Digital Certificate and Beyond

By Sangrae Cho (ETRI)

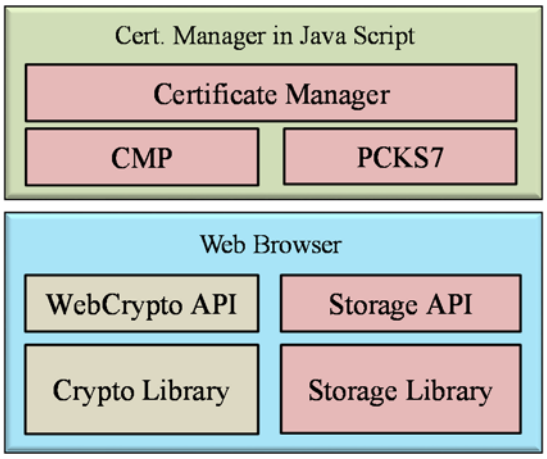
Background

In Korea, X.509 certificate is publicly and widely used in various financial sectors including banking, stock trading and insurance. However, the certificate management program for a user is developed using a technology called ActiveX control, which is a plugin type program to support certificate management functionality in Microsoft Internet Explorer web browser. Today, approximately over 30 million certificates are issued to organizations and individual users. This means that almost every adult citizen in Korea actually uses a certificate for financial transactions and other web services.

PKI is the sound and secure technology with international standards to establish a trust between relying parties and users. The problem lies with underlying technology and insecure environment to provide certificate services in the web. For instance, a few years ago, a malicious code that exploited a security hole in ActiveX control was widely spread causing to halt online banking services in Korea and nowadays there are various malicious codes targeting specifically to steal a user certificate and its related password for a private key. This is the reason that we have tried very hard to remove ActiveX control by redeveloping certificate management service based on Web standards.

Working with WebCrypto API

Currently we are developing authentication and digital signature services using WebCrypto API. In this development, we are building a certificate management library in JavaScript, which is called “polyfill”.



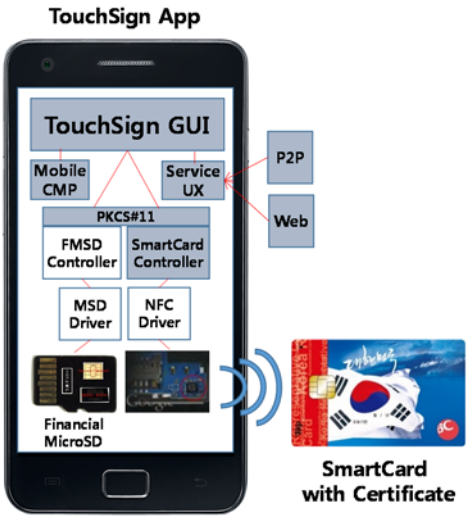
The figure in the right illustrates Certificate Manager in JavaScript. The implementation includes CMP (Certificate Management Protocol) and PKCS#7, which is digital signature format. The WebCrypto API is called for cryptographic functions such as key generation, hashing, digital signature and the storage API is used to store and manage a private key and a digital certificate in the browser. Certificate management service is implemented using only web technology such as JavaScript and HTML5. In the workshop, we will talk more detailed technical approach. This will demonstrate how WebCrypto API is applied

extensively for authentication and digital signature services in Korea.

Certificate with hardware token

A private key and certificate issued from a CA server are usually stored in the system as a file. Of cause the private key is stored in encrypted format. However, any malicious code can steal those private key files. This is a very serious problem in Korea.

The solution we have tried is to use a secure element or hardware token for a private key. Therefore last year we developed the program called TouchSign for secure authentication and digital signature solution. TouchSign uses a hardware token, which is a smartcard with cryptographic function and NFC. As you can see the figure in the right, a smartcard is physically separate from a smart phone. Smartcard only communicate with the smart phone using NFC. Now the private key is secure since it never leaves out of smartcard and exists separately. When you need to authenticate or sign digitally, you can just touch your card to your smartphone. We would like to demonstrate TouchSign and express its technical aspect in the workshop.



Korean PKI with FIDO

PKI in Korea is widely deployed and extensively used in various financial transaction. However the solution we are using is not for smart mobile environment. User still need to type a password to sign digitally in the smartphone display. FIDO tries to provide a universal framework for passwordless authentication. If we can combine Korean PKI with FIDO, then we can use more secure and convenient FIDO authenticator for better user experience. We think that Korean PKI will be synergized by FIDO. In the workshop, we would like to briefly introduce what our intension is and discuss about any technical or standard implication.

Proposition

We will try to present three research activities to overcome security problems of PKI in Korea. We think that authentication with a hardware token and biometrics is undeniable trend and it will be very beneficial if those functionalities are provided in the browser. We hope that our research effort can help WebCrypto WG make the scope of next standardization effort.