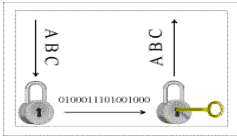


## OVERVIEW OF TECHNOLOGICAL CONTROLS SUPPORTING SECURITY REQUIREMENTS IN PART 11



**Orlando López**

IM Systems Part 11 Remediation  
Program Manager

**McNeil Consumer Healthcare**

---

---

---

---

---

---

---

---

## Objective

- Based on the context of Part 11, review the implementation of **current technologies** mitigating threats and vulnerabilities of computer resources.
  - hashing
  - encryption
  - digital signatures

---

---

---

---

---

---

---

---

## Agenda

- What's the problem?
- Security Regulatory Requirements
- **Review Technologies** (addressed Computer II)
- Implementation Part 11 Security Requirements
- Case Example

---

---

---

---

---

---

---

---

**"I have traveled the length and breadth of this country and talked with the best people, and I can assure you that data processing is a fad that won't last out the year."**

**~ The editor in charge of business books for Prentice Hall, 1957**

---

---

---

---

---

---

---

---

## **Disclaimer....**

- **Cryptography is an arcane field and I don't pretend to be an expert.**
- **Any mention of products or reference to organizations is for information only; it does not imply recommendation or endorsement by McNeil Consumer Healthcare (MCH) or Johnson & Johnson (J&J) nor does it imply that the products mentioned are necessarily the best available for the purpose.**
- **The opinions expressed in this article are strictly those of the author. They in no way represent the view of MCH or J&J.**

---

---

---

---

---

---

---

---

## **References**

- **O. Lopez, Understanding 21 CFR PART 11 for Compliance, SUE HORWOOD PUBLISHING, ISBN 09540706-7-4, URL: [www.euromed.uk.com/shpl\\_publishing.htm](http://www.euromed.uk.com/shpl_publishing.htm)**
- **American Bar Association, *Digital Signature Guidelines*, August 1, 1996, URL: <http://www.abanet.org/scitech/ec/isc/dsg-toc.html>.**
- **American Bar Association, *Public Key Infrastructure (PKI) Assessment Guidelines (Draft)*, June 18, 2001, URL: <http://www.abanet.org/scitech/ec/isc/>**

---

---

---

---

---

---

---

---

## References (cont.)

- **DHHS, 45 CFR Part 142, *Security and Electronic Signature, Standards; Proposed Rule*, August 12, 1998**
- **IEEE Working Groups, *IEEE P1363 Standard Specifications For Public-Key Cryptography*, URL: <http://grouper.ieee.org/groups/1363/index.html>**
- **National Archives and Records Administration, *Records Management Guidance for Agencies Implementing Electronic Signature Technologies*, October 18, 2000**

---

---

---

---

---

---

---

---

## References (cont.)

- **NIST Computer Security Division, URL: <http://www.itl.nist.gov/div893/>**
- **Public-Key Cryptography Standards (PKCS), URL: <http://www.rsasecurity.com/rsalabs/pkcs/>**
- **PKI Forum, URL: <http://www.pkiforum.org>**
- **RFC 2527, *Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework*, URL: <http://www.ietf.org/rfc.html>**

---

---

---

---

---

---

---

---

## References (cont.)

- **RSA, *Understanding Public Key Infrastructure Technology Whitepaper*, URL: <http://www.rsasecurity.com/products/keon/whitepapers/pki/PKIwp.pdf>**
- **The PKI Page, URL: <http://www.pki-page.org>**
- **Windows® 2000 Security Services URL: <http://www.microsoft.com/windows2000/technologies/security/default.asp>**
- **Digital Notary, URL: [http://www.ecom.or.jp/qecom/about\\_wg/wg15/electronic.htm](http://www.ecom.or.jp/qecom/about_wg/wg15/electronic.htm)**

---

---

---


---

---

---

---

---



**What's the problem?**

---

---

---

---

---

---

---

---

**What's the problem?**

- **Security of records in transit / storage**
- **Person / records authentication**

---

---

---

---

---

---

---

---

**Records in transit**

- **The Internet / Intranet provides a convenient medium to connect to other networks, but it does not provide reliable security features, such as entity authentication, or protection from hostile users or software.**

---

---

---

---

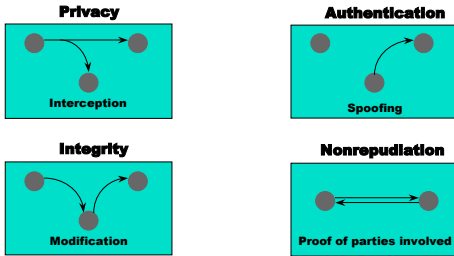
---

---

---

---

## Multiple security issues to be solved




---

---

---

---

---

---

---

---

## What's the problem?

Security of records in storage

---

---

---

---

---

---

---

---

## Sample Threat Rates\*\*



<u>Web Site Hacks</u>	<u>Threat rate</u>
May 1999	12 per day
October 2000	48 per day
March 2001	180 per day
May 2001	580 per day

<u>Internet RATs*</u>	<u>Threat rate</u>
Sep 1999	12 per day
Sep 2000	28 per day
March 2001	122 per day

What's the problem?

\* Remote Access Trojans planted to steal passwords  
 \*\* Statistics by ICSALabs

---

---

---

---

---

---

---

---



## Security Regulatory Requirements

---

---

---

---

---

---

---

---

## Regulatory Requirements

- **21 CFR Part 11**
  - a record rule....
  - trustworthy
    - reliability
    - authenticity
    - integrity
    - usability

---

---

---

---

---

---

---

---

## Part 11 Security Requirements

Part 11	Description	GAMP Technological Controls
11.10(c)	Protection of records	The system should be able to maintain electronic data over periods of many years regardless of upgrades to the software and operating system.
11.10(d)	Access controls	The system should restrict access in accordance with pre-configured rules that can be maintained. Any changes to the rules should be recorded.
11.10(d)	Authentication	
11.10(e)	Audit trail controls	The system should be capable of recording all electronic record creates, update, and delete operations. This record should be secure from subsequent unauthorized alterations.
11.10(e)	Computer systems time controls	
11.10(g)	Authority checks	The system should restrict use of system functions and features in accordance with pre-configured rules that can be maintained. Any changes to the rules should be recorded.
11.10(h)	Device checks	Where pharmaceutical organizations requires that certain devices act as sources of data or commands, the system should enforce the requirement.
11.30	Technical controls to open systems	Not covered by the GAMP
11.70	Signature/record linking	The system must provide a method for linking electronic signatures, where used, to their respective electronic records, in a way that prevents the signature from being removed, copied, or changed to falsely that or any other record.
11.100(a)	Uniqueness of Electronic signatures	The system should enforce uniqueness, prevent relocation of electronic signatures, and prevent deletion of information relating to the electronic signature once it has been used.
11.300	Electronic signatures security	The system should be able to identify changes to electronic records in order to detect invalid or altered records.

---

---

---

---

---

---

---

---

## Paper vs Digital

p  
a  
p  
e  
r

Condition	Solution
Privacy	Envelopes
Authenticity	Notaries, strong ID, physical presence
Reliability	Signatures, watermarks, barcodes
Nonrepudiation	Signatures, receipts, confirmations

d  
i  
g  
i  
t  
a  
l

Condition	Solution
Privacy	Data Encryption
Authenticity	Digital Signatures, Digital Certificates
Reliability	Hash Algorithms, Message Digests, Digital Signatures
Non-repudiation	Digital Signatures, Audit Trails

---

---

---

---

---

---

---

---

## Key condition and solution

- **Authentication** - verifies person identity and integrity of e-records.
- **Encryption** - protect the privacy of e-records.

---

---

---

---

---

---

---

---

## Digital Certificates

- Certificates establish your identity in an electronic world
- They are as important as your passport when traveling
- Certificate ties your identity to a private/public encryption key pair
- With these keys you can
  - Authenticate yourself to applications
  - Encrypt and decrypt e-mail
  - Sign documents

---

---

---

---

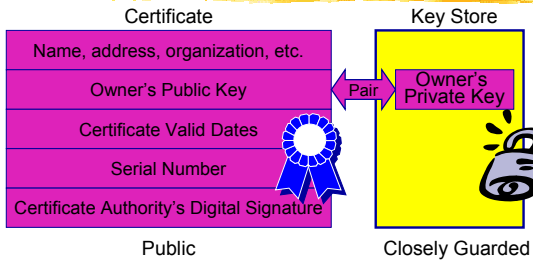
---

---

---

---

## Digital Certificates



**Certificate is publicly available**

---

---

---

---

---

---

---

---

## Authentication, 11.10(d)

- **Two types:**
  - records/messages
  - person
    - Passwords based credentials
    - Certificates based credentials

---

---

---

---

---

---

---

---

## Authentication, 11.10(d)

- **Records/messages authentication**
  - encrypting records/messages using recipients' public-key.
  - employing a session key.

---

---

---

---

---

---

---

---

## Authentication, 11.10(d)

- **Records/messages authentication**



To send private data, encrypt it with the *recipient's* public key

---

---

---

---

---

---

---

---

## Authentication, 11.10(d)

- **Session Key**

- Each session key is only used with one customer during one connection, and that key is itself encrypted with the server's public key.

---

---

---

---

---

---

---

---

## Authentication, 11.10(d)

- **With the latest Secure Sockets Layer (SSL) and a Secure Server Digital ID, a Web site will support the following functions:**

- **Mutual Authentication.** The identity of both the server and the customer can be verified so that all parties know exactly who is on the other end of the transaction.
- **Message Integrity.** The content of all communications between the server and the customer are protected from being altered en route.
- **Message Privacy.** All traffic between the server and the customer is encrypted using a unique "session key."

---

---

---

---

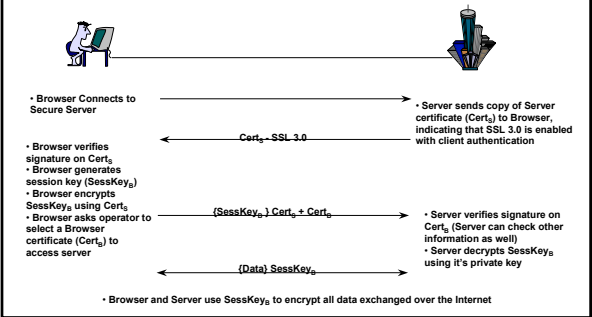
---

---

---

---

# Web-client authentication




---

---

---

---

---

---

---

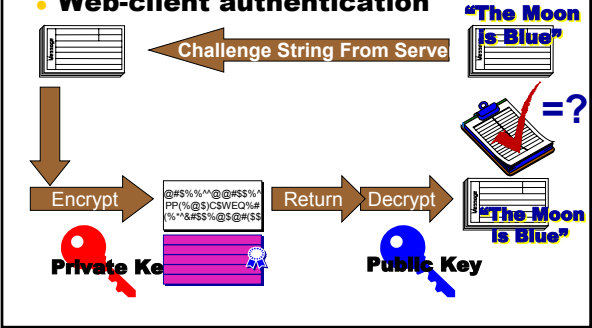
---

---

---

# Authentication, 11.10(d)

## • Web-client authentication




---

---

---

---

---

---

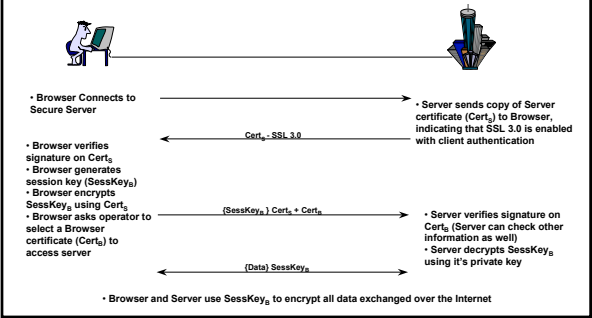
---

---

---

---

# Web-client authentication




---

---

---

---

---

---

---

---

---

---

## Authentication, 11.10(d)

- **Person Authentication**
  - Passwords based credentials or simple authentication
    - ⌘ User ids and static passwords
    - ⌘ User ids and dynamic passwords
      - one-time passwords generators
  - digital certificate-based authentication or strong authentication
    - ⌘ x.509 v3

---

---

---

---

---

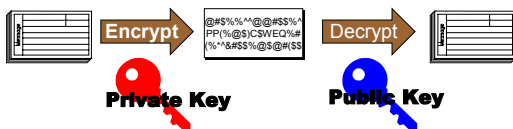
---

---

---

## Authentication, 11.10(d)

- **Certificates based credentials or strong authentication**



This sequence can authenticate the sender

---

---

---

---

---

---

---

---

## Protection of records, 11.10(c)

- **Records in storage** (with/without signatures)
  - access controls
  - encryption
  - hashing
  - consideration -- degradation electronic media
- **Records in transit**
  - encryption
  - SSL, Transport Layer Security (TLS) or VPN
  - Secure/Multipurpose Internet Main Extension (S/MIME)

---

---

---

---

---

---

---

---

## Access Controls, 11.10(d)

- **Preserve confidentiality and integrity of data.**
  - A database server is also commonly used in conjunction with the web server.
- **The primary security concern:**
  - Ensuring that individuals only have access to the computer resources for which they are authorized.

---

---

---

---

---

---

---

---

## Access Controls, 11.10(d)

- **Access right list (ACLs)**
  - authority checks
  - digital certificates
    - ✎ user authentication is the input to the access control decision function(s)

---

---

---

---

---

---

---

---

## Time Controls, 11.10(e)

- **Time stamping**
  - audit trails
  - e-signatures
  - service to support non-repudiation of transactions
- **Digital Time Stamping**
  - hashing => message digest
  - message digest sent to DTS
  - DTS returns a signed time stamp and certification

---

---

---

---

---

---

---

---

## Time Controls, 11.10(e)

- **Local Server**
  - connected to a trusted time site
  - connected to a time calibration service
  - time stamping
    - time
    - message digest
    - time certificate

---

---

---

---

---

---

---

---

## Authority Checks, 11.10(g)

- **Complementary to access and authentication controls**
- **Granting access to correct computer resources and correct level of access**
- **Implementation**
  - ACL
  - authentication, e.g., digital certificates

---

---

---

---

---

---

---

---

## Device Checks, 11.10(h)

- An entity can present a digital certificate to prove their identity or their right to access information.
- It links a public-key value to a set of information that identifies the entity associated with use of the corresponding private key.
- An entity can be a person, server, organization, account, or site.
- The entity is known as the "subject" of the certificate.

---

---

---

---

---

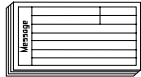
---

---

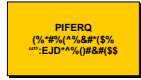
---



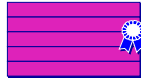
## Complete Signed Document



Document/records



Encrypted Digest



Sender's Certificate

---

---

---

---

---

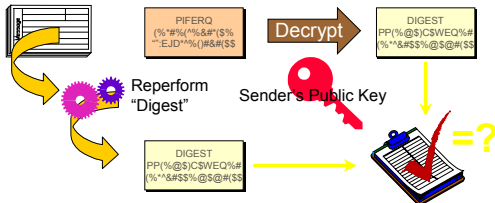
---

---

---

## Verifying a digital signature

### Signed Message



Only the sender's private key can have encrypted a digest that will match

---

---

---

---

---

---

---

---

## Impact of (advanced) linking

- **Changing any document data after capturing the signature, results in a changed and effectively lost encryption key.**
- **Without the original document, you cannot examine, print, or display the signature.**

**This is evidence of a powerful link between data and signature**

---

---

---

---

---

---

---

---

## Uniqueness of electronic signatures

- In digital signatures, the private key is the main element to sign documents/records.
- Users or PKI can generate the key-pairs.
- When generated by PKI, the keys are generated using prime numbers based on ANSI X9.17.

---

---

---

---

---

---

---

---

## Uniqueness of electronic signatures

- The private key is uniquely associated with an entity and is not made public.

---

---

---

---

---

---

---

---

## Security electronic signatures

- Integrity and security of the PKI components.
  - ▣ Integrity of the CA and CARL.
  - ▣ Protection of CSPs and public keys.
  - ▣ Physical and logical security of servers.
  - ▣ Protection of private key
    - ✎ on local disk (encrypted)
    - ✎ in a token

---

---

---

---

---

---

---

---

## Protection of private key

- **Browser Database**
  - ▣ Well supported by IE and Netscape
  - ▣ Not very secure
- **Tokens and Smart Card**
  - ▣ Very secure
  - ▣ Standards are *almost* here
  - ▣ Some compatibility issues

---

---

---

---

---

---

---

---

## Security electronic signatures

- **Integrity and security of the PKI components.**
  - ▣ Tokens or smart cards
  - ▣ 11.300(e)
    - ⌘ Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

---

---

---

---

---

---

---

---

## Qualification

- **IQ infrastructure (HW, SW and procedural controls) in support to encryption and digital signatures**
- **Hashing**
- **Data Encryption**
- **Cryptographic Modules**
- **PKI**
- **Digital Signatures**

---

---

---

---

---

---

---

---

## Operation

- Security Policy
- Protection user's private key
- Keys management
  - generation
  - distribution
  - maintenance
- Periodic audits
- Backups
- Disaster recovery

---

---

---

---

---

---

---

---

## Case Example: Security of records in transit

---

---

---

---

---

---

---

---

## Case: Security of records in transit / storage



QA person sends encrypted and signed email for a drug master production record or a drug batch release authorization.

Email is signed and encrypted



Individual or Organization receives the approved drug master production record or a drug batch

- Decrypts the message
- Checks the authenticity of the sender

"Validate e-mail systems that carry master production records approvals"

Part 11 Compliance Report, 17OCT01

---

---

---

---

---

---

---

---

## Case: Security of records in transit / storage

- 820.75(a)
  - “Where process results cannot be fully verified during routine production by inspection and test, the process must be validated according to established procedures”
  - Process must be validated if:
    - results cannot be fully verified by inspection and test
  - But...encrypted and signed files can be fully verified!



---

---

---

---

---

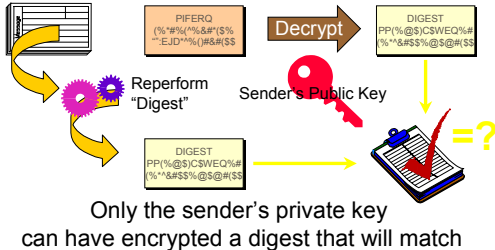
---

---

---

## Verifying a digital signature

### Signed Message



---

---

---

---

---

---

---

---

## Case: Security of records in transit / storage

- Validate e-mail systems that carry master production records approvals?



---

---

---

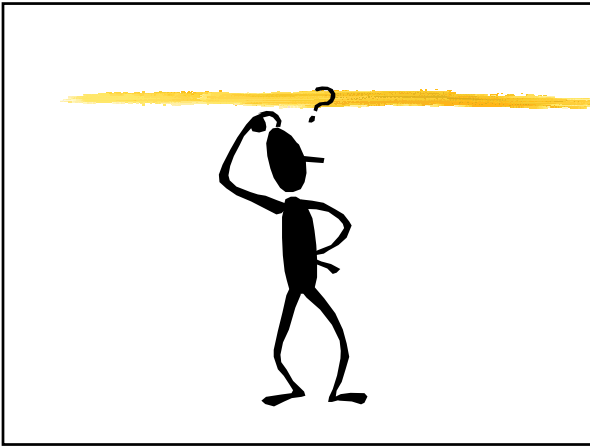
---

---

---

---

---



---

---

---

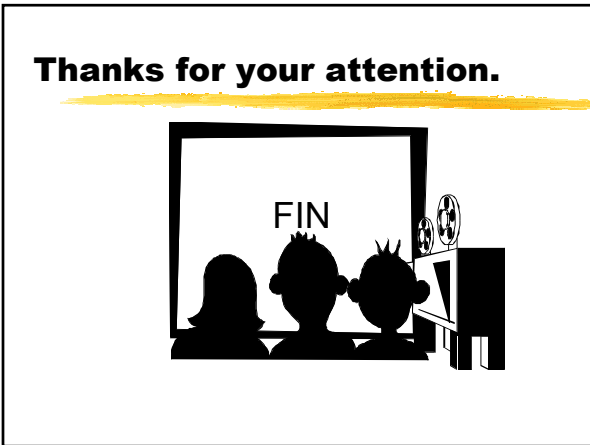
---

---

---

---

---



---

---

---

---

---

---

---

---