Forward Secure Password-Enabled PKI with Instant Revocation*

Seung Wook Jung[1] and Souhwan Jung[2,**]

[1] Institute for Data Communications Systems, University of Siegen
Hölderlinstraße 3, 57076 Siegen, Germany
[2] School of Electronic Engineering, Soongsil University, 1-1, Sangdo-dong,
Dongjak-ku, Seoul 156-743, Korea
seung-wook.jung@uni-siegen.de, souhwanj@ssu.ac.kr

Abstract. Recently the concept of password-enabled PKI is an emerging issue to support user mobility. Virtual soft token and virtual smartcard were proposed as the password-enabled PKI. However, the virtual soft token does not support key disabling. In the virtual smartcard, the user must interact with remote entity per signing operation. In addition, both schemes do not support forward secrecy and instant revocation.

In this paper, we propose a new approach that supports user mobility. The proposed approach supports key disabling and the user does not need interaction with the remote entity for each signature. Moreover, the proposed scheme allows instant key revocation. Thereby, the distribution of CRL is not required. Furthermore, the proposed scheme supports forward secrecy. In this sense, our scheme, implemented only software, is stronger than a long-term private key with physical smart cards. By forward secrecy and instant revocation, signing documents using a timestamp provided by a trusted authority is not required to protect from modifying signed document by the adversary who knows private key.

Keyword: Password, PKI.

1 Introduction

The Public Key Infrastructure (PKI) is the basis of a pervasive security infrastructure for ensuring user's digital identity. However, the user mobility, also called the roaming user, and private key management for the pervasive security is still issue. Ideally, the private key is stored in a hardware smartcard and the user moves amongst multiple PCs. However, in reality, smartcard readers are not available at every computers. Given the cost and availability problems of hardware smartcard, the concept of password-enabled PKI, which relies on passwords to enable the usage of private keys for providing user mobility, is recently focused on by PKI vendors and researchers as an interesting issue for true pervasive security.

* This work was supported by the Soongsil University Research Fund.
** Corresponding author.

A.S. Atzeni and A. Lioy (Eds.): EuroPKI 2006, LNCS 4043, pp. 54–67, 2006.

Recently, to support the roaming user, virtual soft tokens [1][2][3], and virtual smartcards[4][5][6][7] are proposed[5] as password-enabled PKI. Both approaches assume that there exists an online network server.

In the virtual soft token, the private key of a public/private key pair is encrypted with a password and the encrypted private key is stored on an online network server. With the password, the user and the server establish an authenticated and confidential channel using a password-authenticated key exchange protocol [8][9][10], and the user downloads the encrypted private key. The user decrypts it and uses the private key as in the conventional PKI.

In the virtual smartcard, the user's private key is split into two parts: the password that the user holds and the secret component stored in the server. In [4][5][6][7], The RSA private key for which the corresponding public key is (N, e) is split into a password-derived private key d_1 and another value d_2, $d = d_1 \cdot d_2 \bmod \phi(N)$, and d_2 is stored on a server, where d is a private key corresponding to the public key (N, e). Therefore, the user and the server have to communicate for each private key operation (signing or decryption).

The disadvantage of virtual smartcard schemes is that the user interacts with the remote server per signing, while the virtual soft token does not require any interaction after downloading the encrypted private key from the online server. The disadvantage of virtual soft token schemes is that they does not support key disabling, while the virtual smartcard supports key disabling. After receiving the key disabling message, the server will not generate a signature or decrypt a message with given user's private value d_2. Therefore, even though the adversary gets the password, the adversary cannot generate the signature for a given user, after key disabling. However, in both schemes, when the private key is disclosed, the user must revoke the private key and the Certification Authority (CA) has to distribute the Certificate Revocation List (CRL). Otherwise, the adversary can generate the signature for a given user. Furthermore, even though CRL is distributed, the adversary, who knows the private key, can modify the existing signatures that are generated before revocation, if the time-stamp from the trusted third party is not included in the signatures[11].

In this paper, we propose a new scheme for the roaming user. The long-term key of the proposed scheme is the only password and the password is used in a part of a session private key. In the proposed scheme, the CA issues a Master Password Certificate (MPC) that certifies the user's password. For the user mobility, a part of MPC, which is encrypted by the password, is stored in an online server and the other part is stored in an online CA. The user downloads the encrypted part of MPC, decrypts it, and modify decrypted part of MPC. Only the legitimate user, who knows the password, can generate a session private key and can properly modify decrypted part of MPC corresponding to the session private key in order to request Short-Lived Certificate (SLC) to the online CA. After receiving the SLC, the user does not need interaction with any entity for signature function.