PKI

Public Key Infrastructure

PKI: Public Key Infrastructure.

Public key infrastructure (PKI) is cryptography-based technology used to secure electronic processes and transmissions.

WOW!

The percentage of email that is actually readable by an attacker, or that can be manipulated while in transit with little chance of discovery is close to 100%.

Why we “MUST” use PKI

- **PKI Meets HIPAA requirements**

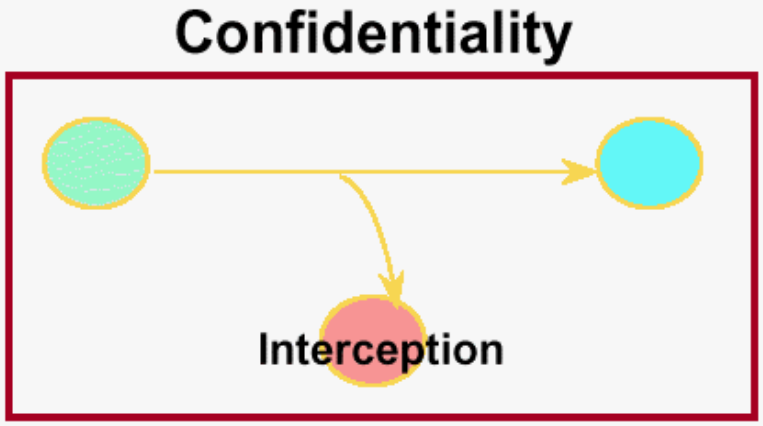
  Because…

- **HCFA, in HHS 45 CFR Part 142 identified PKI as the “most viable technology that will insure the proper level of protection for health care information” and…**

- **HHS 45 CFR Part 142 specifically indicates that its security requirements apply to HIPAA**

Front Page News

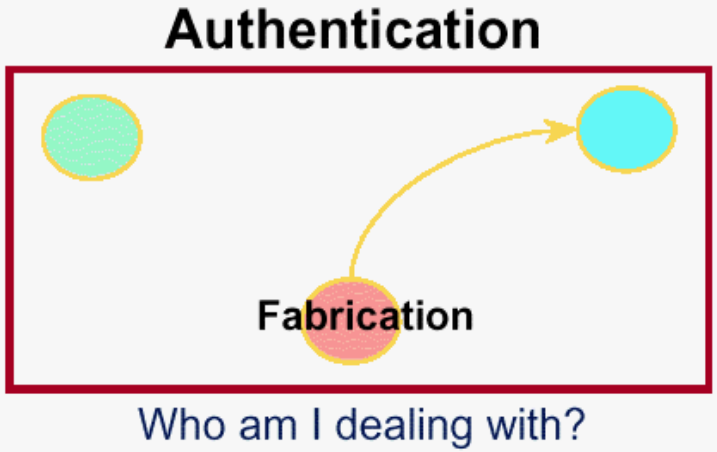
PKI allows you to communicate securely



Is my communication private?

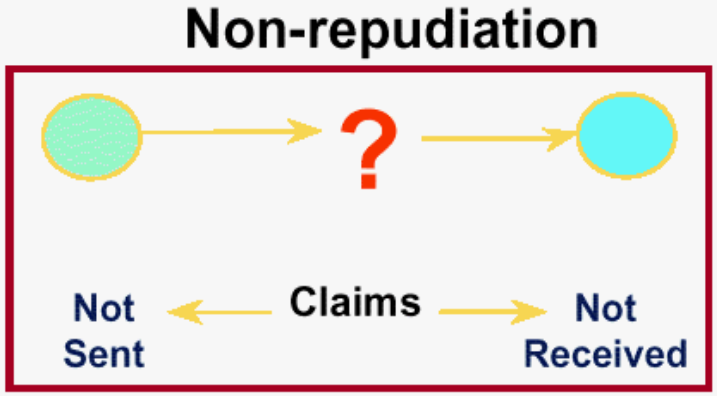
"The property that information is not made available or disclosed to unauthorized individuals, entities or processes." p. 43272

PKI includes the ability to encrypt a message so that only the person the data is meant for can read it



"The corroboration that an entity is the one claimed" p. 43273

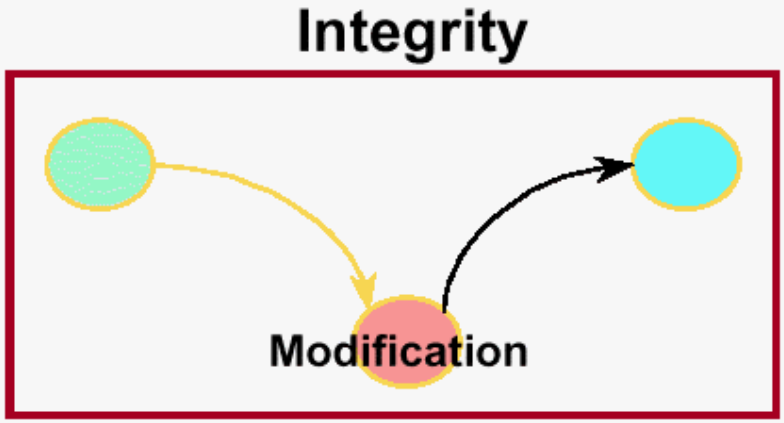
PKI allows you to prove the identity of the sender



Who sent/received it and when?

"Strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents " p. 43274

PKI assures the message wasn't tampered with

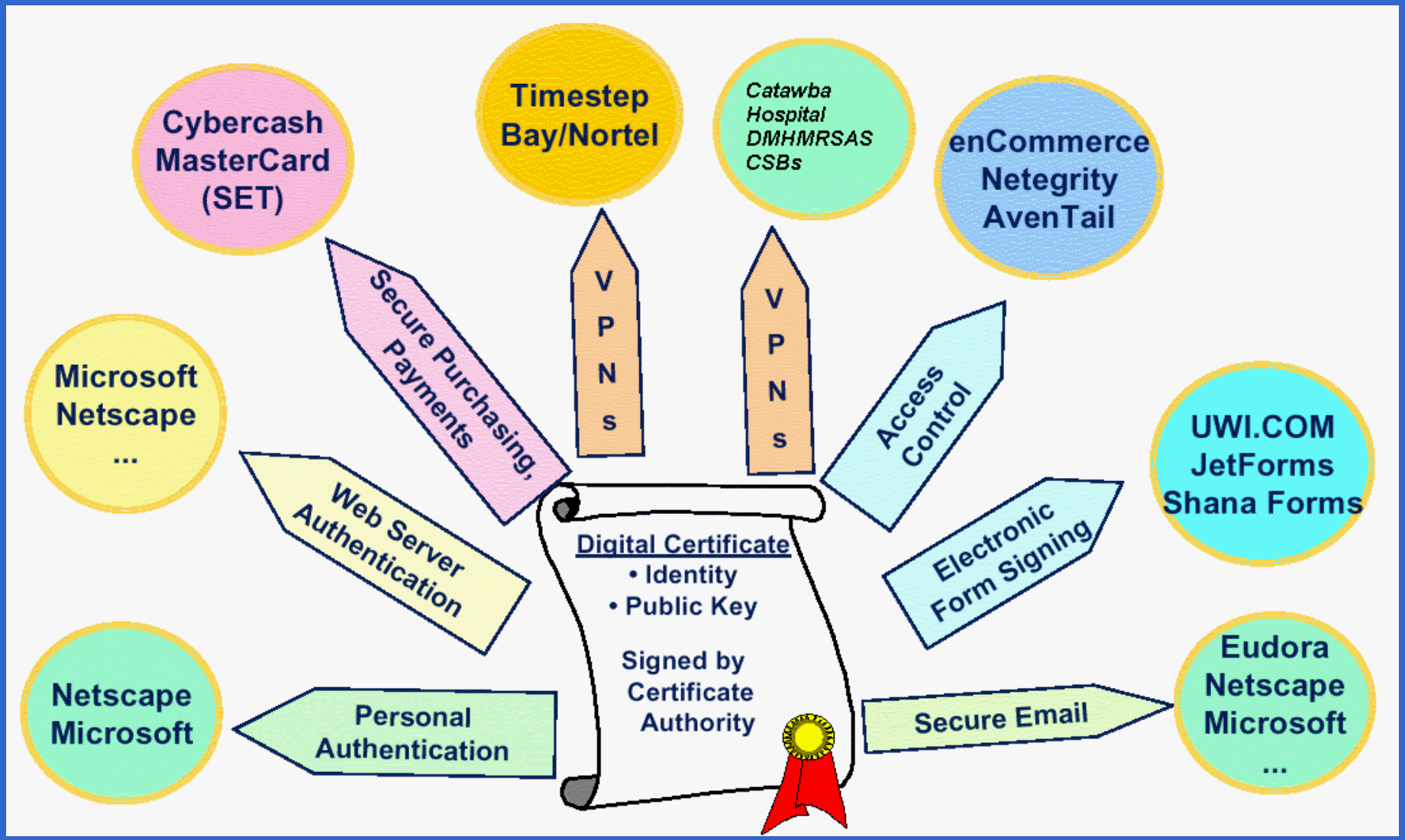


Has my communication been altered?

"Ensuring, typically with a message authentication code, that a message received matches the message sent"

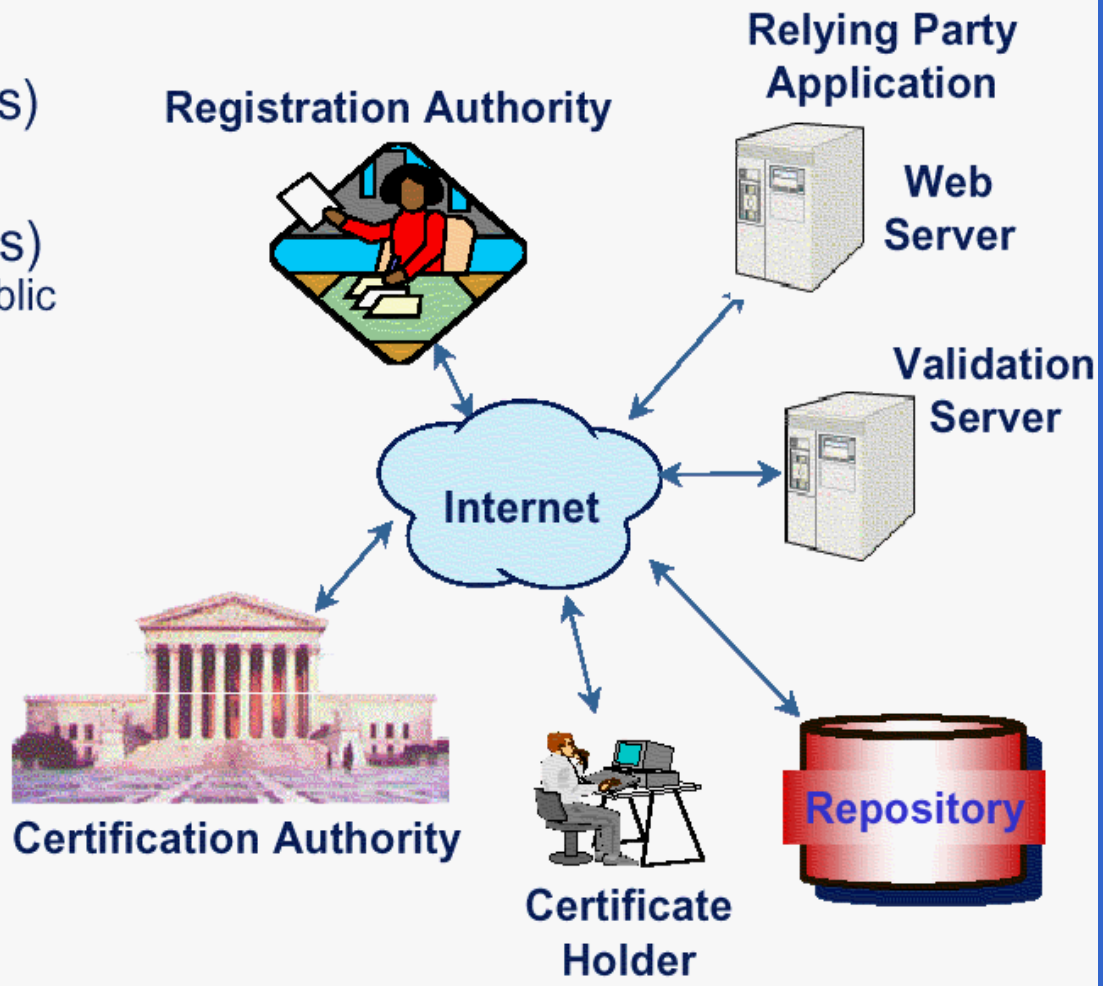
p. 43274

Ways to Use PKI and Digital Certificates



PKI is a framework of servers, products and policies that govern the use, distribution and management of digital certificates.

- Certification Authorities (CAs)
  (Issuers)
- Registration Authorities (RAs)
  (Authorize the binding between Public Key & Certificate Holder)
- Certificate Holders
  (Subjects)
- Relying Parties
  (Validate signatures & certificate paths)
- Repository
  (Store & distribute certificates
- Validation Server
  (Provide certificate status: expired, revoked, etc.)



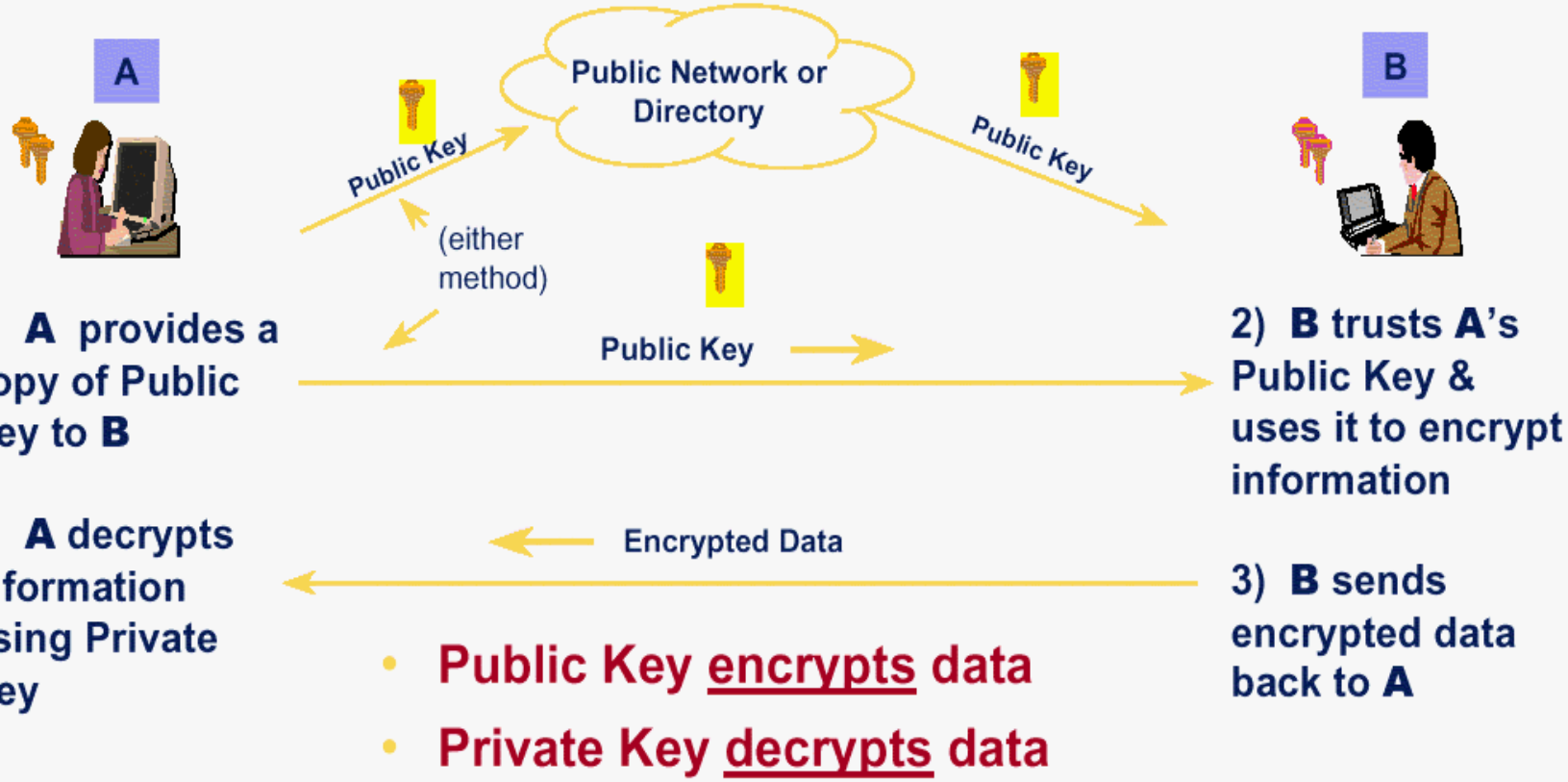
Certificate Authority

- A CA verifies and vouches for the identity information in a Certificate
  - like a Government for passports
  - like a bank for ATM cards
- CA verification techniques:
  - Check existing records - employee databases
  - Examine typical identification - passport, license
  - Background check - government database, personal interview, references, etc.

Public Key Cryptography

Cryptography

Everyone has a Key Pair: Public Key & Private Key



3rd Party Keys

Typically you have trusted 3rd parties (such as Verisign) that have a set of keys that are preinstalled in software (such as web browsers and email clients. Using these keys the third party supposedly checks up on the identity of organizations or people and then signs their public keys, you can verify that signature since the keys required to do so are built into your software (and if you cannot trust your software you've got bigger problems). These 3rd parties also typically run servers that maintain copies of the keys so you can search them, for say "John Parker" entries, and also allow the owner of the key to issue a "revocation" (meaning the key is no longer valid). In a nutshell if Alice trusts Bob, Bob can then verify the identities of Charles and David, Alice can then verify that Charles and David's keys have been okayed by Bob, and use them with a relative degree of safety.

Roll Our Own Keys With the MS Key Management Server

Software Requirements

- Microsoft Windows 2000 Certificate Server
  (Provided with the OS)
- Microsoft Exchange Server
  (DMHMRSAS Standard)
- Microsoft Exchange Messaging and Collaboration Services
  (Provided with the Microsoft Exchange Server)
- Microsoft Exchange Key Management Services
  (Provided with later versions of Microsoft Exchange Server)

Note: Installation of Key Management Server covered in Microsoft Knowledge base article Q267273: XADM: How to Install the Key Management Server (Q267273)

Digital Certificates

An electronic passport that proves your identity and authenticates you

- Who you are
- What your public key is
- Who issued your certificate

Physical World Analogies

ATM Card - a Certificate to conduct electronic banking

Driver's license - a Certificate to operate a vehicle

Employee badge - a Certificate to gain facility access

U.S. Passport - a Certificate telling who you are

Of course the real world is far from perfect.

Simplified

Overview of CA / PKI Rollout

if using the Microsoft Solution

1. DMHMRSAS CO to establish a Certificate Authority "Root Authority Server"
2. Each DMRMHSAS Exchange site (Hospital, etc.) would need to establish a CA server and these servers would need to be AUTHORIZED by the DMHMRSAS root CA server.
3. Each CSB would need to have their own CA server or establish a relationship with a third party CA (Thawte/Verisign).