

Securing Enterprise Data in the Cyber World

Regional Data Security Summit

Session: Practical Applications of Digital Certificates
(Encryption, Hashing, Digital Signatures &
Key Management)

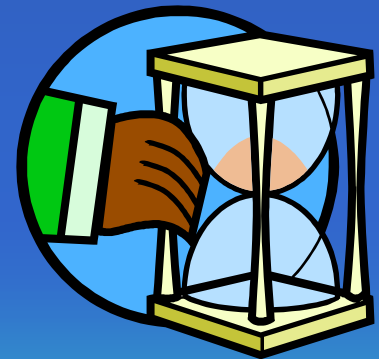


Trevor Libert, CISSP, MBA, MSc
Managing Director
SecureLynX

Objectives

At the conclusion of the session you will have gotten an overview of:

- The components of a Public Key Infrastructure
- The technology behind cryptographic keys for:
 - ❖ Encryption
 - ❖ Digital Signatures
 - ❖ Digital Certificates
- Key Management
- Practical Applications of
 - ❖ Digital Certificates
 - ❖ Digital Signatures



Target Audience

Primary:

- Chief Information Officers
- Heads of Technology
- Security Officers
- Network Administrators
- Application Developers



Agenda

- Introduction
- Internet Security Issues
- Cryptography
- Encryption – An Overview
- Digital Signatures
- Digital Certificates
- Key Management
- Public Key Infrastructure
- Applications of Digital Certificates



Introduction



Cryptography, the art or science of making and breaking ciphers has long been the purview of the military/government--no longer.

It provides

- Encryption and Decryption
- Integrity
- Authentication
- Nonrepudiation

Internet Security Issues

In simple terms the issues that affect today's use of computing technology can be grouped as follows:

- Eavesdropping
- Tampering
- Impersonation
(Spoofing)

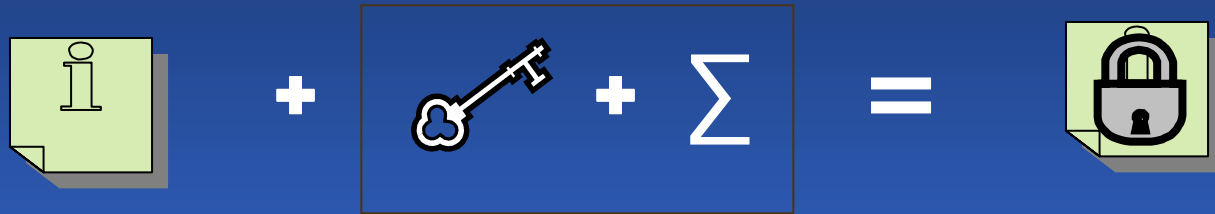


Solutions to Security Requirements



Requirements & Threats	Paper based solutions	Electronic solutions
<ul style="list-style-type: none"> •Confidentiality <ul style="list-style-type: none"> -Eavesdropping 	<ul style="list-style-type: none"> •Envelopes 	<ul style="list-style-type: none"> •Data Encryption
<ul style="list-style-type: none"> •Integrity <ul style="list-style-type: none"> -Tampering 	<ul style="list-style-type: none"> •Signatures, Watermarks, Barcodes 	<ul style="list-style-type: none"> •Digital Signatures, Certificates, Digital Ids
<ul style="list-style-type: none"> •Authenticity <ul style="list-style-type: none"> -Impersonation, Spoofing 	<ul style="list-style-type: none"> •Notary services, physical presence 	<ul style="list-style-type: none"> •Hash Algorithms, Message Digests, Digital Signatures
<ul style="list-style-type: none"> •Non-repudiation 	<ul style="list-style-type: none"> •Signatures, receipts, confirmations 	<ul style="list-style-type: none"> •Digital Signatures, Audit Logs
<ul style="list-style-type: none"> •Availability <ul style="list-style-type: none"> -DDoS 	<ul style="list-style-type: none"> •Alternate routes, sites, etc. 	<ul style="list-style-type: none"> •Redundant Systems

Encryption – An Overview



Plaintext

Key

Algorithm

Ciphertext

Provides:

- Confidentiality
- Authentication
- Integrity



Symmetric Cryptography I

The same key is used for both encryption and decryption.



Symmetric Cryptography II

Features:

- Very fast encryption of bulk data
- Provides confidentiality
- Can be hard to break

Issues:

- Key Distribution
- Scalability
- Limited Security



Asymmetric Cryptography I

Uses a pair of keys, one public and one private.

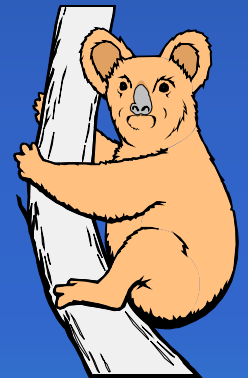


- The private key is known only to the owner.
(e.g., securely stored in a file or a smartcard)
- The public key can be known or made available to everyone.
(e.g., a telephone number in a directory)

Asymmetric Cryptography II

Features:

- Key Distribution and Scalability
- Can provide:
 - Confidentiality
 - Authentication
 - Integrity
 - Access Control



Issues:

- Much Slower than Symmetric systems

The Result – A Hybrid Approach “Public Key Cryptography”



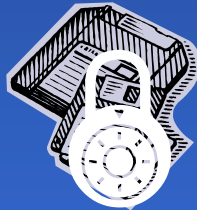
Uses both methods of cryptography

- ❑ Encrypt the data using symmetric cryptography
 - Very fast encryption and decryption
- ❑ Encrypt the symmetric key using asymmetric cryptography
 - Large key size provides excellent security
 - Encrypt symmetric key for multiple users simultaneously

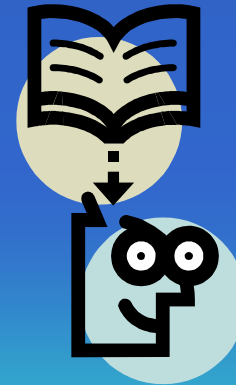
The Encryption Operation



Client software generates a one-time symmetric session key



Symmetric key is used to encrypt the file

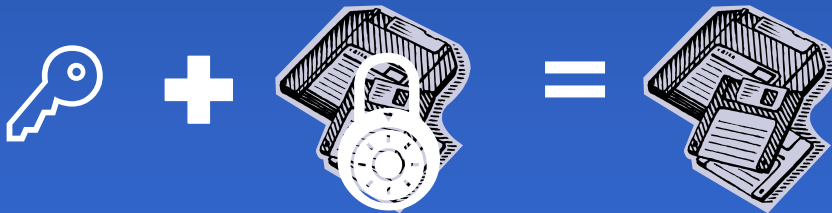


The public key of each recipient is used to encrypt a copy of the symmetric key and BOTH are sent to recipients

The Decryption Operation



The recipient's private key is used to decrypt the symmetric key



The symmetric key is then used to decrypt the file

An output file is generated containing the now decrypted data in its original unprotected form

Hash Functions

When a (mathematical) function is applied to a message, the resulting text is referred to as a hash value or message digest.



Features:

- It uniquely identifies a specific message
- The hashing function is publicly known
- The function is run in only one direction
- It provides integrity, but not confidentiality nor authentication



Digital Signatures

A Digital Signature is an encrypted hash value.

Features:

- Integrity – that the data has not been changed since it was signed
- Authentication – use of the sender's private key
- Confidentiality – the message can be encrypted
- Nonrepudiation – the sender cannot deny sending the message

Digital Signatures

The process:

A one-way hash function is run against the message and then encrypted using the private key of the sender.



Hash function

Message

A hash value is created



Private key

Hash value

The sender's private key is used to encrypt the hash value and produce the digital signature

Applying Digital Signatures

The output file will consist of (3 parts)



Digital
Signature

+



Sender's
public key

+



Original
message

OR



Encrypted
original
message

Part 1

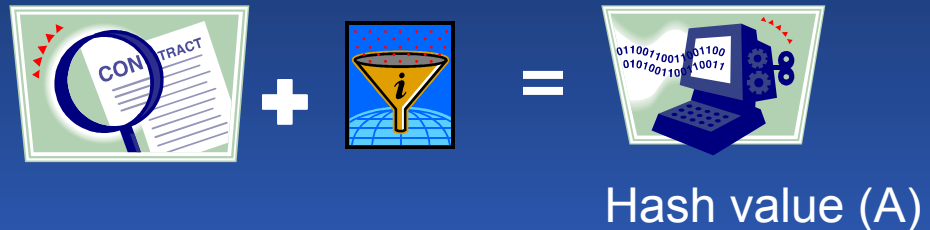
Part 2

Part 3

Verifying Digital Signatures

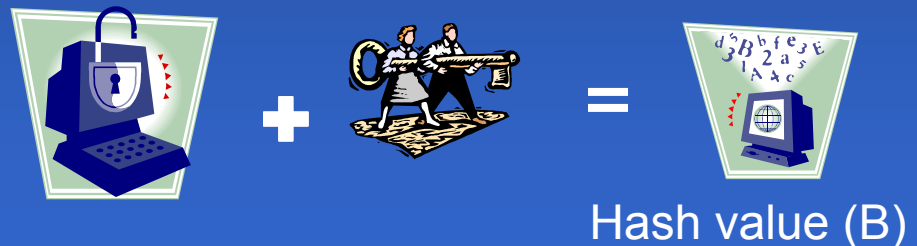
Step 1:

Perform hash on the **original** message



Step 2:

Decrypt the sent hash value (digital signature)



Step 3:

Compare hash values A and B



Key Management - Issues

Cryptography is based on a Trust Model.

We trust:

- ❑ Individuals to protect their own keys
- ❑ Administrators in maintaining the keys
- ❑ The server that holds, maintains and distributes the keys

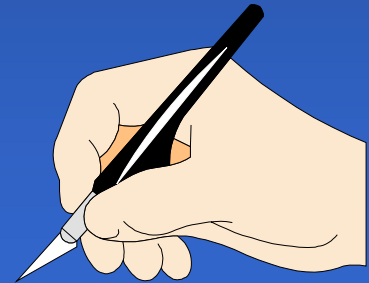
Keys can be:

- Captured
- Modified
- Corrupted
- Disclosed to unauthorized individuals

Key Management - Rules

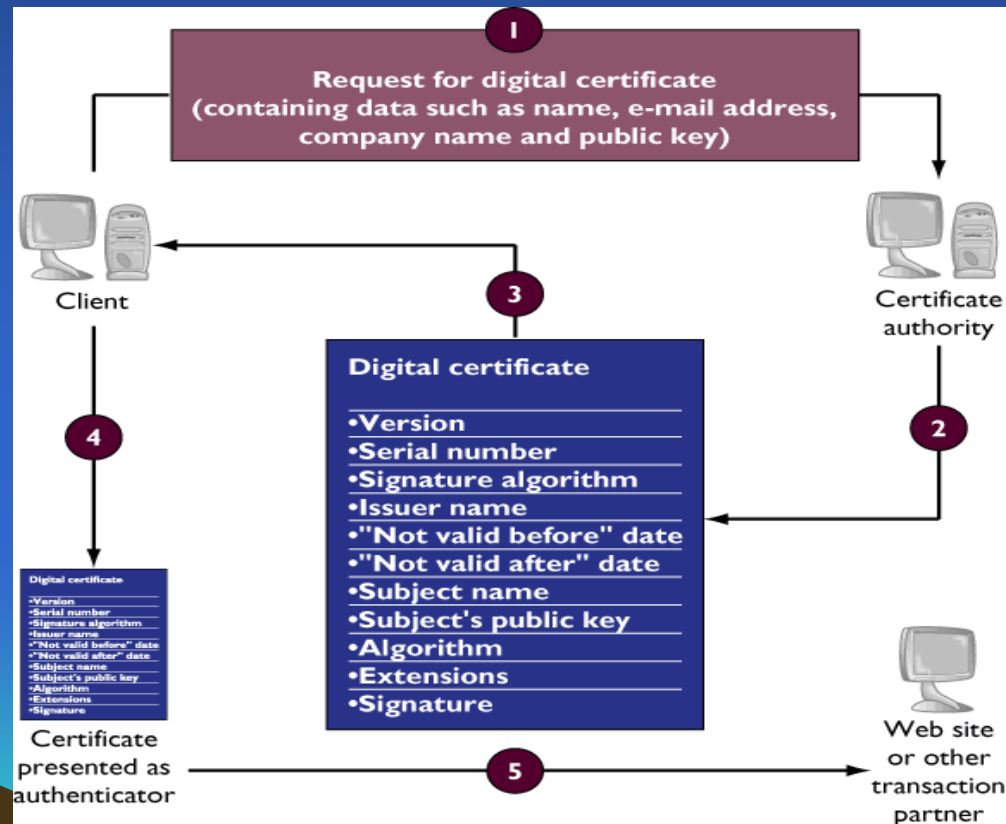
Key Management is the most challenging part of cryptography

- Distribution
- Random
- Key Length
- Secure Backups
- Certificate Revocation List



Digital Certificates

An electronic credential that is used to identify an entity and to associate that entity with a public/private key pair.



Digital Certificates

Features:

- ❑ It is (digitally) signed by a trusted 3rd party or Certificate Authority (CA) verifying the identity of the key owner
- ❑ The CA is an organization that creates, issues, maintains and revokes (if necessary), public key certificates
- ❑ A Registration Authority (RA) performs the certification registration duties on behalf of the CA
- ❑ The RA cannot issue certificates



Types of Certificates

- ❑ Server SSL certificates: Used to identify servers to clients
- ❑ Client SSL certificates: Used to identify clients to servers
- ❑ S/MIME certificates: Used for signed and encrypted email and attachments.
- ❑ Object-Signing certificates: Used to identify the signer of software for distribution over the internet.
- ❑ CA certificates: Used to identify Certificate Authorities.

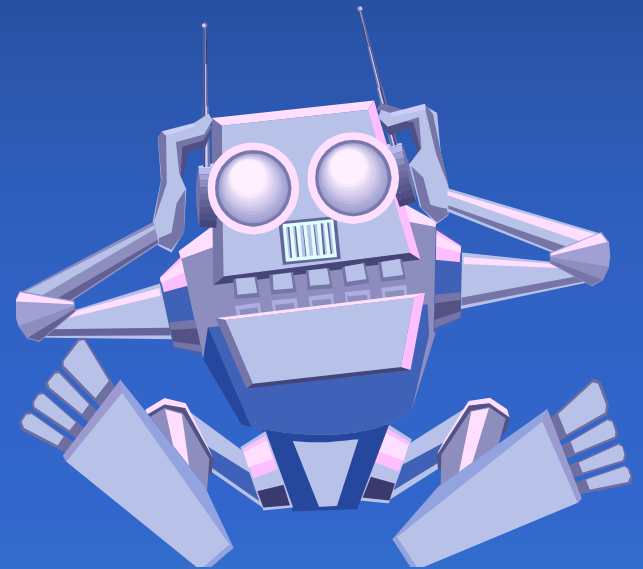
Public Key Infrastructure (PKI)



Putting it all together

This consists of:

- Programs
- Data formats
- Procedures
- Communication protocols
- Security Policies
- Public Key Cryptography mechanisms



Steps in a PKI

A PKI is made up of the following entities and functions:

- Certificate Authority
- Registration Authority
- Certificate Repository
- Certificate Revocation System
- Key Backup and Recovery System
- Automatic Key Update
- Management of Key Histories
- Cross-certification with other CAs
- Time stamping
- Client-side Software



PKI Do's & Don'ts

Do:

- Perform a Risk Analysis
- Know what the problem is
 - What is your specific security problem and how you expect PKI to solve it
- Remember that PKI is 10% technology and 90% policies and procedures
- Get high level (CIO,CEO) support
 - Business needs must drive the security agenda
- Expect to do major infrastructure re-engineering
- Have a budget for the project
- Know that the technology is not the primary issue
- Take significant time to research, plan and design a strategy



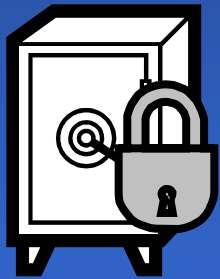
PKI Do's & Don'ts

Don'ts:

- Expect PKI to solve all (or even most) of your security problems
- Get into PKI religious wars (Entrust vs. Verisign, Baltimore vs. Xcert) before performing a complete architecture and technology assessment
- Expect to be successful unless you know why you are deploying this PKI
- Expect to get things working without hiring extra staff
- Believe often exaggerated or useless marketing material
- Pick a PKI vendor until you know your needs

Who is at Risk?

- Customer/User
- Credit Card Companies
- Banks, Insurance Co.'s
- Stock Markets
- E-Businesses
- Online Payment Facilities
- Any Network-based Access to Data



Practical Applications of Digital Certificates

- Secure Web Access
- Signed and Encrypted Email
- Single Sign-On
- Form Signing
- Object Signing



Secure Web Access

Such as Internet Banking/Ins., Money Remittance, Online Stock Trading, Internet Payment/Shopping, E-Bidding, E-Government



Signed and Encrypted Email

Some email programs support digitally signed and encrypted email and attachments using a protocol known as Secure Multipurpose Internet Mail Extension (S/MIME).

Benefits:



- Authentication – confirms the identity of the sender of the email
- Integrity – Alerts the recipient to any changes to the message
- Confidentiality – Since the message was encrypted
- Nonrepudiation – Since message was signed with the sender's private key, s/he cannot deny sending it

Single Sign-On

Such as Multiple Database Servers, Web Portals, Trade Point Initiatives.

Issues:

- Multiple passwords are a headache to remember
- Keeping track (for both Users and System Administrators)
- Choosing poor passwords
- Writing down passwords and storing in obvious places

Single Sign-On solution:

- Users logon once using a single password or certificate
- Get authenticated access to all network resources that the user is authorized to use
- Both client SSL and S/MIME certificates can play a significant role



Form Signing

Some types of e-commerce transactions often involve filling in forms on a web page rather than sending an email.

There must be “hard evidence” that someone has authorized the transaction.



The process:

- When the user clicks the submit button on a web-based form, a dialog box appears that displays the exact text to be signed
- A certificate is selected from among the client SSL and S/MIME certificates that are installed in the browser
- When the user clicks OK, the text is signed, and both the text and the digital signature are submitted to the server.

Object Signing

Most Web browsers and email products support a set of tools and technologies called Object Signing.

Object Signing uses standard techniques to let users get reliable information about the code they download in much the same way they get reliable information about shrink-wrapped software.



Object signing certificates are used to identify the signer of Java code, plug-ins, applets, JavaScript scripts or other signed files.

Conclusions and Recommendations

- ❑ **Proceed slowly**- Take a significant amount of time for research, planning and designing a strategy for a digital certificate implementation
- ❑ Develop a corporate policy for electronic signatures
- ❑ Communicate the policy to all employees and business partners
- ❑ Spell out to the limitations on interpretations of digital signatures for legally binding purposes to employees and business partners
- ❑ Incorporate electronic signature agreement provisions into business contracts
- ❑ Require notice before the use of any electronic signatures is binding on the company
- ❑ Treat electronic signature authorization similar to traditional signature delegation

References

- Shon Harris, “CISSP All-in-One Exam Guide”, McGraw-Hill, 2002
- [Http://developer.netscape.com/docs/manuals/security/pkin/contents.htm](http://developer.netscape.com/docs/manuals/security/pkin/contents.htm)
- Ben Rothe, “ PKI for Dummies”, CSI Security Conference, 2001
- George Dolicker, “Cryptographic Support of E-Business”, CSI Security Conference, 2001
- Andrew Nash, William Duane, Celia Joseph, Derek Brink, “PKI Implementing and Managing E-Security”, McGraw-Hill, 2001
- Christopher King, Curtis Dalton, T. Ertem Osmanoglu, “Security Architecture: Design, Deployment & Operations”, McGraw-Hill, 2001
- Se Hyun Park, “Digital Signature and PKI Technology”, 2004
- John Choi, “Computer Security”, 2004
- InHye Kang, “Network Security Systems”, 2004



Thank You

Q & A



Trevor Libert, CISSP, MBA, MSc
Managing Director
SecureLynX