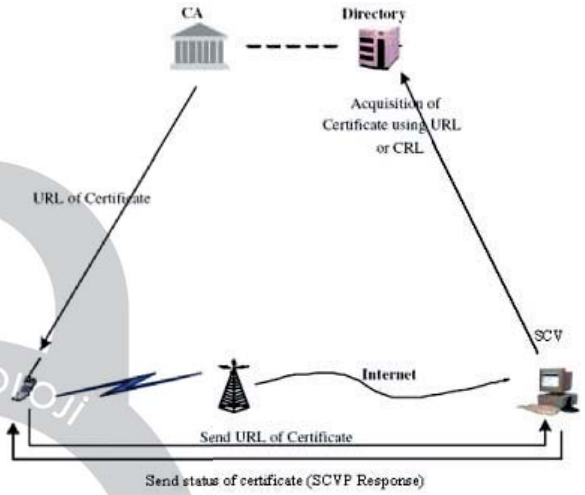

Fig. 3. SCVP Based WPKI

The Server-Based Certificate Validation Protocol (SCVP) allows a client to delegate certification path construction and certification path validation to a server. The path construction or validation (e.g., making sure that none of the certificates in the path are revoked) is performed according to a validation policy, which contains one or more trust anchors [9]. It allows simplification of client implementations and use of a set of predefined validation policies. With this protocol we can exclude the assumption of having one CA from Model.

B. SCVP

As we mentioned before mobile phone is burdened with the overhead of constructing and validating the certification paths. SCVP reduces this overhead for two classes of certificate-using applications [9]. The first class of applications wants just two things: confirmation that the public key belongs to the identity named in the certificate and confirmation that the public key can be used for the intended purpose. Such clients can completely delegate certification path construction and validation to the SCVP server. This is often referred to as delegated path validation (DPV).

The second class of applications can perform certification path validation, but they lack a reliable or efficient method of constructing a valid certification path. Such clients delegate certification path construction to the SCVP server, but not validation of the returned certification path. This is often referred to as delegated path discovery (DPD) [9]. In

constrained execution environments, such as telephones and PDAs, memory and processing limitations may preclude local implementation of complete, PKIX compliant certification path validation [9]. The Delegated Path Validation (DPV) protocol allows a server to validate one or more public key certificates on behalf of a client according to a validation policy. If the DPV request does not specify a validation policy, the server response must indicate the validation policy that was used. Policy definitions can be quite long and complex. Hence mobile phone can simply reference a validation policy or accept the DPV server's default validation policy. The certificate to be validated must either be directly provided in the request or unambiguously referenced [9]. Based on our WPKI Model, mobile phone prepares URL of certificate in DPV request. The DPV server must have the certificate to be validated. The DPV server must include either the certificate or an unambiguous reference to the certificate (in case of a CA key compromise) in the DPV response [9] and [10].

For the client to be confident that the certificate validation was handled by the expected DPV server, the DPV response must be authenticated, unless an error is reported (such as a badly formatted request or unknown validation policy). There are two mechanisms for validation of SCVP responses [9]:

- Based on the client's knowledge of a specific SCVP server key (simple key validation)
- Based on validation of the certificate corresponding to the private Key used to protect the SCVP response. (SCVP Server Certificate Validation)

The simple key validation method is where the SCVP client has a local policy of one or more SCVP server keys that directly identify the set of valid SCVP servers. Mechanisms for storage of server keys or identifiers are a local matter. For example, a client could store cryptographic hashes of public keys used to verify Signed Data responses. Alternatively, a client could store shared symmetric keys used to verify MACs in Authenticated Data responses. Because of limitation of mobile phone mentioned in the last section, SCVP Server Certificate Validation is not advisable, hence we don't describe it.

IV. Performance Analysis

This section analyzes the performance of the proposed model in comparison to the antecedent Model. At the 163-bit ECC/1024-bit RSA security level, an elliptic curve exponentiation for general curves over arbitrary prime fields is roughly 5 to 15 times as fast as an RSA private key operation, depending on the platform and optimizations [8]. Since the short-lived certificate has excluded from the proposed model, 181 bytes is removed from the model. In certificate validation scheme, SCVP is the best choice for certificate validation to the mobile phone, the mobile phone does not need to acquire CAs certificate and ARL from directory or send short lived certificate to OSCP. This reduces the number of transactions between mobile phone and the wired system through wireless bandwidth. In the proposed WPKI model, the mobile phone has only two stages for certificate validation through SCVP request and response.

Certificate validation cost of the proposed scheme is not increased, compared to the validation cost of the wired PKI. The validation cost of the wireless PKI is same as the cost of the wired PKI in the worst case as follows. In wireless PKI, certificate validation procedure is the same as the wired PKI. To save the cost due to expensive wireless bandwidth, we need to optimize the certificate validation procedure in wireless link. Instead of the procedure that user terminal directly requests and download CA certificate and ARL from directory, after server validate the certificate which mobile phone requested, the server sends the status of certificate to user terminal in the short size scheme. Therefore not only the CA certificate and ARL of the directory are not transferred to the user terminal but also user terminal doesn't do anything more to validate certificate. Thus the cost of direct download of CRL from directory and certificate download from server in user terminal is reduced. Compared to the antecedent model, because SCVP request/response procedure is substituted to OCSP procedure and server, the number of the total transactions is decreased to two and of course the big size of CRL is not transferred through wireless link, so the wireless bandwidth is saved. Also unlike the antecedent model, having more than one CA is conceivable and certificate path validation is available. Also based on [1] comparing wireless CMP to RFC2511 and RFC2510 as the certificate management protocol for wired PKI, the module size of the WCMP is smaller than the wired CMP, nevertheless having the same functionality [1].

V. Conclusion

In this paper, we proposed wireless PKI technology that provides similar security level as wired PKI supporting mobile phone. The proposed wireless PKI model aimed at secure M-commerce based on mobile phone through wireless communication. On the mobile phone with low performance, we selected ECDSA algorithm to reduce the computational complexity of public key algorithm. To reduce the complexity of certificate validation, we suggest the Server-Based Certificate Validation Protocol (SCVP) which allows a mobile terminal to delegate certification path construction and certification path validation to a server.

References

[1] Y. Lee, J. Lee, J. Song, "Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce", Computer Communications, Elsevier, 30 (2007), pp. 893–903.
[2] M. Hassinen, K. Hypponen, E. Trichina, "Utilizing national public-key infrastructure in mobile payment systems", Electronic Commerce Research and Applications, Elsevier, 2007, pp. 214-231.
[3] R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile: IETF RFC3280", IETF Network Working Group, April 2002.
[4] OMA, Online Certificate Status Protocol Mobile Profile Candidate Version V1.0, 27 Jan 2004.
[5] OMA, Wireless Application Protocol Architecture Specification, WAP-210-WAPArch-20010712.
[6] OMA, Wireless Application Protocol Public Key Infrastructure Definition, WPKI WAP-217-WPKI Version 24-Apr-2001.
[7] OMA, Wireless Transport Layer Security, WAP-261-WTLS, April 2001.
[8] K. Lauter, "The Advantage of Elliptic Curve Cryptography for Wireless Security", IEEE Wireless Communications, February 2004 -1536-284/04.
[9] T. Freeman, R. Housley, A. Malpani, D. Cooper, W. Polk, "Server-Based Certificate Validation Protocol (SCVP)", NIST RFC5055, December 2007.
[10] D. Pinkas, R. Housley, "Delegated Path Validation and Delegated Path Discovery Protocol Requirements", RSA Laboratories, RFC3379, September 2002.