

Data Security & Privacy Certification
Technical Certification Study Guide



Technical Study Guide

Demonstrate your sales and technical knowledge by participating in the Echworx Data Security & Privacy Certification (DSPC) Program

The Importance of Data Security

- Securing company and customer data is vital to an organizations success
- Many organizations today are ill prepared to deal with identity theft, data thieves, etc
- According to IDC data breaches are more costly than ever:
 - *“... it costs \$6.6 million to rebuild your brand image and retain customers for a typical 1000 employee company”*

Encrypted Data

- The most effective way to achieve data security is to encrypt all confidential information
- Data and email encryption can be hard for companies to understand and deploy
- A managed service model is the easiest way to get encryption deployed within an organization
- Using FTP (File Transfer Protocol) to send large amounts of data across the Internet is not secure

Securing Confidential Information

- **Customer Information**
 - Securing customer information should be the # 1 priority for any business
 - Without customers there is no business
 - Without data security customers will take their business elsewhere
 - Securing customer data results in happy customers

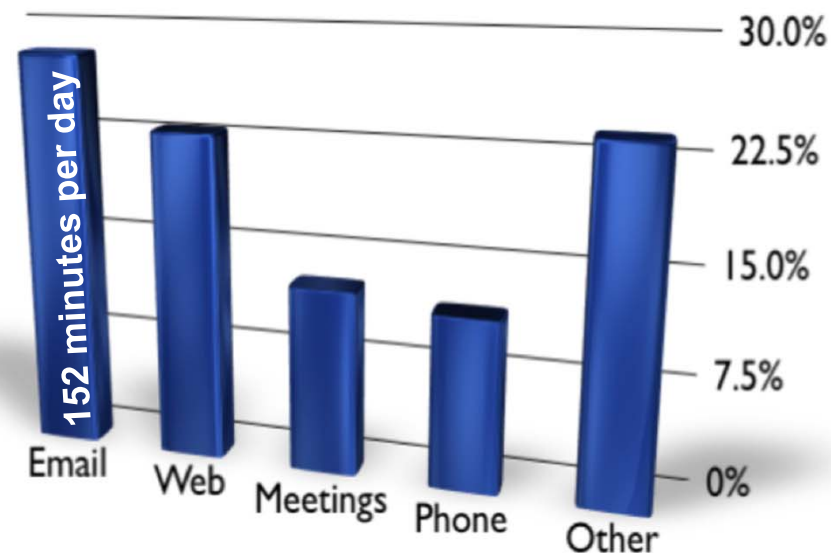
- **Product Information**
 - Protecting product information is a high priority in any organization
 - Protect product information from competitors looking for the next big idea
 - Protect intellectual property from prying eyes

- **Employee Information**
 - Protect employee information such as social security numbers, addresses, telephone numbers, and employment records

- **Company Information**
 - Protect company information such as financial and other business data
 - Leakage of this data could harm a company's reputation and can result in legal action

Why Encrypt Email?

- Email is still the number one business communication tool
- Workers spend 152 minutes per day on average on email

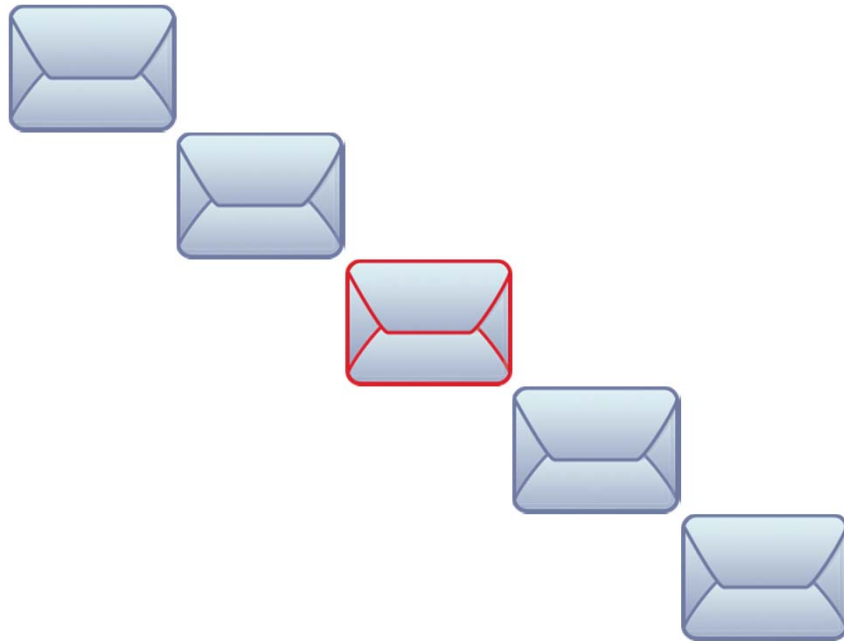


Source: Forrester Research 2009

Why Encrypt Email?

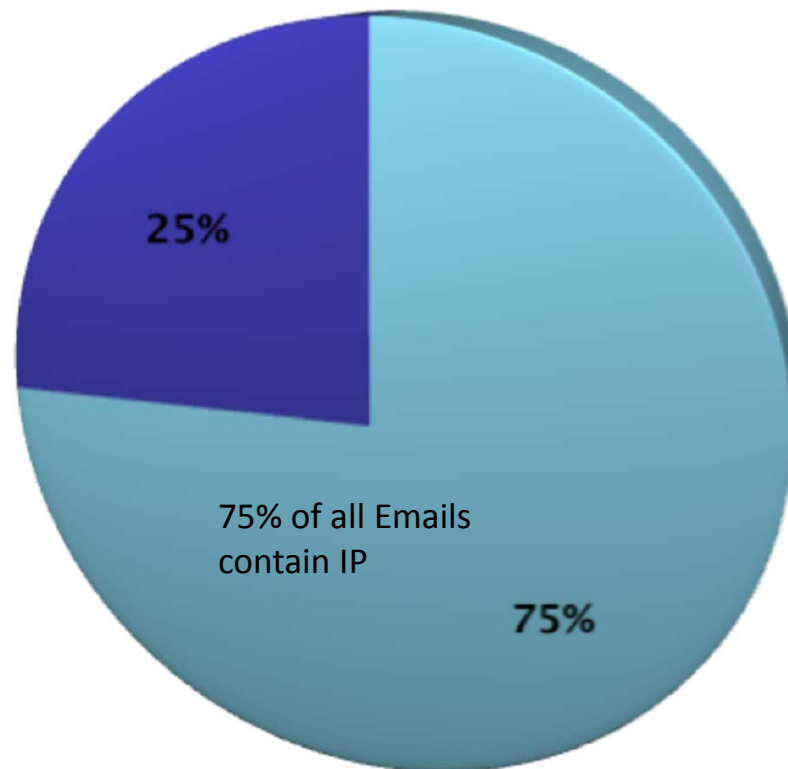
- 1 in 5 outgoing emails contain content that poses a legal, financial, or regulatory risk

Source: Forrester Research 2009



Why Encrypt Email?

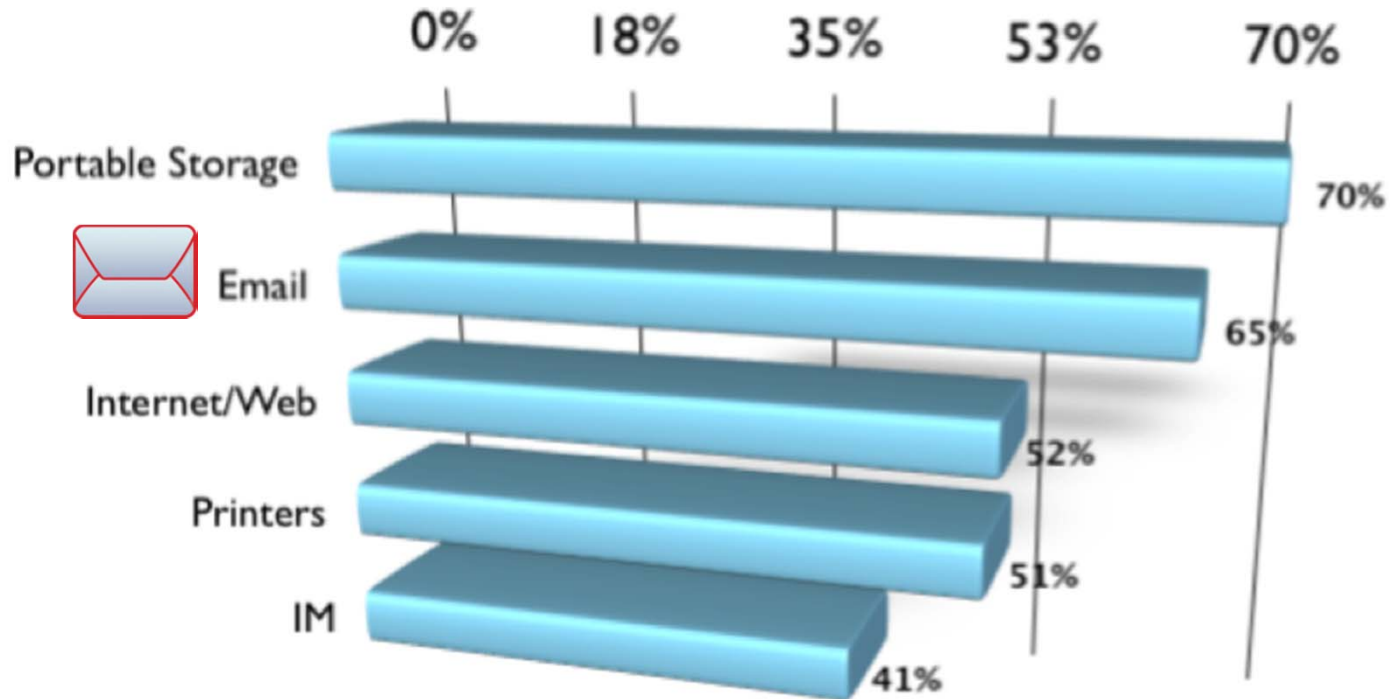
- 75% of all Email contain some Intellectual Property



Why Encrypt Email?

- Email continues to be one of the Most common data leakage channels

Source: Forrester Research 2009



Data Security Goals for all Organizations

1. Know who you are dealing with (Authentication)
2. Keep private information private (Confidentiality)
3. Ensure people don't cheat (Non-Repudiation)
4. Ensure information has not been altered (Integrity)



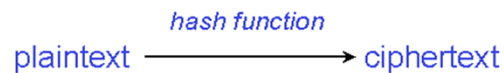
What is Cryptography?



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.



B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.



C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

- Cryptography is the practice and study of hiding information by using mathematical operations to protect data and messages traveling between parties or stored on computers.
- Before the modern era, cryptography was concerned solely with message confidentiality (i.e., encryption) — conversion of messages from a comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge (i.e. the key needed for decryption of that message).

What is Cryptography?

- Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans.
- It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.

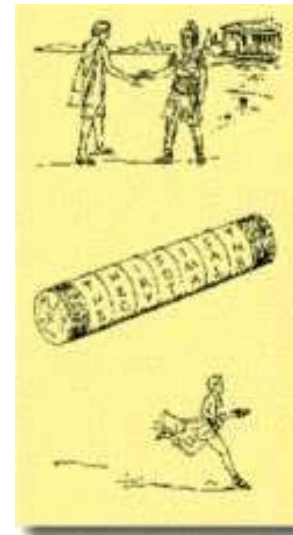
Cryptography throughout History

- In 2000 B.C. substitution of Hieroglyphics were used by the Egyptians to communicate securely amongst themselves.
- The Ancient Chinese used Cryptography first to transform messages in Ideographs for privacy.
- Around 1500 B.C. in India used “Networks spies” using phonetics encryption (Javanese or reverse speaking) to communicate securely.



Cryptography throughout History

- The ATBASH cipher: In the Bible
 - ABCDEFGH... (clear)
 - ZYXWVU...(encrypted)
- Skytale Cipher (Greek)
 - key: stick
 - papyrus enrolled
- Polybius square (Greek)



	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

What is Encryption?

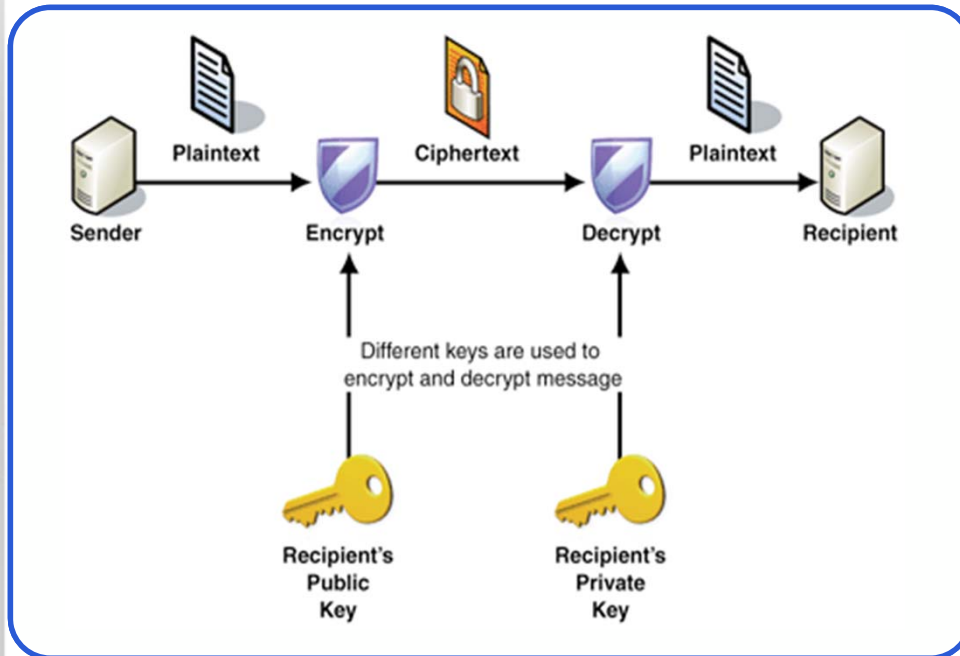


- Encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.
- Another way to look at Encryption is by thinking of it as a process of converting Plaintext into an unintelligible form using a set of procedures and algorithms.
- Plaintext is used as input to an encryption algorithm, the output is usually called ciphertext particularly when the algorithm is a cipher.
- The use of encryption/decryption is as old as the art of communication. As an example, the Egyptians used Encryption to securely communicate with each other in wartime.
- Cryptographic techniques have been used for centuries to protect important information from prying eyes.
- Encryption is used to provide confidentiality and integrity protection
- Digital Signatures are used to provide authentication, integrity protection and non-repudiation
- Checksums / hash algorithms are used to provide integrity protection and can provide authentication

Types of Encryption

- There are 2 main types of encryption including
 - Symmetric Encryption
 - Asymmetric Encryption
- Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.
- The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it.
 - Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key.
 - This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

More on Asymmetric Encryption



- Asymmetric algorithms use a different key for encryption and decryption.
- With Asymmetric encryption models, the encryption key is known as the public key because it is the recipient's public key that is used to encrypt an email.
- Asymmetric Encryption is the premise for PKI (Public Key Infrastructure) based Email Encryption technologies.

Different Types of Email Encryption

- S/MIME or Secure/Multipurpose Internet Mail Extensions is a form of Email Encryption that is included in several email clients by default (such as Outlook Express and Mozilla Thunderbird) and relies on the use of a Certificate Authority (CA) to issue a secure email certificate.
 - To use S/MIME, a sender gets a certificate issued by a CA that is "installed" on the computer. You then email anyone you are likely to want to send encrypted email to and Digitally Sign your email. Once the other person has a copy of your Digital Signature, they are able to use their S/MIME certificate to encrypt email to you. You need to have both the sender's certificate and the recipient's Digital Signature on your computer in order to send encrypted email.
- Another type of email encryption model is PGP. PGP takes a de-centralized approach to email encryption. It does not rely on trusting a Certificate Authority, rather the users create encryption keys themselves. This allows you to choose key size (minimum 1024bit, maximum normally 4096bit), you can choose an encryption/signing algorithm (eg. RSA, DSA or El Gamal) and you are able to set your own expiry date. The problem with PGP is that it is complicated to setup and use for the normal user.
- A less secure form of email encryption is also using Transport Layer Security (TLS) or Secure Socket Layer (SSL) to encrypt messages from one server to another.

Introduction to Public Key Infrastructure (PKI)

- The aim of PKI is to integrate all components of encryption mechanisms and algorithms into a coherent and efficient structure.
- If done right, it will answer the following fundamental security needs:
 - Authentication
 - Confidentiality
 - Non-Repudiation
 - Integrity
- The basis of PKI relies on the concept of digital certificates.

A Certificate is like a Passport.

A Digital Certificate is like a Passport!

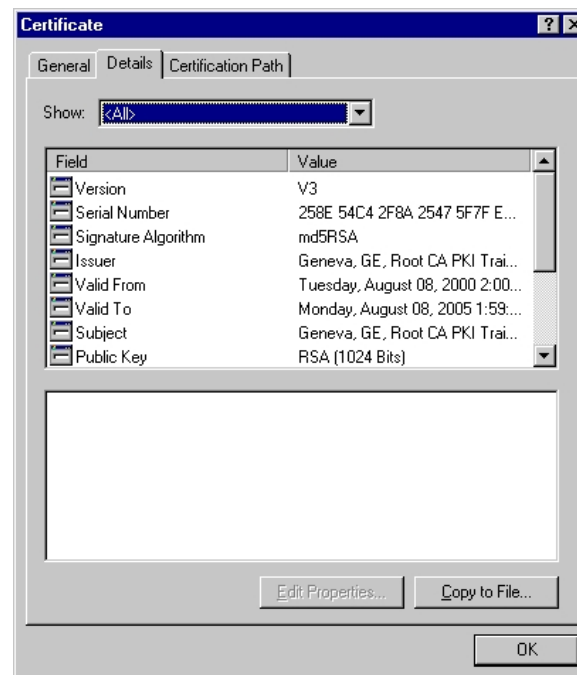
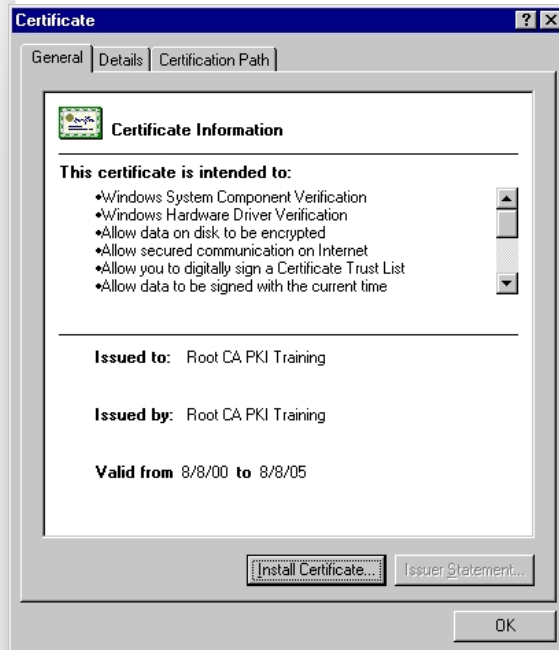


Applying for a Certificate

- As with passports, you give proof of your identity to an official (or trusted) authority.
- The authority checks this proof.
- The authority delivers a signed passport .
- This procedure is defined as an “enrollment”
- Instead of “enrolling” for a passport we’ ll enroll for digital certificate.

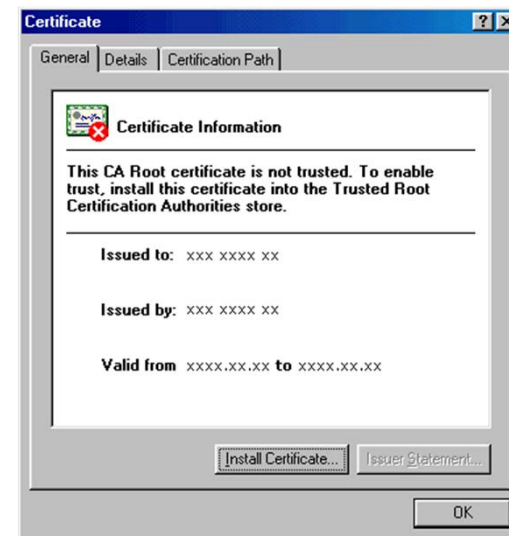


What does a digital certificate look like?



Digital Certificates

- A public-key certificate is a bond between an entity's public-key and one entity.
- The entity can be:
 - A person
 - A role (Manager Director)
 - An organization
 - A piece of hardware (Router, Server, IPSEC, SSL, etc.)
 - A software process (JAVA Applet)
 - A file (Image, Databases, etc.)



Digital Certificates

- A Public-key certificate provides assurance that the public-key belongs to the identified entity.
- A Public-key certificate is also called a digital certificate, digital ID or certificate.
- The entity identified is referred to as the certificate subject.
- If the certificate subject is a person, it is referred to as a subscriber.



Digital Certificate Standards

- Organizations had to think about common public key techniques and key exchanges and sharing when sending keys from their company to another.
- Hence, the PKCS (Public Key Cryptography Standards) and X.509 standards were born.
- RSA Security and its research division, RSA Labs, were interested in promoting and facilitating the use of public-key techniques. To that end, they developed the PKCS standards. They retained control over them, announcing that they would make changes/improvements as they deemed necessary.



PKCS

- Public Key Cryptographic Standard (PKCS)
 - Standardization of public-key algorithmic, in order to maintain interoperability.
 - Developed by RSA Laboratories, a consortium of information technology vendors and academic institutions.
 - Apple
 - Microsoft
 - Compaq
 - Lotus
 - Sun
 - MIT etc.

PKCS List

- PKCS #1: Encrypting and signing using RSA public key crypto-system
- PKCS #3: Key agreement with Diffie-Hellman key exchange
- PKCS #5: Encrypting with a secret key derived from a password
- PKCS #7: Syntax for message with digital signature
- PKCS #8: Format for private key information
- PKCS #9: Attribute type for use in other PKCS standard
- PKCS #10: Syntax for certification request
- PKCS #11: Define a crypto programming interface (API for smart cards)
- PKCS #12: Portable format for storing and transporting private keys
- PKCS #13: Encrypting and signing data using elliptic curves cryptography
- PKCS #14: Standard for pseudo number generation
- PKCS #15: Standard to store credentials on tokens

X.509 another standard for digital certificates

- Another standard is X.509 which is an ITU-T (ITU Telecommunication Standardization Sector) standard for PKI in cryptography, which, amongst many other things, defines specific formats for PKC (Public Key Certificates) and the algorithm that verifies a given certificate path is valid under PKI.
- X.509 is a standard for digital certificate by International Telecommunications Union (ITU).
- First published in 1988 (V1.0).
- Version 2.0 (1993) adds two new fields.
- Current version is v3.0 (1996) and allows additional extension fields.

X.509 Certificates

- In a X.509 system, the Certificate Authority issues a certificate binding a public key to a given but unique name in the X.500 tradition, or to an alternate one such as a DNS entry or email address.
- The authenticity of a certificate and the certification authority in turn is dependent on the root certificate, which is integral to the X.509 certification chain model.
- X.509 system also includes the method for CRL - certificate revocation list and implementations.
 - Protocols Supporting X.509 Certificates
 - Transport Layer Security (SSL/TLS)
 - IPSec
 - Secure Multipurpose Internet Mail Extensions (S/MIME)
 - Smartcard
 - SSH
 - HTTPS
 - LDAPv3
 - EAP

Certificate Authorities issue Digital Certs

- CAs are entities that issue and manage digital certificates including
 - maintaining
 - revoking
 - publishing status information
- CAs' security policy is usually defined in the CPS (Certification Practice Statement)
 - Security measures to guarantee CA's integrity
 - Security measures to check enrollment's identity
- Trust level relies upon CPS and not technology

Certificate Authority Security

- PKI security relies on CA's private-key secrecy
 - Should never be accessed
 - Should be backed-up
 - Solution: store it inside dedicated tamperproof hardware



Types of CAs

- Private CAs:
 - Hold by a private entity (Company, Administration, the Military)
- Public CAs:
 - Echoworx, Verisign, Swisskey, GTE, Thawte, Global-sign, Certplus

Registration Authority

- A Registration Authority is the entity receiving the certification requests and managing them before sending them to the CA. RA acts as a front end.
- As in hybrid CAs, the registration authority can be separate from the CA itself. In this case we talk about Local Registration Authority (LRA)
 - Multiple sites for big companies
 - Distributed environment

Certification Revocation

- Certificate Revocation:
 - Mechanism used by the CA to publish and disseminate revoked certificates
- Revocation is triggered in the following cases:
 - Key compromise
 - CA compromise
 - Cessation of operation
 - Affiliation change



Certification Revocation Process

- Several data structures exist to publish revocation
 - CRL (Certificate Revocation List)
 - ARL (Authority Revocation List)
 - CRT (Certificate Revocation Trees) by Valicert
- Also online query mechanisms
 - OCSP (Online Certificate Status Protocol)

Certification Authority Trust

- Because a CA has a certificate itself and represents the highest possible trust level, the CA has its self-signed certificate.
- A self-signed certificate is a Root Certificate or Meta-Introducer.
- A certificate-using application (any X.509 holders) must trust the Root certificate.
- Importing a Root certificate into such an application is called Bootstrapping a CA.

PKI Summary

- Based on Certificates (X.509)
- Trusted third party (CA)
- (L)RA
- CRL
- Data repositories
- PKI is really the mechanism and protocols between all these elements

S/MIME & PKI

- S/MIME or Secure/Multipurpose Internet Mail Extensions is a form of Email Encryption that is included in several email clients by default (such as Outlook Express and Mozilla Thunderbird) and relies on the use of a Certificate Authority (CA) to issue a secure email certificate.
 - To use S/MIME, a sender gets a certificate issued by a CA that is "installed" on the computer. You then email anyone you are likely to want to send encrypted email to and Digitally Sign your email. Once the other person has a copy of your Digital Signature, they are able to use their S/MIME certificate to encrypt email to you. You need to have both the sender's certificate and the recipient's Digital Signature on your computer in order to send encrypted email.

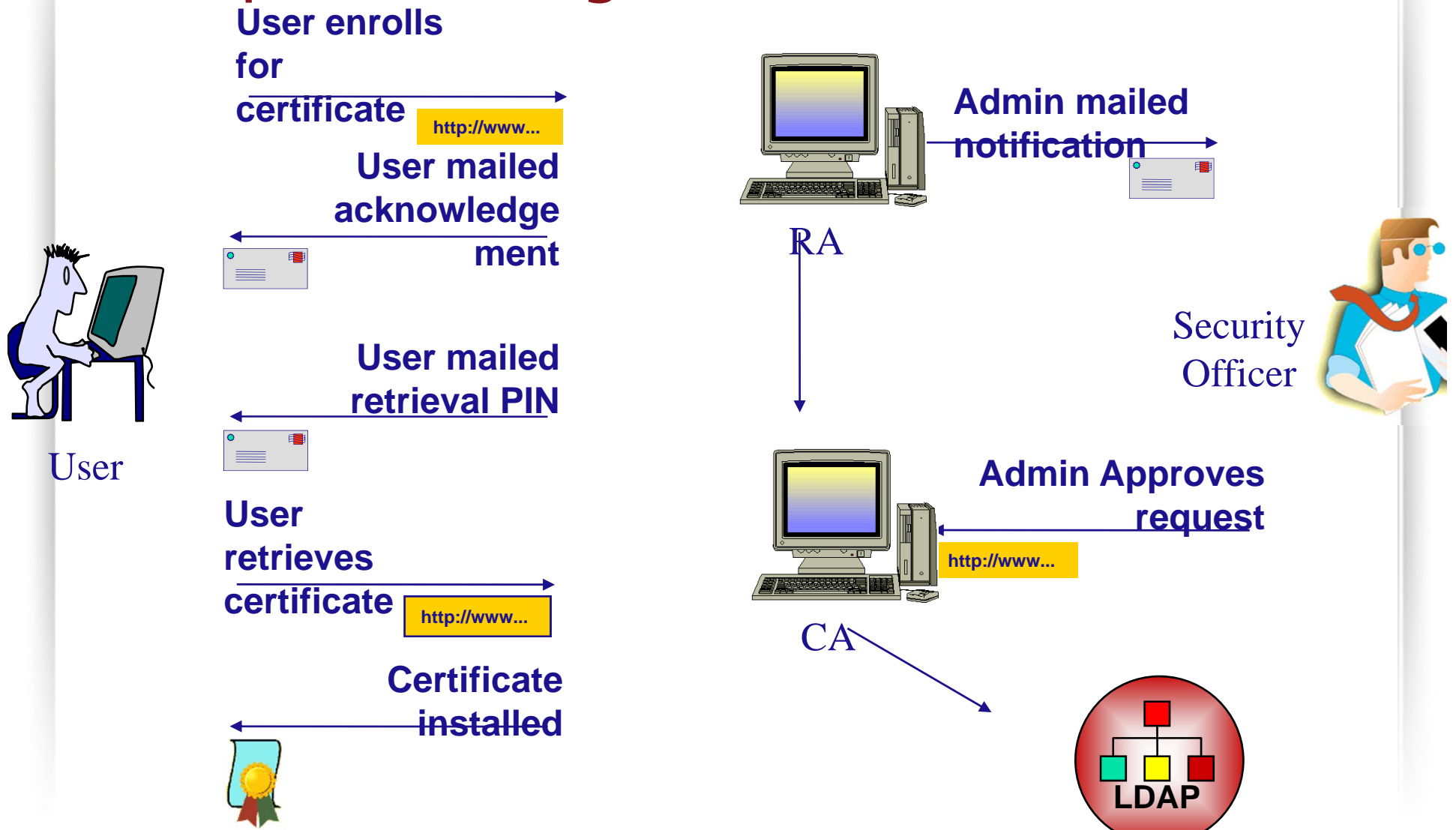
S/MIME & Email Encryption

- Secure Multipurpose Internet Mail Exchange
- Developed by RSA, Microsoft, Lotus, Banyan, and Connectsoft in 1995
- Implemented at application layer
- Build on top of PKCS #7 and PKCS #10
- Very strong commercial vendor acceptance
 - Netscape, Microsoft, Lotus, etc.
- IETF developed S/MIME v3 (last version)
- Use X.509 certificates

Four Services Provided by S/MIME

<i>Security Services</i>	<i>Security Mechanism</i>
Message origin authentication	Digital Signature
Message integrity	Digital Signature
Non-repudiation of origin	Digital Signature
Message confidentiality	Encryption

Let's put it all together



DSPC Summary



- Increase Revenue Opportunity
- Higher Confidence in selling Encryption / Security Services
- Opportunity to use DSPC Logos
- Reference Worthy
- Zero Cost to Certify
- Exclusive Pool of Certified / Qualified Candidates
- Simple Re-Certification Process