Live-CA：Design and Implementation of a PKI/CA System Integrating with Java Cards

蔡育儒(Yu-Ru Tsai)、楊中皇(Chung-Huang Yang)
tasis@wtps.ptc.edu.tw、chyang@computer.org
國立高雄師範大學資訊教育研究所
Graduate Institute of Information and Computer Education, NKNU

摘要

網際網路的應用例如電子文件和電子商務不斷的普及，已經逐漸改變人們生活方式和交易型態，因此開放式網路環境中的安全機制也更顯其重要性。除了對資料傳輸的保密外，網路使用者的身分認證更是重要的議題。公開金鑰基礎建設(Public Key Infrastructure, PKI)是目前可提供一個可信賴及安全基礎的網路環境中最成熟及最有效的解決方案，本研究採用開放原始碼 OpenCA 建置一個符合 PKI 架構的二層 CA 憑證管理中心並提供 LDAP 目錄服務。研究中亦開發出 PKI 使用者介面，避免使用者需不斷的切換頁面來進行憑證的申請、註銷及查詢的作業，同時結合 OpenCA 自動安裝程式、Open CA Live CD 和 Java Card 的應用，讓使用者能快速的安裝及使用更安全的 PKI 網路環境。

關鍵詞：PKI, Open CA,憑證,憑證機構,數位簽章

Abstract

With the wide applications of Internet, it has gradually impacted and changed the life styles and business models. Therefore, increasingly importance has been attached to the security problem of the public networks. When users access the Internet application services, they expect to have services with integrity, confidentiality and authentication. PKI (Public-Key Infrastructure) is a mature and consummate formula for establishing a trusted and secure open network services at present. In this research, we use the OpenCA open source software to realizes the technology of PKI and establish a two layer management of the Certification Authorities (CAs) that provides LDAP directories service. We also develop the PKI user interface program integrating with Java cards, OpenCA installation program, and Open CA Live CD to establish the development of PKI much more quickly and more secure network.

Keyword: PKI, OpenCA, Certificate, Certification Authority, Digital Signature

1. Introduction

Since the technology of information and network continues to progress , many users can obtain the resources and services from Internet .The applications of the network , like e-commerce and e-government, are relying on the conjunction and booming development of Internet. In the meantime, the security problem is an importance issue. Internet is principally a large public network, which may be easily suffered the attack from interruption, interception, modification, and fabrication etc. Thus, providing users a network security including confidentiality, authentication, data integrity, non-repudiation, the access control and availability [1] to insure the applications of security and credibility is the most important issue currently.

PKI (Public Key Infrastructure) [7] combining the public keys with certificates is an appropriate technology to provide security services including confidentiality, authentication, data integrity, and non–repudiation. Clearly, PKI itself needs to be trusted; therefore, it is managed by a certification authority (CA). Many international communities and enterprises promote the establishment of the Public Key Infrastructure strongly now [4].

Our country has begun to establish the Government Certification Authority, (GCA)which provides not only online identity authentication services to citizens and issues certificates in Internet Tax Report, but also various application systems for e-government services in 1998 [5].

Java Card [9] is the smart card using Java programming language to compose the application program (applet) at the payment security in the network and plays an important role in digital signature applications. The citizen personal certificate issued by the GCA is a kind of PKI applications integrating Java Card in recent years.

Because the commercial software which performs PKI is expensive and it's very complicated to put into practice, those retard the progress of widespread usage of PKI .Thus, in this research we use the open source software: OpenCA [22] which realizes the technology of PKI to establish a two layer management of the Certification Authority (CA) that provides LDAP directories service. We also use shell script to develop the OpenCA installation program that can provide users an automatically and quickly OpenCA platform. Finally, we make the OpenCA platform into the Live CD and develop the PKI user interface integrating Java Card. Therefore, the users can establish a more secure network require PKI easily and conveniently.

2. Related Work

2.1 Cryptography Background

E-commerce is demanding a secure way to transmit financially or legally sensitive data. The main problems faced by users of Internet are confidentiality, authentication, data integrity and non-repudiation. Cryptography converts the plaintext using some mathematical algorithm transforming it into a "unreadable" ciphertext and this process is encryption. Decryption is changing it back to its original form. Therefore, cryptography is a useful and efficient tool to adequately solve above problems. Cryptographic techniques are typically divided into two types: secret key cryptosystem and public key cryptosystem.

2.1.1 Secret key cryptosystem

Secret key cryptosystem also known as symmetric cryptosystem, requires that the sender and receiver share a key : a secret piece of information that is used to encrypt or decrypt a message. If this key is secret, then nobody other than the sender or receiver can read the message. The task of privately choosing a key before communicating occurs a very serious problem; a key management. Many well–known cryptosystems have been developed such as DES(Data Encryption Standard) 、Triple DES [17] 、AES (Advanced Encryption Standard) [20] ,etc.

2.1.2 Public key cryptosystem

Public key cryptosystem, also known as asymmetric cryptosystem, solves the key exchange problem by defining an algorithm which uses two keys, each of which can be used to encrypt a message. If one key is used to encrypt a message, then the other must be used to decrypt it. Public key cryptosystem was conceived in 1976 by Diffie and Hellman [8]. This makes it possible to receive secure messages by simply publishing one key (the public key) and keeping the other secret (the private key).Anyone may encrypt a message using the public key, but only the owner of the private key is able to read it. However, a trusted and authenticated key distribution infrastructure is necessary to support the use of public keys on a public network such as the Internet. There are famous public-key cryptosystem such as the factor problem, RSA[13],and elliptic curve discrete logarithm problem, Elliptic Curve [10].

2.1.3 One-Way Hash Function

One-way hash function is a hash function takes a long string (or message) of any length as input and produces a fixed length string as output, sometimes termed a message digest or a digital fingerprint. Digest algorithms are designed to produce unique digests for different messages. Message digests make it difficult to determine the message from the digest, and difficult to find two different messages which create the same digest — eliminating the possibility of substituting one message for another while maintaining the same digest. In various standards and applications, the two most-commonly used hash functions are MD5 [12] and SHA [18].

2.1.4 Digital signature

Digital signatures [19] are created by encrypting a digest of the message, and other information with the sender's private key. Though anyone may decrypt the signature using the public key, only the signer knows the private key. This ensures that only the signer signed it. Including the digest in the signature means the signature is only good for that message; it also ensures the integrity of the message since no one can change the digest and still sign it. The signature contains an unique sequence number. This protects the sender who did not send the message — only he/she could have signed it (non–repudiation).

2.2 Public Key Infrastructure

PKI (Public Key Infrastructure) is a system for publishing the public keys used in public key crypto -system .PKI provides the core framework for a wide variety of components, CA(Certification Authority), RA(Registration Authority), Certificate/CRL Repository ,and End Entity, displayed in Figure 1. A

PKI consists of hardware and software products, applications, along with governing security policies that use public key cryptosystem, digital signature, and certificates management to combine and achieve the four key security functions (confidentiality, authentication, data integrity, non-repudiation) [15].Nowadays, PKI is widely regarded as the most secure platform for e-commerce and a useful tool to establish a trusted and secure network.

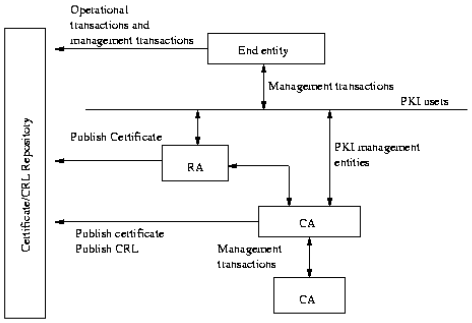

Figure 1 PKI Entities

2.2.1 Certificate

A certificate is a message signed by a publicly trusted third party —the certification authority, which has to be trusted by the entities using the certificates issued by this trusted party. The certificate guarantees that the public key is bound to the entity that is stated in the certificate. This assurance of correct binding and hence assurance that the certified party has been identified is the crucial requirement for public key techniques. The most widely used format is the X.509 V3 public key certificate [11] .Among information the certificate contains: version, serialNumber, signature, issuer, validity, subject, subjectPublicKeyInfo, issuerUniqueID, subjectUniqueID, extensions, signatureAlgorithm, signatureValue.

2.2.2 Certification Authority

The Certification Authority (CA) is a publicly trusted third party which issues and revokes certificates. A CA provides the trust basis for a PKI as it manages public key certificates for their whole life cycle. The CA will issues certificates by binding the identity of a user or system to a public key with a digital signature and ensure certificates are revoked when necessary by publishing certificate revocation lists (CRLs).

2.2.3 Registration Authority

The Registration Authority (RA) provides the interface between the user and the CA. The users who are issued certificates after a registration request has been approved. The RA authenticates the identity of the users and submits the certificate request to the CA. These interactions may also include certificate revocation and the other services that users need when interaction with a PKI.

2.2.4 Certificate/CRL Repository

The certificates and corresponding public keys need to be publicly available before they can be put to work. If a publication mechanism is provided to support dissemination of public certificates, a repository will be the usual place to publish certificates. The repositories that are usually utilized as part of a PKI are directories—occasionally X.500 directories, but more typically LDAP directories [14].

2.2.5 Certification Path

Certification paths [16] are chains of certificates that use trust relationships between CAs to determine when a certificate signed by another CA is trusted. A certification path starts with the public key of a Root CA and ends with the certificate containing the public key the user wants to use. Each certificate in the path is validated by the preceding certificate's public key. The user verifies a signature by successively verifying the signatures on certificates in the path. Figure 2 is the most simple certificate path.

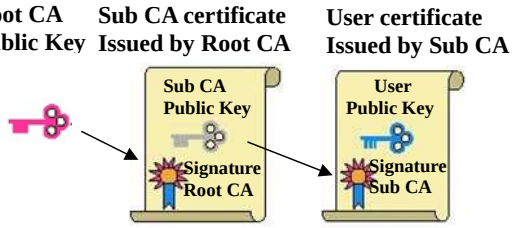

Figure 2 Certification paths

2.3 OpenCA Labs

As we know, PKI is a mature and consummate formula for settling the security problem of Internet at present, but the commercial software which performs PKI is expensive. In face of this actual state, the Open CA Labs, born from the former OpenCA Project, is an open organization aimed to provide a framework for PKI studying and development of related projects. The OpenCA PKI Development Project is a collaborative effort to develop a robust, full-featured and Open Source Certification Authority implementing the most used protocols with full-strength cryptography world-wide. OpenCA is based on many Open-Source Projects. Among the supported software is OpenLDAP, OpenSSL, Apache Project, Apache mod_ssl.

2.4 Java Card

Java Card [6,9] is a typical smart card: it conforms to all smart card standards and thus requires no change to existing smart card-aware applications.

In the smart card world, Java Card has been one of the most hyped products around for years. The main reason for the hype is Java Card's potential. Not only would it let all Java programmers develop smart card code, but such code could be downloaded to cards that have already been issued to customers. This flexibility and post-issuance functionality would significantly extend smart card possibilities.

3. Implementation

3.1 System architecture

This research is composed of three parts(see Figure 3): the management of Certification Authority, the PKI user interface, and a generic OpenPlatform Java Card The Certification Authority is installed with the open source software: OpenCA in two different Fedora Core4 servers and shows a general hierarchy of two layer management of the Certification Authority. Then we make the OpenCA hierarchy platform into the Live CD. The PKI user interface, we use Borland C++ Builder 6.0 to develop a user friendly implementation on the Windows environment integrating Java Card. Therefore, it can be used to add authentication and secure access to information systems that require a high level of security and stored information is portable.

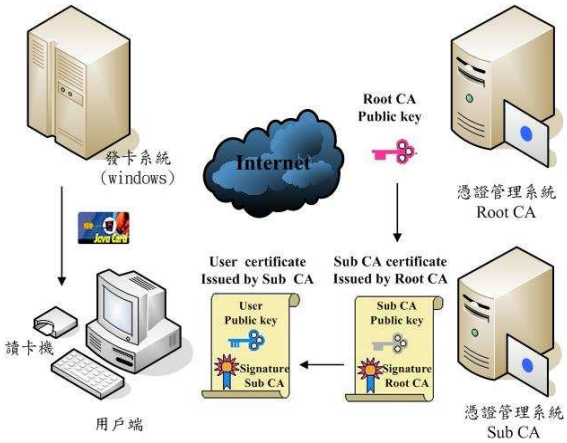

Figure 3 System architecture

3.2 Install the OpenCA

The OpenCA is based on many Open-Source Projects. Our OpenCA server is made on a very bare bones installation of Fedora Core4. Thus, the following packages must be added to meet all OpenCA dependencies: OpenSSL、Apache、Perl5、mod-ssl、MySQL and OpenLDAP [2] .Because of installing the OpenCA software is very difficult and complicated to put into practice, we use shell script to develop the OpenCA installation program that can provide users an automatically and quickly OpenCA platform. Figure 4 shows the OpenCA installation program.

Figure 4 OpenCA installation program

3.3 OpenCA Live CD

Because Linux is a open source software, it is regarded as at the earliest stage operation system of developing the Live CD, and KNOPPIX Linux [3,21] is the most complete among them. KNOPPIX is designed by the German programmer (Klaus KNOPPER) and it is a bootable CD or DVD with a collection of GNU/Linux software. In this research, we use the KNOPPIX Live CD as foundation with installing the OpenCA and remaster KNOPPIX Live CD to our own customized OpenCA Live CD. The users only need a OpenCA Live CD to set into CD-ROM, exempt the installment, no more need hard disk, can run OpenCA server in the memory. Figure 5 displays the bootable screen of OpenCA Live CD.

Figure 5 Bootable screen of OpenCA Live CD

3.4 Implementation of PKI user interface

We use Borland C++ Builder 6.0 to develop the PKI user interface on the Windows environment integrating Java Card. This software may facilitate the PKI user who wants to issue certificates or revoke certificates easily and allows the user to use Java Card as the medium for certificates or private keys storage. Figure 6 displays the main form of the PKI user interface.

First, the user must input IP address or DNS of the OpenCA server in the column. If the user has connected successfully to the OpenCA server, the message screen will display the piece and the edition message of the related software used in the OpenCA server. The PKI user interface also supports the SSL communication to secure online data transfer. So that the user can issue certificates or revoke certificates easily and securely in Figure 7.If the user wants to use

Java Card as the medium for certificates or private keys storage, certificates or private keys could be imported/exported from computer to Java Card according to the user's requirements, and contrariwise. Finally, the PKI user interface can use Online Certificate Status Protocol (OCSP) which can provide more timely information regarding the status of a certificate. Therefore, the user can request the certificate supplied in the request is 'valid', 'expired', 'suspended' or 'revoked' (see Figure 8).

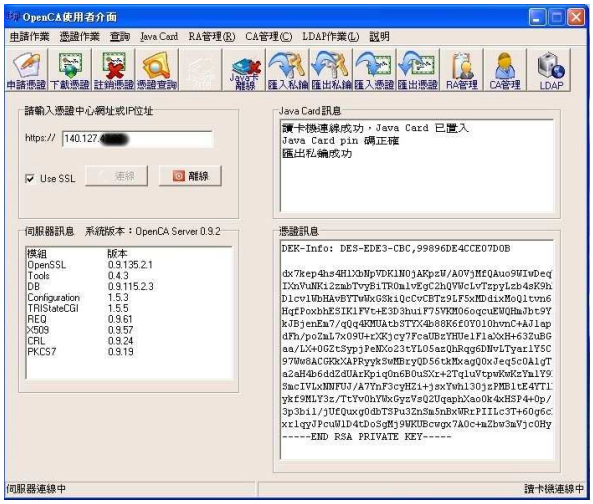

Figure 6 Main form of the PKI user interface

Figure 7 Issue certificates

Figure 8 Request the status of certificates

4. Conclusion

In this research, we design and implementation of PKI certification authority system using the open source software: OpenCA in the public network. Because installing the OpenCA software in the GNU/Linux is very difficult and complicated to put into practice, we develop the Live CD installation program and customize OpenCA to exempt the installment. Therefore, the user can establish a OpenCA platform much more quickly and easily. The PKI user interface program integrating with Java cards is used to manage every operation of certification authority and to enhance the data's privacy.

References

[1]楊中皇，網路安全理論與實務，2006，台北：金禾資訊。

[2]鄭佩技，Live-CA：結合 IC 卡的 PKI 憑證管理系統之設計與實現，國立高雄師範大學資訊教育研究所碩士論文，2005。

[3]KNOPPIX 中文交流網, http://kxoppix.tnc.edu.tw/

[4]亞洲公開金鑰基礎建設論壇, http://www.pki.org.tw

[5]政府憑證管理中心，http://www.pki.gov.tw/

[6] M. Baentsch , "JavaCard—From Hype to Reality" , IEEE Concurrency, pp.36-42, October 1999.

[7] W. Burr , "Public Key Infrastructure (PKI) Technical Specifications: Part A –Technical Concept of Operations" , September 1998. http://csrc.nist.gov/pki/twg/baseline/pkicon20b.PDF

[8] W. Diffie and M. Hellman, "New Directions in Cryptography" ,IEEE Transactions on Information Theory 22,pp.644-654,1976.

[9] C. Enrique Ortiz, "An Introduction to Java Card Technology ", May 2003. http://java.sun.com/products/javacard/

[10] A. Menezes and S.Vanstone , "Elliptic curve cryptosystems and their implementation" , Journal of Cryptology, Vol. 6 , pp.209-224, 1993 .

[11] R.Housley，W.Ford，W. Polk and D. Solo "Internet Public Key Infrastructure Part I: X.509 Certificate and CRL Profile "，March 1996. http://www.faqs.org/ftp/rfc/pdf/rfc2510.txt.pdf

[12] R. Rivest ,The MD5 Message-Digest Algorithm, April 1992. http://www.faqs.org/ftp/rfc/pdf/rfc1321.txt.pdf

[13] R. Rivest, A. Shamir, and L. Adleman,"A Method for Obtaining Digital Signatures and Public- Key Cryptosystems ", Communications of ACM, Vol. 21, pp.120-126 , February 1978.

[14] M. Wahl, T. Howes, and S. Kille, Lightweight Directory Access Protocol (v3), December 1997. http://www.ietf.org/rfc/rfc2251.txt

[15] S.Xenitellis, "The Opensouce PKI Book,OpenCA Team ",2000.

http://ospkibook.sourceforge.net/docs/OSPKI-2.4.7/OSPKI.pdf
[16] William T.Polk and Nelson E. Hastings ,"Public Key Infrastructures that Satisfy Security Goals" , Internet Computing IEEE , Vol.7, pp.60-76, August 2003.
[17] NIST FIBS 46-3 ,Data Encryption Standard (DES) October 1999. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
[18] NIST, FIBS 180-2,Secure Hash Standard, August 2002. http://csrc.nist.gov/publications/ fips/fips180-2/ fips180-2withchangenotice.pdf
[19] NIST, FIBS 186-2, Digital Signature Standard (DSS), January 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf.
[20] NIST, FIBS 197, Advanced Encryption Standard (AES), November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[21]KNOPPIX, http://www.knoppix.org/
[22] OpenCA Labs, http://www.openca.org/