An Efficient POP Protocol Based on the Signcryption Scheme for the WAP PKI

Sungduk Kim[1], Kyungjin Kim[2], Jaedong Jung[3], and Dongho Won[1,⋆,⋆⋆]

[1] Information Security Group, Sungkyunkwan University, Korea
netsec@naver.com, dhwon@security.re.kr
[2] Mobile Communication Division, Samsung Electronics, Korea
kjkim.kim@samsung.com
[3] IT Infra. Business Division, KOSCOM Corporate, Korea
jjd@koscom.co.kr

Abstract. WAP Forum recommends to use WTLS handshake protocol and signText() function to certify the POP (proof of possession) of authentication key and signing key. However, it causes plenty of computation and communication overload to mobile devices with low computation and communication power. In this paper, we propose an efficient POP confirmation protocol based on the signcryption scheme, which requires less computation and communication cost. It would be useful for the wireless and wired PKI. The proposed protocol is based on Zheng's signcryption scheme, because it is the first and only signcryption scheme submitted to the international standard institute(IEEE p1363).

Keywords: POP, proof of possession, signcryption.

1 Introduction

POP (proof of possession) confirmation is a cryptographic procedure that CA or RA certifies whether a certificate applicant possesses a proper private key accordance with a public key sent by a certificate applicant. Therefore, the detail steps may differ from the selected algorithm and the purpose of keys [1, 2, 10].

The well known standards relating to POP confirmation are RFC 4210 CMP (Certificate Management Protocols), and RFC 4211 (CRMF : Certificate Request Message Format) of IETF[1, 2, 3, 4]. However, such standards are too complicated to apply to small mobile devices such as cellular phones. There is a specific standard procedure for small devices which was released by the WAP Forum[10, 11].

In conformance with WAP specifications, the POP of authentication key is validated through the PKI portal which is based on a successful WTLS handshake which makes session key such as ECDH key. The POP of a signing key is a signature for the least part of the information (containing a challenge from the

⋆ This work was supported by the University IT Research Center Project funded by the Korean Ministry of Information and Communication.

⋆⋆ Corresponding author.

A.S. Atzeni and A. Lioy (Eds.): EuroPKI 2006, LNCS 4043, pp. 223–232, 2006.
© Springer-Verlag Berlin Heidelberg 2006

PKI portal) and it is generated by the signText() function. Signature may be passed to the PKI portal in the form of signedContents. It consists of a signature and a self-signed certificate(or original signing certificate)[10, 11, 12].

Although the performance of mobile devices has improved rapidly, this approach causes much computation and communication cost and problems. Therefore, we propose an efficient POP confirmation protocol based on the signcryption scheme which is original and only signcryption scheme submitted to the international standard institute(IEEE p1363)[9].

This paper assumes the following situations :

- ECDSA and ECDH scheme are used in the mobile device.
- The mobile device has no user certificate.
- The user requests two certificates simultaneously, applies ECDH for the authentication key, and ECDSA for the signing key.

In this paper, we briefly introduce relating works in section 2(the POP procedure of WAP) and section 3(Signcryption scheme). We propose an efficient POP confirmation protocol based on signcryption scheme in section 4, and analyze the efficiency and security of the proposed protocol in section 5. Finally we make conclusions in section 6.

The following notations will be used in this paper, it is based on the ANSI X9.62[6].

- $X \parallel Y$: Concatenation of two strings X and Y
- n : The order of the base point G
- G : A distinguished point on an elliptic curve of large prime order n, called the base point or generating point
- d_{X_Y} : An elliptic curve private key, X means a owner, and Y means the purpose of key; S is signing, and KM is key management
- Q_{X_Y} : An elliptic curve public key, X means a owner, and Y means the purpose of key; S is signing key, and KM is key management key
- $Cert_{X_Y}$: An elliptic curve public key certificate, X means a owner, and Y means the purpose of key; S is signing key, and KM is key management key
- H : a one-way hash function
- KH_X : A keyed one way hash function. X is a key value
- $[x, y]$: The interval of integers between and including x and y
- $barx$: Convert the field element x to an integer
- ID/PW : one time ID and password issued by PKI portal

2 The POP Confirmation Procedure of WAP

According to the definition of WAP PKI, the PKI portal considers that the user obtain POP confirmation of authentication key when one executes the WTLS protocol and successfully logs in to the PKI portal. The PKI portal considers that the user obtain a POP confirmation for a signing key when a signature of signedContent which is generated by the signText() function is verified by the PKI portal.