Internet Draft
Document: draft-choi-pkix-ui-03.txt
Expires: December 8, 2005

B.H. Park
J.H. Yoon
I.K. Jeon
H.G. Lee
J.I. Lee
KISA
June, 2005

# Required functions of User Interface for the Internet X.509 Public Key Infrastructure <draft-choi-pkix-ui-03.txt>

## Status of this Memo



## Copyright Notice



## Abstract

This document provides guidance to PKI client software developers on what required functions are needed on user interface of PKI client

software for human users to generate and verify digital signatures easily and securely.

## 1. Introduction

Even though PKI is one of the most secure and influential technologies to offer information security, most people say that it is difficult to understand and utilize PKI technology because PKI gives responsibilities for "human users"(users) to manage their certificates and private keys.

General users of PKI technology generate their digital signature and verify digital signatures by taking those responsibilities at the application level. At this time, the users are usually directed by user interface of PKI client software. Actually, they do not have to know the whole mechanism of how PKI client software works, but they just want to manage and use their certificates and private keys with an aid of user interface keys and with any convenience.

However, businesses have so far neglected requirements for user interface of PKI clientsoftware because most PKI technologies are focusing on CA implementation. Consequently, the reason of people's giving up accepting PKI technology is not difficulty of the very PKI technology, but unkind user interface of PKI client software.

On the other hand, kind user interface should join in the following processes of PKI client software when users generate and verity digital signatures. First, user interface of PKI client software shows users' certificates and private keys without users' involvement in order that users can generate digital signatures with their certificates and keys regardless of sorts of PKI applications. Second, user interface gives access to users' certificate information and enables users to manage their certificates without complexity of user interface. Lastley, user interface uses the certificate of users' trust anchor when the client software verifying digital signatures. These processes can be implemented through core required function that the PKI client software offters to users.

Thus, this document provides core required functions of user interface when users generate and verify digital signatures so that more users can utilize kind PKI technology. As for these functions are certificate sharing function, import and export function, certificate handling function, automatic update function, and integrity verification function.

## 2. Required functions

This section defines core required functions of user interface when users generating and verifying digital signatures.

### 2.1 When generating digital signatures

Users use their own certificates and private keys provided by user interface of PKI client software when generating digital signatures. Thus, user interface should assist users to find and use their certificates and private keys without any inconvenience when PKI applications are operating. In other words, user interface should provide the following compatibility and usability when users try to generate digital signatures.

Compatibility shall be accomplished for using one certificate to many PKI applications. Generally, PKI application such as the Internet Banking or E-mail application defines the user's certificate and private key location by their own way. Thereby, when using those applications, users are at a loss whenever receiving a question where their certificates are. Most users do not know the answer, and they want to use different PKI programs with their own certificate without answering the question. It comes true as a certificate sharing function and transfer function that mainly aim for increasing certificate compatibility, which benefits the user's convenience.

Usability shall be considered for a user who does not know about any PKI knowledge to use PKI services by managing his or her certificates easily. In this section, it specifies certificate handling function of storage media and automatic updating function at the user interface of PKI client software.

To meet both compatibility and usability when generating digital signatures, user interface shall provide certificate sharing, import, export, certificate handling, and automatic update funcion.

#### 2.1.1 Certificate sharing function

User interface should allow multiple PKI applications to share users' certificates and private keys for increasing compatibility in different PKI applications. In addition, user interface should allow users to utilize their own certificates and private keys without inconvenience to search the certificates and keys. For these requirements, there should be standardards for storing users' certificates and private keys according to the users' operating system and storage media, which is implemented through a certificate

sharing function.

For example, a common storage location of a user's certificate and private key in HARD DISK driver of different operating systems can be assigned to be:

- MS Windows : C:Program Files/IETF/PKIX
- Linux/Unix : (User Account)/IETF/PKIX
- Mac OS X : (Hard disk label):Library/IETF/PKIX

For another example, in case of cryptographic tokens such as a smardcad containing certificates and priviate keys, if the smartcards follow a standard [PKCS#15], user interface of any application can search the certificate with keys and present the contained certificates and keys to users.

In these examples, a user can access to his or her own certificate and key for generating digital signatures without answering the question of where his or her certificate is. Note that it is supposed that generating digital signatures are processed independently and securely in the user's system.

Regarding as the user's certificate and private key, it may be stored as a form of xxx.der or xxx.key, after creating a directory named by DN. xxx naming is identically used for distinguishing between digital signature and certificate distribution purpose.

In addition, the client software should define application programming interface for accessing to various storage media such as HARD DISK driver, SMARTCARD, FLOPPY disk, etc.

Format of the user's certificate in storage media may be encoded as DER or PEM in order that the user interface can list all the certificates in any storage media. For storage format of the private key, it should use [PKCS5], which is a password based cryptographic method. Afterward, it should be stored to a storage medium according to [PKCS8].

### 2.1.2 Import and export function

The user interface shall provide import and export function to support certificate's mobility according to [PKCS12]. This function makes certificate and private key transfer to other PKI applications so that the user can utilize his or her certificate and private key in other PKI applications on the Internet X.509 Public Key Infrastructure.

### 2.1.3 Certificate handling function

User interface shall have at least three responsibilities for handling the user's certificates;

- Certificate information notice
- Storage type selection
- Certificate management

Firstly, Certificate information notice at user interface is to display certificate that was searched by client software so that user can select the certificate to use it. At this point, important information of certificate including subject name,expiration date, and issuer name about certificate may be listed. In addition user interface shall provide certificate information in detail if the users want to receive the more information on their certificates.

Secondly, for selecting various storage types, storage type selection in client software shall be made appropriately to display its storage medium by categorization, which can be changed according to the application's purpose.

On the certificate representation, a choice for storage media should effectively provide for user to select the desired choice. In order to do so, storage media are independently categorized by the nature of storage media, which helps users to differentiate their own storage easily from all the storage media. User interface may consider including the followings:

- Hard disk
- Floppy disk
- USB
- Smartcard
- CD ROM

Lastly, the user interface shall contain certificate management commands as followings;

- Integrity verification function of trust anchor : defined in [2.2.1]
- Import and export : defined in [2.1.2]
- Certificate verification : when a user wants to know whether his or her certificate is valid or not
- Private Key password change : when a user wants to change the password of his or her private key
- Certificate deletion : when a user wants to delete his or her certificate

### 2.1.4 Automatic update function

The PKI client software must provide a secure method to update PKI client software and trust anchor's certificate. This document defines it as automatic update function, which makes user involvement minimized. Note that there must be the integrity verification function defined in 2.2.1 when the trust anchor's certificate is updated automatically.

## 2.2 When verifying digital signatures

User interface of PKI client of PKI client software provides user transparency when verifying digital signatures. Users do not have to understand for the softwares how to make certificate chanis, verify certificate signs, and validate the certificates. However, user interface should provide users a way to confirm that trust anchor's key is not compromised because security of trust anchor's key is paramount for verification process of digital signatures. The way should be implemented in the client software by integrity verification function of trust anchor.

### 2.2.1 Integrity verification function of trust anchor

Users should acquire securely certificates of trust anchors which are selected and trusted directly by users, which requires some out-of-band steps.[CMP] This document describes integrity verification function of trust anchor using user interface of PKI client softwares as one of out-of-band steps.

First of all, PKI client software must be installed and upgraded with a reliable and secure manner. This document does not refer to this manner for PKI client software. Just after secure installation of PKI client software, the client software will download the trust anchor's certificate. At this point, the user interface of the client software should offer integrity verification function of trust anchor in order that users accept the trust anchor's certificate with reliability. And also the user interface shall assist the users to make the decision on whether or not the downloaded trust anchor's certificate can be trusted. The user must accept the trust anchor's certificate only if the trust anchor's certificate is verified through the direction from the user interface.

The user interface shall help users to receive the trust anchor's information for verifying out of band channel. The information must not be received via more than two channels to reduce risks to be attacked.

For example when PKI client software acquires the trust anchor's certificate after installation of client software, the user interface can show the hash value of acquired trust anchor's certificate and also direct how to acquire the trust anchor's information. The user will acquire the hash value of the trust anchor's certificate through at least two ways among face-to-face contacting, trust anchor's web site, or cards by postal service, etc by the directions of the user interface. Note that this example is sutible for the self-signed certificate of trust anchor because it is possible not to compare the hash values if the trust anchor's certificate is not self-signed.

In case that the trust anchor's certificate is updated, the client software also must acquire updated trust anchor's certificate. At this point, the client software can use its automatic upgrading function of the trust anchor's certificate. And then user interface must provide the same integrity verification function with an initial installation of trust anchor's certificate.

In addition, the user interface should support integrity of trust anchor's certificate with the verification function because there can be malicious attack to the trust anchor's certificate after reliably accepting the trust anchor's certificate when installing the client software.

## 3. Security Considerations

Malicious attackers can access to a user's certificate and private key because there is a common location for storing a certificate and a private key according to a user's operating system and storage media. However, it is supposed that there must be appropriate access control for the user's system and storage media in this document.

## 4. Reference

### 4.1. Normative References

[RFC2119] S.Bradner, "Key words for use in RFCs to Indicate Requirement Levels",RFC3467, March 1997

### 4.2 Informative References

[PKCS5] RSA Laboratories, PKCS#5 v2.0 "Password-Based Cryptography Standard", RSA Data Security Inc., 1993

[PKCS8] RSA Laboratories, PKCS#8 v1.2 "Private Key Information Syntax Standard", RSA Data Security Inc., 1993

[PKCS12] RSA Laboratories, PKCS#12 v1.0 "Personal Key Information Exchange Syntax Standard", RSA Data Security Inc., 1993

[PKCS15] RSA Laboratories, PKCS#15 v1.1 "Cryptographic Token Information Syntax Standard", RSA Data Security Inc., 2000

[CMP] Adams, C. and Farrell, S., "Internet X.509 Public Key Infrastructure Certificate Management Protocols", RFC 2510, March 1999.

## 5. Authors' Address

Baehyo Park
Korea Information Security Agency
Phone: 2-405-5443
FAX : 2-405-5219
Email: parkbh@kisa.or.kr

Jaeho Yoon
Korea Information Security Agency
Phone: 2-405-5434
FAX : 2-405-5219
Email: jhyoon@kisa.or.kr

Inkyoung Jeon
Korea Information Security Agency
Phone: 2-405-5432
FAX : 2-405-5219
Email: inkyoung@kisa.or.kr

Hyangjin Lee
Korea Information Security Agency
Phone: 2-405-5446
FAX : 2-405-5219
Email: jiinii@kisa.or.kr

Jaeil Lee
Korea Information Security Agency
Phone: 2-405-5200
FAX : 2-405-5219
Email: jilee@kisa.or.kr

## Intellectual Property Statement



## Disclaimer of Validity



## Copyright Statement



## Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.