



## **EverLink<sup>®</sup> Certificate Authority (CA) Server White Paper**

**Copyright © 2001 by Anyware Technology, Inc. All rights reserved.**

*June 28, 2001*

**Recipients cannot redistribute this document to any third parties without written permission from Anyware Technology, Inc. Anyware Technology, Inc. assumes no liability for any damages caused by the implementation of any software or services suggested in this document. The information in this document is subject to change without prior notice from Anyware Technology, Inc.**

## TABLE OF CONTENTS

<b>ABSTRACT .....</b>	<b>1</b>
<b>OVERVIEW.....</b>	<b>2</b>
<b>1. What is CA.....</b>	<b>3</b>
<b>2. Functions and Features of EverLink CA Server .....</b>	<b>4</b>
<b>3. The Program Structure of EverLink CA Server .....</b>	<b>6</b>
<b>4. Version.....</b>	<b>6</b>
<b>5. Firewall Setup.....</b>	<b>6</b>
<b>EVERLINK CA SYSTEM MODEL .....</b>	<b>8</b>
<b>1. System Model .....</b>	<b>8</b>
As the Certificate Authority of Your Own Organization .....	8
Secure Your Networks .....	8
B2B E-commerce certificate authority .....	9
<b>2. Certificates.....</b>	<b>9</b>
Personal Certificates .....	10
Double Key Personal Certificate .....	10
SSL Server Certificate .....	10
<b>KEY TECHNOLOGIES OF EVERLINK CA SERVER .....</b>	<b>12</b>
<b>1. EverLink CA's Implementation of PKI.....</b>	<b>12</b>
Security .....	12
Interoperability and Multiple Languages Support .....	13
CRL.....	13
Ease-of-Use.....	14
<b>3. User Group .....</b>	<b>14</b>
<b>4. End-to-End SSL .....</b>	<b>14</b>

---

Security Level of SSL Channel.....	14
Certificate Authenticated SSL Channel .....	15
<b>5. Browser/Server Structure .....</b>	<b>15</b>
<b>6. Intrusion Lock.....</b>	<b>16</b>
<b>7. Log and Audit.....</b>	<b>16</b>
Server Logs .....	16
Exporting Logs To an Audit Database.....	17
<b>8. Hardware Support .....</b>	<b>17</b>
<b>9. Standard Database Interface .....</b>	<b>18</b>
<b>10. Password Protection .....</b>	<b>18</b>
<b>11. Key Technology Summary.....</b>	<b>19</b>
Support the X.509 v3 Certificate and its Extensions .....	19
Certificate Feature.....	19
Supports Various Certificate/Private-Key Storage Media .....	19
Supports SSL Crypto Accelerators and Key Management Modules.....	19
Browser/Server Structure for both Administrators and Users .....	19
Easy to Manage User’s Certificate.....	20
Segmented Certificate Revoking List (CRL).....	20
<b>MULTIPLE PLATFORM SUPPORT AND SCALABILITY .....</b>	<b>21</b>
<b>1. Cross-Platform Solution.....</b>	<b>21</b>
<b>2. Scalability.....</b>	<b>21</b>
<b>REFERENCES.....</b>	<b>23</b>
<b>Reference 1: Terminologies .....</b>	<b>23</b>
<b>Reference 2: Standards Compliant in EverLink CA Server.....</b>	<b>28</b>

# Abstract

Anyware Technology's latest product is EverLink CA (Certificate Authority) Server, which is 100% PKI-compliant. With the CA Server it's now possible for a corporation to become its own certificate authority, issuing digital certificates based solely on corporate criteria. This will permit any organization to have complete control over certificate issuance and management. And, because it's an in-house CA, it's highly flexible, and can be easily personalized to meet and enforce specific corporate security needs. Furthermore, this is the server on the market that can issue certificates in English, as well as in foreign languages.

The CA Server is accessed via a standard Internet browser, allowing a system administrator to securely add, delete, and fully manage individual users and group accounts. Users themselves can apply for a certificate account through a browser, and then install a certificate via the browser after the account has been approved by an administrator. For added security, the CA Server maintains intrusion locks, which can be enforced against any IP address. All network activity is monitored as the CA Server keeps an extensive number of various kinds of logs, which can be easily overseen and managed. With all of its adaptability, functionality and power, the CA Server is available at a lower cost than the services of traditional certificate authority companies.

EverLink CA Server is a secure network operating system. It provides the following business values to a corporation:

1. Strong 3 factor user authentication (possession of hardware token, knowledge, and 3rd party verification); avoid weak password problem on the network logon.
2. Secure extranet applications; certify your customers and partners to authenticate them with 3 factor instead of weak password;
3. Support non-repudiation on web based business transactions; support digital signatures on your web site HTML forms;
4. Secure business communication; support secure email (encrypted and signed messages);
5. Support VPN and other secure remote access software.

# Overview

EverLink CA is digital certificate issuance and management software that allows an enterprise to quickly and easily establish itself as a certificate authority (CA). It provides user account application, user approval, user management, key generation, revocation, storage and signing. It allows CA server administrators to customize digital certificates for their employees, customers and business partners to gain secure access to e-commerce applications as well as to digitally sign and encrypt electronic mail, etc. EverLink CA Server is all an enterprise needs to fully control the digital certificate lifecycle management process and enables organizations to issue certificates under their requirements. Using the digital certificate guarantees:

- Confidentiality
- Authentication
- Non-repudiation
- Integrity

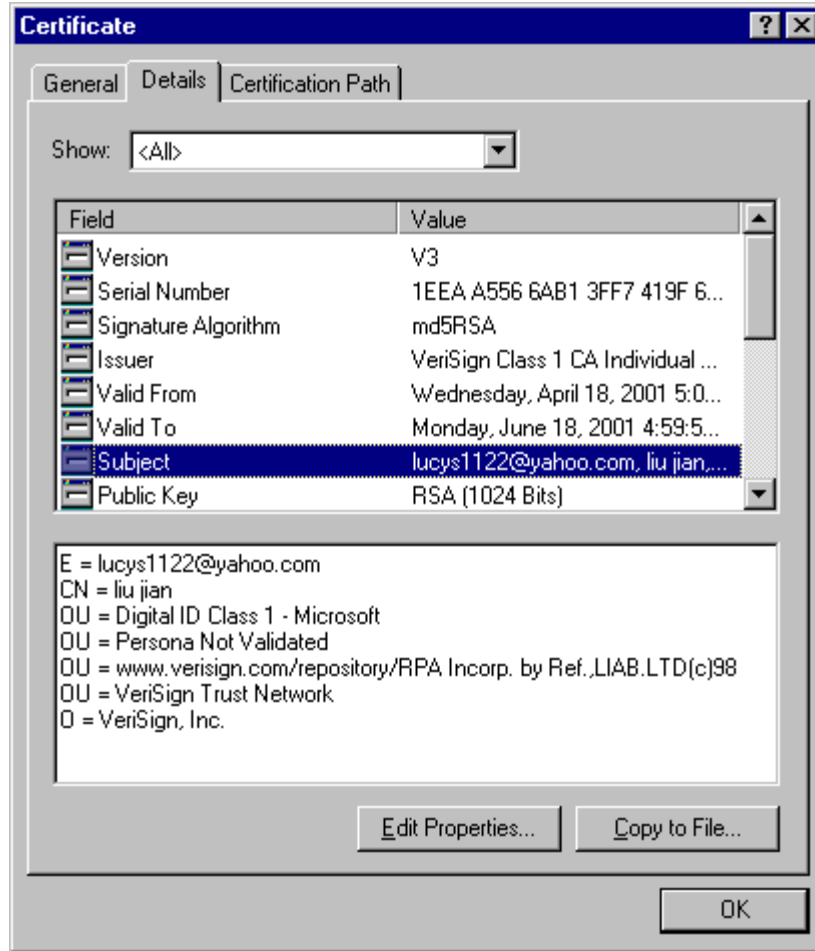
The advantages of using EverLink CA are:

- The CA Server functions as the authorization center for enterprise business application systems. There's no need to wait for approval from an external certificate authority company, and no need for outsourcing. An organization can build its own trust base for their PKI enabled applications.
- With the CA Server, a company can easily transform their LANs into a secure WAN, while still maintaining centralized access control policy as a whole. And a corporate access control policy can remain in force even if their users move from one LAN to another.
- As the certificate authority for enterprise B2B applications, a company can issue certificates to chosen business partners and customers. Therefore, they can access your resources which are securely under your control.
- The CA Server can also provide public certificate authentication services. The flexible design, scalability and adoption of international standards allow this server to be easily expanded from an enterprise CA to a public CA.

## 1. What is CA

CA (Certificate Authority) is an organization or company that issues digital certificates. Digital certificates are digitally signed by certificate authorities. A digital certificate is a tamperproof piece of data that packages a public key together with some attributes such as who owns it, what it can be used for, when it expires, so on and so forth. The most widely accepted format for certificates is defined by the CCITT X.509 international standard. Its newest version is X.509 v3. A certificate consists of the following fields:

- Version: the version of X.509, for example V1、 V2、 V3.
- Serial number: a unique number assigned to the certificate by the certificate issuer.
- Signature algorithm identifier: the algorithm identifier for the algorithm used by the CA to sign the certificate.
- Issuer name: the entity that issued the certificate (CA), including all the information about CA.
- Validity period: the valid period of the certificate, usually one year in length.
- Subject name: identity of the entity associated with the public key, including all the information of the entity. It is owner of the certificate.
- Subject public key information: subject's public key, optional parameters, and algorithm identifier.



A certificate authority (CA) as a trusted third party can issue, revoke and manager digital certificates for its users.

## 2. Functions and Features of EverLink CA Server

A standard certificate authority (CA) can issue, revoke, verify digital certificates, maintain its certificate revocation list (CRL), and provide real-time certificate status. Additionally, EverLink CA server can also maintain its user database, set up user groups, keep logs of activities, support X.509 v3 extensions, support a wide range of hardware tokens for certificate storage and set intrusion locks to prevent password hacking.

- 1) **Web-based user account applying and managing:** A user accesses EverLink CA server via a standard Internet browser (Internet Explorer、Netscape) through secure HTTPS protocol.

- 2) **SSL server certificate:** EverLink CA version 2.0 and above can issue SSL server certificates.
- 3) **Wireless Device Certificate:** EverLink CA can issue certificates to wireless devices such as PDA or Cell Phone to enable secure mobile business transactions or commerce.
- 4) **Double Key Certificates:** Separating a user's encryption key from his signing key is very important in the enterprise environment. The encryption key can be backed up by the corporation to ensure that employees' encrypted email messages always can be read by the management. At same time, the signing key is held only by the user to ensure the message non-repudiation. EverLink CA can issue double key certificates.
- 5) **CRL:** A user can revoke his/her certificate. The CA server will add the revoked certificate to the Certificate Revocation List (CRL). Any application can retrieve the CRL through the CA server's public port. The CRL refresh period can be as short as one hour.
- 6) **Online Certificate Status Protocol (OCSP):** The entity, either a person or a program, can check certificate validity in real time via OCSP. The real-time validity of a certificate is crucial for some applications such as electronic funds transfer.
- 7) **Cross-Sign:** EverLink CA can cross-sign another CA's signing certificate with its own signing certificate to provide trust between two certificate authorities. The cross-sign signer certificates can inherit the trust in the business world into the digital world to use the trust in the business world to ensure secure digital communications.
- 8) **User Database:** EverLink CA provides its own user database to store users' information. Any user in the user database can create and manage his/her digital certificate from the server. An EverLink CA server can also support a third party database through JDBC technology.
- 9) **X.509 Certificate and its Extensions:** EverLink CA server issues standard X.509 v3 digital certificates to its users. The certificates can be used in any PKI-enabled applications. EverLink CA server can also set its users to predefined organizations and organization units for a role-based application.
- 10) **Certificate Storage:** EverLink CA supports a wide range of media to store digital certificates, such as Internet Explorer, Netscape Navigator certificate database, disk, iKey from Rainbow Technology, eToken from Aladdin and iButton from Dallas

Semiconductor, etc.

- 11) **Intrusion lock** : EverLink CA Server maintains intrusion locks, which can be enforced against any user account or IP address. Any password trials to a locked user account are forbidden. Any network connections from a locked IP address are forbidden.

### **3. The Program Structure of EverLink CA Server**

EverLink CA is developed by Java language, so it is a cross-platform software solution. EverLink CA provides server setup, server start, root certificate manager and certificate manager from console. EverLink CA server has three servers: Administration Server, Private Server and Public Server. They are listening on the different TCP ports (The default setting is 444 for Administration Server, 443 for Private Server, 80 for Public Server). All the three servers are accessed through web browser.

- Administration Server: administrators of CA server manage its users, certificates, CRL, and viewing logs etc.
- Private Server: users of CA server apply for an account, install their certificates, revoke their digital certificates or change their passwords after being successfully authenticated by the server.
- Public Server: anybody can search and download a user's certificate and obtain the CRL from the CA's public server.

### **4. Version**

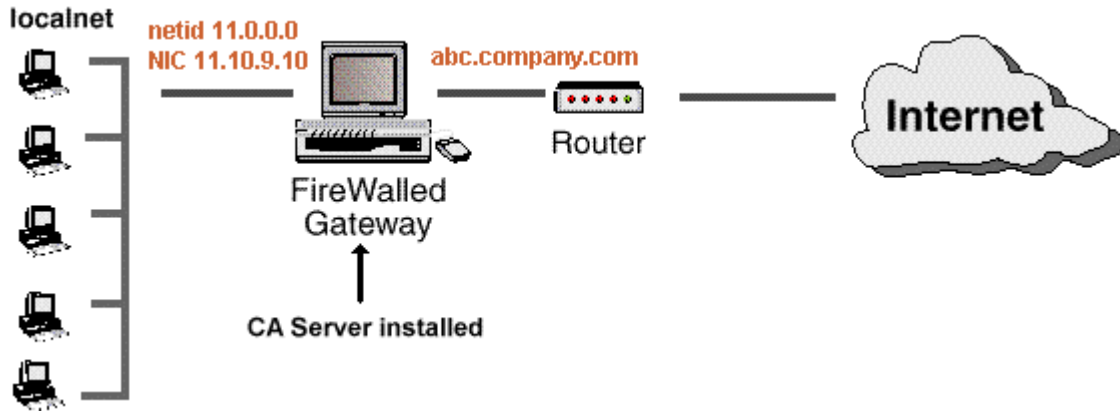
Anyware Technology Inc. released EverLink CA version 1.00 in Dec. 2000. After the version 1.24 and 1.50 release, the current version is 2.00.

### **5. Firewall Setup**

As a trusted digital certificates issuer, the security of the CA server is very important. It is highly recommended to protect CA server with firewall.

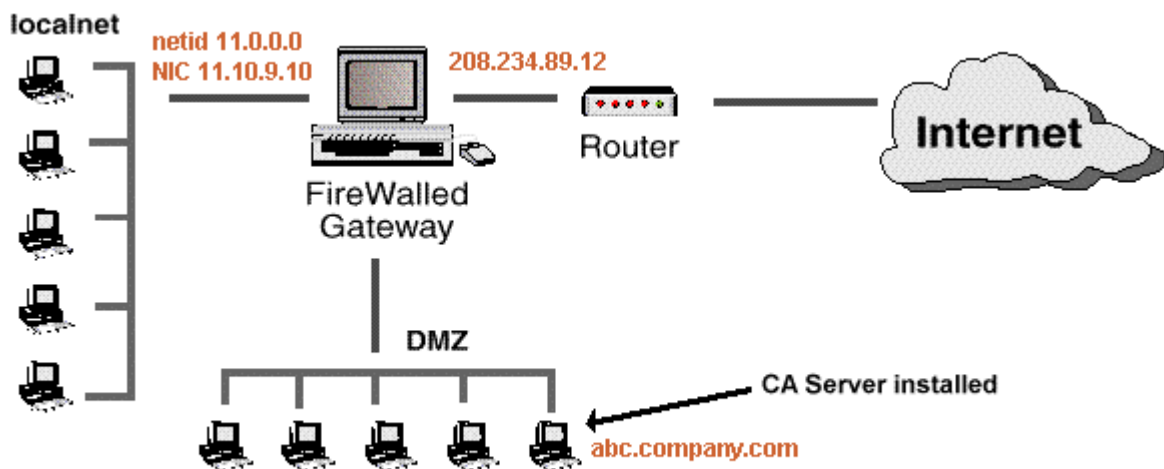
- 1) Install CA Server and Firewall on the Same Computer.  
EverLink CA Server and firewall can be installed on the same computer. In this case,

firewall needs to open access to the ports of CA private server and public server from the Internet, so its users can access the private server and public server from the Internet. But firewall should close access to the port of the administration server from the Internet and limit the access to the administration server only from LAN or a computer on the LAN. The administrator of the CA server will be able to manage the server through a web browser on a computer in the LAN.



2) Install CA Server in DMZ Zone

If EverLink CA is installed in DMZ Zone, firewall needs to open access to the ports of its private server and public server from the Internet. But firewall should close access to the port of the administration server from the Internet. If access from LAN to DMZ zone is controlled by firewall, firewall needs to open access to the ports of its private server and public server from LAN to DMZ zone and open access to the port of its administration server from LAN or a computer on the LAN.



3) Install CA Server on LAN

If EverLink CA server is installed in the LAN, no change to the firewall is needed.

# EverLink CA System Model

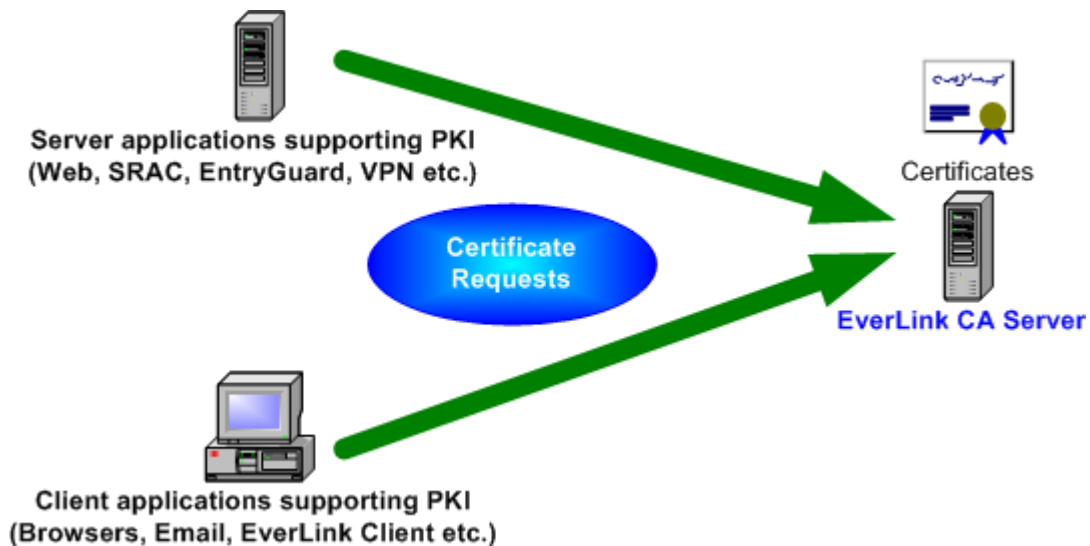
## 1. System Model

EverLink CA Server has a browser/server (B/S) structure. No client installation is needed. Via a web browser (such as Internet Explorer, Netscape Navigator), a user can securely access CA server through an insecure network such as the Internet.

EverLink CA server is simple in design and supports a wide range of application models. An organization can setup its own CA server according to its own needs. For example:

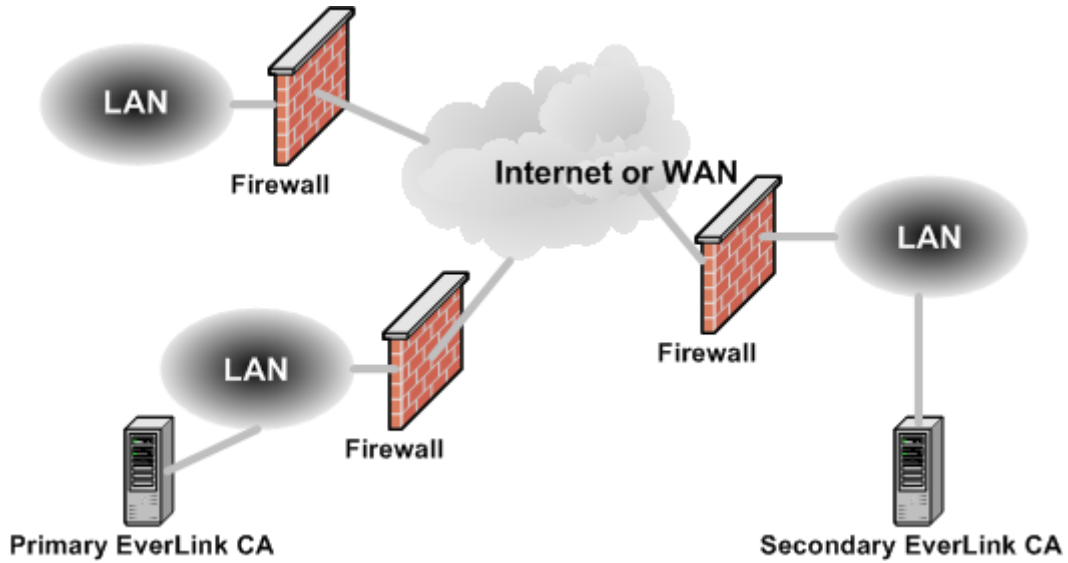
### As the Certificate Authority of Your Own Organization

Figure 1. Issue certificates to PKI enabled applications.



### Secure Your Networks

Figure 2. Using CA and PKI enabled VPN or SRAC Servers to link company's LANs together into a secure WAN.



**B2B E-commerce certificate authority**

Figure 3. Secure extranet by certifying business partners. Support non-repudiation business transactions by signing HTML forms in B2B web applications.



**2. Certificates**

EverLink CA Server issues two kinds of digital certificates: personal certificate and SSL server certificate. A personal certificate is mainly used to sign and encrypt personal e-mail, sign HTML forms and to authenticate a person to a web server. The SSL server certificate is mainly used to authenticate your Web site.

## **Personal Certificates**

Personal certificates are used to perform secure authentication across public networks like the Internet. You can use personal certificates to create secure communications between business partners and across enterprises in an extranet environment. The personal certificate contains information about a person's identity such as name and email address etc. EverLink CA server is in X.509 v.3 certificate format. The personal certificates can be used with Netscape Navigator or MSIE to authenticate the person during online web sessions or used to digitally sign and/or encrypt email in any S/MIME enabled email client.

## **Double Key Personal Certificate**

Usually a personal certificate can authenticate the user, sign user's outgoing email messages and decrypt user's incoming email messages. In the corporate environment, sometimes it desires to separate decryption of user's incoming email messages from other functions of the personal certificate. EverLink CA accommodates this requirement by issuing two certificates with two different RSA key pairs to the user. One certificate is limited to sign the email messages and authenticate the user only. Another certificate is limited to decrypt the email messages. The decryption certificate and its key pair can be backed up to a server or a separate hardware token. With backup decryption certificate and its key pair, the company management can decipher the encrypted email messages of their employees.

## **SSL Server Certificate**

SSL server certificate will authenticate your Web site and enable SSL on your web server, thereby giving you the ability to communicate securely in your e-commerce applications. A SSL certificate:

- Contains the identity of the server such as: domain name, organization name, organization unit name, country, state and city.
- Is in X.509 v.3 certificate format and can be used in a standard browser.
- Enables SSL on your web server with your customers thereby giving you the ability to communicate securely with your online customers. SSL protects all communications with your customers, so you can take credit card orders and protect sensitive personal information.
- Can be used for Microsoft IIS server, Netscape Enterprise server and Apache server.
- Can be used for SRAC and VPN servers.

Once you have applied an SSL certificate, you are given a username and password that allows you to return any number of times to obtain certificates, to renew or to revoke existing certificates.

EverLink CA server can also be used as an intermediate certificate authority by obtaining its certificate from a trusted root certificate authority.

# Key Technologies of EverLink CA Server

EverLink CA is a new generation of security software that meets the challenges of the Internet age. It offers the convenience of global information exchange to users. At the same time, it ensures the external security and the internal security of information exchanges. Security is the cornerstone of EverLink CA design.

This section explains the basic concepts and the technologies used in EverLink CA.

## 1. EverLink CA's Implementation of PKI

EverLink CA Server is compliant with PKI technology standards. Its implementation is completely transparent to users. A user doesn't need to know the what is key pair generation and how his certificate is signed by the CA. With just a simple mouse click, everything will be taken care of by EverLink CA. The server's web page contains step-by-step instructions to teach users how to apply and install certificates.

The following are the 4 features in EverLink CA's PKI implementation:

- **Security:** High strength encryption algorithms and private key protection.
- **Interoperability:** Capability of exchanging information, certificates and services with other standard PKI applications.
- **Flexibility:** Configuration to meet the security needs of the corporation with easy setup steps.
- **Ease-of-use:** Secure online administration and management by administrators, and secure online certificate management by end-users.

### Security

EverLink CA Server supports various encryption algorithms, including symmetric algorithms, such as DES, Triple-DES (168 bits), RC2 and AES (128 bits, 192 bits, 256 bits) etc, and asymmetric algorithms, such as RSA (1024 bits), and hash algorithms such as MD5 and SHA-1.

EverLink CA Server can use private key protection hardware that supports the PKCS #11 standard. There are two kinds of private key protection hardware:

1. Key protection accelerator card: the private key is protected with hardware tokens on the hard disk of the computer. Without the tokens the private key cannot be read. The private key is not loaded into the memory of the computer during asymmetric calculations. An example of this kind of hardware is nShield from nCipher.
2. Key and code protection hardware: In addition to protection of the private key, the code to use the private key is also protected with hardware tokens. The code is also digitally signed and encrypted then stored on the hard drive of the computer. The code integrity is guaranteed with the digital signature. An example of this kind of hardware is Secure Execution Engine (SEE) from nCipher.

## Interoperability and Multiple Languages Support

EverLink CA server is 100% PKI-compliant and adopts international standards. This makes it possible to interoperate with other PKI-compliant applications from other developers.

EverLink CA server issues standard X.509 v3 digital certificates. The certificates issued by EverLink CA server are compatible with those issued by other CA servers and can be used in any applications, which requires X.509 v3 digital certificates. EverLink CA server supports a number of standard X.509 extensions. For example, you can customize your Key Usage extension. EverLink CA server also supports multiple languages.

For other standards used in EverLink CA server, please refer Appendix II.

## CRL

In some situations, the user's certificate may need to be revoked, for example, if the private key has been compromised, the information in the certificate has changed or the certificate will never be used again. EverLink CA Server maintains a list of the revoked certificates, called the certificate revocation list (CRL). The information of certificate revocation will remain in the CRL list until the certificate expires. An application can check the revocation status of a certificate issued by EverLink CA Server to make sure that the certificate is reliable.

EverLink CA server's CRL implementation has the following features:

- **CRL easy to use :** In traditional PKI application software, there is usually no easy way to transfer certificates and CRL's between sender and receiver. EverLink CA server provides an easy way for users to revoke their certificates and for application to retrieve CRL through server's public port via HTTP protocol.
- **CRL timely update :** EverLink CA's CRL refresh period can be defined in an hour.
- **CRL distribution point :** All the certificates issued by EverLink CA Server contain

CRL distribution point extension.

- **Segmented CRL** : reduces server processing time, CRL transmission time and query response time.

## **Ease-of-Use**

- **Certificate management**: CA administrators can assign which root certificates to trust from the root certificate manager. EverLink CA server can act as a sub CA after applying its certificate from a trusted CA.
- **Authentication criteria**: When configuring CA Server, the administrator can specify what information in the certificate is to be used to authenticate himself according to the security requirement. The information such as country, company and department etc, can be used as criteria in addition to the name and email address in the certificate.
- **Security level setup**: Security level can be adjusted through the CA setup program, according to the requirement of the corporation. For example, if high security is required in some corporations, then the encryption algorithms of low security level can be deleted.

## **3. User Group**

EverLink CA server supports user groups and assigns each user to a predefined user group. Any application can use the user groups in the users' certificates to set role-based access control. The user group is defined by the organization and organization unit information in a user's certificate.

## **4. End-to-End SSL**

SSL is a security protocol that is between transfer and application layers. The symmetric encryption key is generated in every network session, based on negotiation between the server and browser. It is generally associated with web applications and HTTP (named as HTTPS) protocol. The EverLink CA Server uses HTTPS to secure the administrator and user accesses.

### **Security Level of SSL Channel**

EverLink CA fully supports SSL suites, and offers easy selection of the SSL suites to the

administrators during the server setup.

1) Multiple encryption levels: CA Server supports multiple encryption levels, and administrator can choose the encryption levels to meet his requirements. These encryption levels are: RC2 encryption (128 bits, 64 bits, 56 bits and 40 bits), DES encryption (40 bits and 56 bits), Triple-DES encryption (168 bits) and AES (128 bits, 192 bits, 256 bits).

2) Priority control: CA Server will search the SSL encryption levels automatically according to the priority of encryption levels set by the administrator. And administrator can add, modify or delete the encryption levels. For example, if the system administrator thinks that it is insecure to encrypt with just 40 bits key, he can delete 40 bits levels from the CA setup program. The reason for EverLink CA keeping these low level encryption algorithms is to connect with the computers using low encryption levels in some countries.

### **Certificate Authenticated SSL Channel**

The EverLink CA administration server uses the administrator's certificate in the SSL handshaking process. The authentication criteria can be specified during the server setup process.

## **5. Browser/Server Structure**

EverLink CA Server provides user account application, certificate installation, and certificate management through a web browser. The end-users can manage their certificate life cycle securely via a web browser.

Using this browser/server model, a server administrator can manage user applications, user accounts, and user certificates all through HTTPS protocol securely, easily and conveniently online via a web browser. An organization will have complete control over certificate issuance and management.

**Minimize Management :** Users apply their accounts through the server's private server (HTTPS protocol). Users choose their own passwords when applying their accounts. A server administrator can approve or reject any user account application. After the server administrator has approved a user's account, the user can manager his/her certificate through the server's private server via a web browser.

**Simplified Certificate Management:** After obtaining an account from EverLink CA server, a user can log on to the server to apply or revoke his/her digital certificate by a few mouse clicks.

## 6. Intrusion Lock

EverLink CA private server allows three username/password authenticate attempts. If all three attempts fail, EverLink CA private server creates an intrusion lock. This lock may be imposed either on the IP address where the failed attempts came from or on the user account making the failed attempts. Further connection from the locked IP address or user account is forbidden.

## 7. Log and Audit

The detail logs and audit trails are important in any information security system. EverLink CA Server provides forcing logs, log backup and a JDBC interface to export logs and duplications to an auditing database.

### Server Logs

EverLink CA Server has detailed access logs and error logs. The access logs record normal activity on EverLink CA Server. The error log records the server errors and any password failures and intrusion locks.

Three HTTP servers of a CA server keep detailed logs on the activities and the errors. There are five kinds of logs:

- Administration server errors: Errors records of the CA administration server.
- Private server accesses: Access activity records on the CA private server.
- Private server errors: Errors records of CA private server.
- Public server accesses: Access activity records on the CA public server.
- Public server errors: Errors records of CA public server.

In the access log, the system records access time to the server, the user name, the domain name and the web request command (For example, GET /internal-cgi/applycertfrombrowser HTTP/1.1) and request object (For example, https://www.my\_CA.com/title.html) from the browser. The server's response and message when an error occurs are also recorded in addition to the above information. To offer the deep level information to the administrator, the log information records all the lower level events. The system therefore requires the administrator to have certain knowledge about the security technologies of the whole system.

EverLink SRAC server will backup the previous seven-day's logs automatically. If the

administrator wants to keep more than seven-days logs, administrator can back up logs manually to a database.

## **Exporting Logs To an Audit Database**

EverLink CA Server can export the server logs to an auditing database. EverLink CA Server provides a JDBC interface to export logs to the database.

To export logs to different customers' auditing databases, EverLink CA Server provides application programming interface (API) for customization.

## **8. Hardware Support**

Hardware vendors have developed various encryption cards to meet the demands of the PKI application market. EverLink CA Server supports the following hardware, which are divided into three categories:

Certificate/private-key storage media mainly used in storing a secret key safely for client and server applications, including:

- Electronic keys such as iKey
- Electronic buttons such as iButton
- Smart cards that support Microsoft Crypto API or PKCS11.

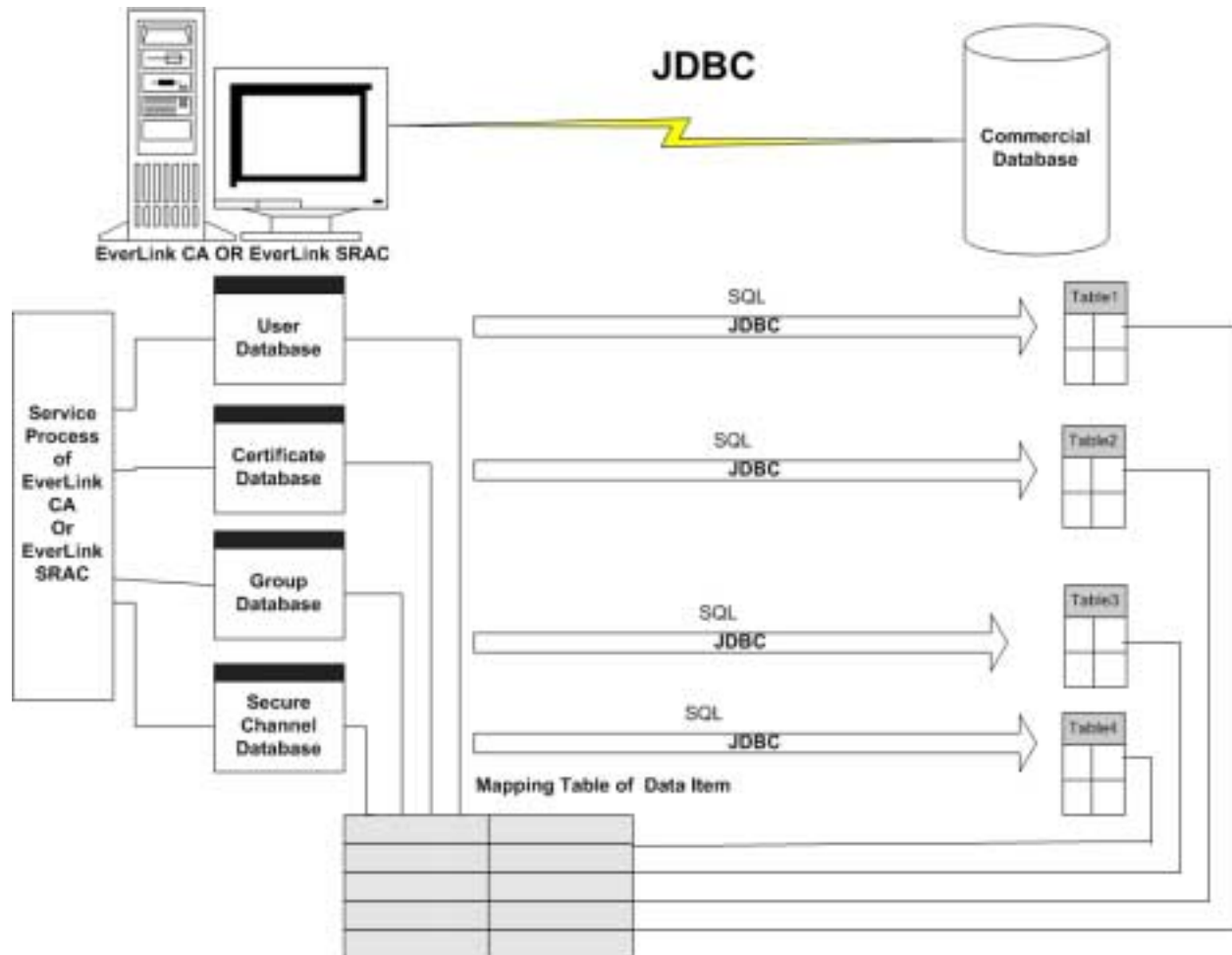
Crypto Accelerators and Key Management Hardware: Mostly used in server applications. Crypto accelerators provide high-speed data encryption and decryption to reduce the bottleneck caused by software encryption. Key Management Hardware protects the private key and critical portion of server code from tempering:

- CryptoSwift e-commerce server accelerator by Rainbow Technologies,
- NForce and Nshield accelerator and key management modules by nCipher;
- SEE accelerator, key management, and code protection module by nCipher;
- Other server accelerators that support PKCS11.

Use of this hardware for EverLink CA Server is optional. For example, a user can choose to store a certificate in the certificate database of a browser (Internet Explorer or Netscape Navigator), or in the installed storage devices. An administrator can choose to store the server private key in the hard disk with password protection or with key management protection. The key management module is strongly recommended in the CA server setup.

## 9. Standard Database Interface

EverLink CA Server provides standard database interface. It can be integrated with third party commercial database through JDBC technology. An EverLink CA Server can choose to use the database which comes with the server or use API provided by EverLink CA Server to integrate with the existing user database. The principle of database API is illustrated in the following chart.



## 10. Password Protection

EverLink CA Server takes the following steps to protect users' passwords on the server.

- 1) Password is encrypted in the database.
- 2) There is no password in the logs.
- 3) Administrator cannot change a user's password from the user's account application.
- 4) In case of user forgetting password, the administrator will change user's password only after the user's private identifier has been verified.

## **11. Key Technology Summary**

### **Support the X.509 v3 Certificate and its Extensions**

- Compatible with other CA
- Support any PKI-enabled applications
- Enforce user group and support X509 extensions
- Support multiple languages (Unicode format)

### **Certificate Feature**

- Periods of validity can be precisely defined in hours
- Provides control of user groups for role-based applications
- Supports RSA keys longer than 1024 bit

### **Supports Various Certificate/Private-Key Storage Media**

- Electronic key: iKey
- Electronic button: iButton
- Smart cards that support Microsoft Crypto API and PKCS 11

### **Supports SSL Crypto Accelerators and Key Management Modules**

- CryptoSwift e-commerce server accelerator by Rainbow Technologies
- NForce and Nshield accelerator and key management modules by nCipher;
- SEE accelerator, key management, and code protection module by nCipher;
- Other server accelerators that support the PKCS #11 standard

### **Browser/Server Structure for both Administrators and Users**

- Simple and convenient

- Secure and private
- Easy maintenance
- Simple configuration
- Cross-browser (IE and Netscape Navigator) support

### **Easy to Manage User's Certificate**

- Certificate application, approval, installation and revocation can all be done securely online.
- Users can manage their own passwords, ensuring privacy protection.

### **Segmented Certificate Revoking List (CRL)**

- Reduces server processing time
- Reduces the time of CRL transmission
- Reduces query response time

# Multiple Platform Support and Scalability

## 1. Cross-Platform Solution

EverLink CA Server was developed using Java™ technology, making it a cross-platform solution. It runs on any server which supports Java VM.

Supports a variety of software platforms:

- Windows 98/NT/2000/ME,
- Unix: Solaris, AIX, HP-UX, Compaq True64, Linux,
- Novell Netware5,
- IBM AS400, S/390.

Supports various hardware platforms

- Intel/AMD PC and servers,
- IBM RISC servers and S/390 servers,
- Sun SPARC servers,
- Compaq Alpha servers.

Server system requirements

- Processor – 166 MHz, RAM – 64 MB, free disk space – 30 MB
- Any operating system that supports a Java Virtual Machine, including small and mainframe computers

## 2. Scalability

The scalability has two issues; how EverLink CA Server handles large amounts of users and how the network handles the encrypted data transfer load.

Due to the EverLink CA architecture, the most CPU intensive operations such as RSA key pair generation are distributed to the client side. The CA server does SSL encryption operation and password authentication. In a real case, a one hundred users CA Server can operate on a 90

MHz Pentium Windows NT server.

In a large user base case, a more powerful server other than Windows NT can be used for the CA server. EverLink CA Server is written in pure Java and any hardware and operating system that supports Java Virtual Machine can be used such as IBM AIX machine. The crypto accelerator hardware can be used on the server side to speed up the SSL handshaking process. The cluster server with server load balancer can be used for a large public CA site.

# References

## Reference 1: Terminologies

**3DES:** An encryption algorithm like DES, it encrypts with three 64-bit keys. It has many different implementations, but they all encrypt, decrypt, and encrypt the same data block with three different keys.

**AES:** Advanced Encryption Standard. AES is much stronger and more effective than 3DES.

**CA (Certificate Authority):** A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be.

**Certificate request:** A Certificate request is a group of encoded text including the content administration input during CA setup. It's required by most CA's when issuing server certificates.

**CRL (Certificate Revocation List):**

You need to revoke a certificate if one of the following situations occurs:

- The owner of the certificate has changed status and no longer has the right to use the certificate.
- The private key of a certificate owner has been compromised.

By revoking a certificate, you are notifying other users that the certificate is no longer valid. CA makes this notification by publishing a list of the revoked certificates. This list is called the certificate revocation list (CRL).

**Decryption:** The translation of secret text into plain text.

**DES (Data Encryption Standard):** is a key encryption method used world-wide. It was developed by IBM in the 70's, and was accepted by the American National Standard Institute (ANSI). In this standard, 72,000,000,000,000,000 (72Q) keys are available. The encryption key

is randomly selected from the 72Q keys to each piece of information. Both encryption side and decryption side should use the same key.

**Digital certificate:** A digital certificate is issued by a certification authority (CA). It contains your name, a serial number, expiration date, a copy of the certificate holder's public key (used for encryption messages and digital signature), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

**Digital Signature:** digital signatures assure the recipient of a digital message of both the identity of the sender and the integrity of the message.

**DMZ:** A Demilitarized Zone is used by a company that wants to host its own Internet services without sacrificing unauthorized access to its private network. The DMZ sits between the Internet and an internal network's line of defense, usually some combination of firewalls and bastion hosts. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

**DNS:** Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Therefore, every time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name `www.example.com` might translate to `198.105.232.4`.

**Electronic fingerprint:** generated by a set of hash algorithms and used for identification.

**Email Certificate:** You can use your email certificate to digitally sign and encrypt your email communications. Using the digital certificate guarantees:

- **Confidentiality:** only intended recipient(s) can read the email message
- **Authentication:** assures recipients that e-mail really came from the sender
- **Non-repudiation:** the sender of an email cannot deny being the source of the email
- **Integrity:** the email message cannot be altered

**Encryption:** The translation of data into a secret code. Encryption is the most effective way to achieve data security.

**Firewall:** A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

**HTTP:** Acronym for HyperText Transport Protocol, the system for requesting HTML documents from the World-Wide-Web.

**HTTPS:** It's the security-enhanced version of HTTP, and is used in the SSL of Internet servers. The example of HTTPS URL is: <https://www.abc.com>.

**Intrusion Lock:** EverLink CA allows three username/password attempts. If all three attempts fail, the server creates an intrusion lock. This lock may be imposed either on the IP address where the failed attempts came from or on the user account making the failed attempts, depending on how the server is set up. Further connection from the locked IP address or password attempt to the locked user account is forbidden.

**IPSec:** Short for IP Security, a set of protocols being developed by the IETF to support secure exchange of packets at the IP layer.

**ISP:** Short for Internet Service Provider, a company that provides access to the Internet, some also providing services such as: disk renting, homepage making, mail service and server setup.

**JVM:** Acronym for Java Virtual Machine. An abstract computing machine, or virtual machine, JVM is a platform-independent programming language that converts Java bytecode into machine language and executes it. Most programming languages compile source code directly into machine code that is designed to run on a specific microprocessor architecture or operating system, such as Windows or UNIX. A JVM -- a machine within a machine -- mimics a real Java processor, enabling Java bytecode to be executed as actions or operating system calls on any processor regardless of the operating system.

**Netstat:** UNIX command (also used in Windows) to show the current TCP/IP connections and addresses.

**NIC:** Abbreviation of Network Information Center, provides services such as help, document and training, etc. for users. NIC locates all over the world.

**PKCS:** The Public-Key Cryptography Standards (PKCS) are a set of intervondor standard protocols for making possible secure information exchange on the Internet using a public key infrastructure (PKI). The standards include RSA encryption, password-based encryption, extended certificate syntax, and cryptographic message syntax for S/MIME, RSA's proposed standard for secure e-mail.

**PKI:** Short for public key infrastructure, a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. It uses an asymmetric encryption algorithm in which the encryption key is different from the decryption key.

**POP3:** POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) will check your mailbox on the server and download any mail.

**Private Key:** In cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. A public key is used together with a private key. Private key is used to decrypt a message that has been encrypted with the public key, and sign the message.

**Proxy server:** A server that sits between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

**Public Key:** A public key is a value provided by some designated authority as a key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and the digital signature. And public key can be distributed to the public.

**RC2:** Short for Rivest Ciphers 2, is a symmetric encryption algorithm by Ron Rivest.

**Router:** A device that connects any number of LANs. Routers use headers and a forwarding table to determine where packets go, and they use ICMP to communicate with each other and

configure the best route between any two hosts.

**RSA:** RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is based on the fact that there is no efficient way to factor very large numbers. It's an asymmetric encryption.

**SMTP:** Short for Simple Mail Transfer Protocol, a protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP.

**S/MIME:** S/MIME is short for Secure Multipurpose Internet Mail Extensions. It is a specification for secure electronic messaging. The specification was designed to be easily integrated into e-mail and messaging products. S/MIME builds security on top of the industry standard MIME protocol according to an equally important set of cryptographic standards, the Public Key Cryptography Standards (PKCS).

**Sock:** Sock is a Circuit-level gateway. It applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

**SSL:** SSL (Secure Sockets Layer) is a commonly used protocol for managing the security of a message transmission on the Internet. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers.

**URL:** A URL (Uniform Resource Locator) is the address of a file (resource) accessible on the Internet. The URL contains the name of the protocol required to access the resource, a domain name that identifies a specific computer on the Internet, and a hierarchical description of a file location on the computer.

## Reference 2: Standards Compliant in EverLink CA Server

	NAME	STANDARD	IMPLEMNET	
1	DES	FIPS PUB 46-3	ALL	Data Encryption Standard
2	3DES		ALL	Triple DES EDE
3	RC2	RFC 2268	ALL	RC2 Encryption
4	AES	AES PROPOSAL	ALL	AES Proposal: The Rijndael Block Cipher
5	RSA	RFC 2437	ALL	RSA Cryptography Specifications Version 2.0
6	SSL	INTERNET DRAFT	VERSION 3.0	Secure Sockets Layer version 3.0
7	PKCS1		ALL	RSA Encryption Standard
8	PKCS3		ALL	Diffie-Hellman Key-Agreement Standard
9	PKCS5		ALL	Password-Based Cryptography Standard
10	PKCS7		ALL	Cryptographic Message Syntax Standard
11	PKCS8		ALL	Private-Key Information Syntax Standard
12	PKCS10		ALL	Certification Request Syntax Standard
13	PKCS11		ALL	Cryptographic Token Interface Standard

14	PKCS12		ALL	Personal Information Exchange Syntax
15	PKI		PHASE3	Public Key Infrastructure
16	X.509	ITU-T X.509	ALL	Information Technology - Open System Interconnection – The Directory: Authentication Framework
17	X.500	ITU-T X.501	ALL	Information Technology – Open System Interconnection – The Directory: Models
18	ASN.1	ITU-T X.680	ALL	Information Technology – Abstract Syntax Notation One (ASN.1): Specification of Basic Notation
19	CMS	RFC 2630	ALL	Cryptographic Message Syntax
20	HTTP	RFC 2616	VERSION1.1	Hypertext Transfer Protocol – HTTP/1.1
21	POP3	RFC 1939	ALL	Post Office Protocol – Version 3
22	SMTP	RFC 821	ALL	Simple Mail Transfer Protocol
23	ARPA NTM	RFC 822	ALL	Standard for The Format of ARPA Internet Text Messages
24	MIME	RFC 1521	ALL	MIME (Multipurpose Internet Mail Extension) Part One: Mechanism for Specifying and Describing the Format of Internet Message Bodies