

PKI & CA

CSH5 Chapter 37

“PKI & Certificate Authorities”

Santosh Chokhani, Padgett
Peterson, & Steven Lovaas

1

Copyright © 2011 M. E. Kabay. All rights reserved.

Topics

- Introduction
- Need for PKI
- Public Key Certificate
- Enterprise Public Key Infrastructure
- Certificate Policy
- Global PKI
- Forms of Revocation
- Rekey
- Key Recovery
- Privilege Management
- Trusted Archival Services & Trusted Time Stamps
- Cost of PKI



2

Copyright © 2011 M. E. Kabay. All rights reserved.

Introduction

- Overview
- Symmetric Key Cryptography
- Public Key Cryptosystem
- Advantages of PKC over SKC
- Combination of the Two



3

Copyright © 2011 M. E. Kabay. All rights reserved.

Overview

- Early days of encryption across Internet
 - ❑ Individuals
 - ❑ Pretty Good Privacy (PGP)
 - ❑ Web of trust
- Today's encryption much more complex
 - ❑ Formalized
 - ❑ Organizational
 - ❑ Fundamentally concerned with trust relationships
- Key applications include
 - ❑ Data in flight (networking)
 - ❑ Data at rest (storage)

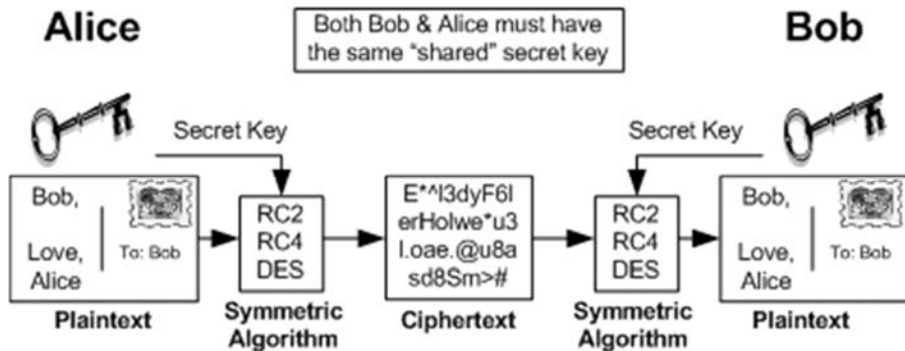


4

Copyright © 2011 M. E. Kabay. All rights reserved.

See CSH5 Chapters
7: Encryption
32: VPNs & Secure Remote Access

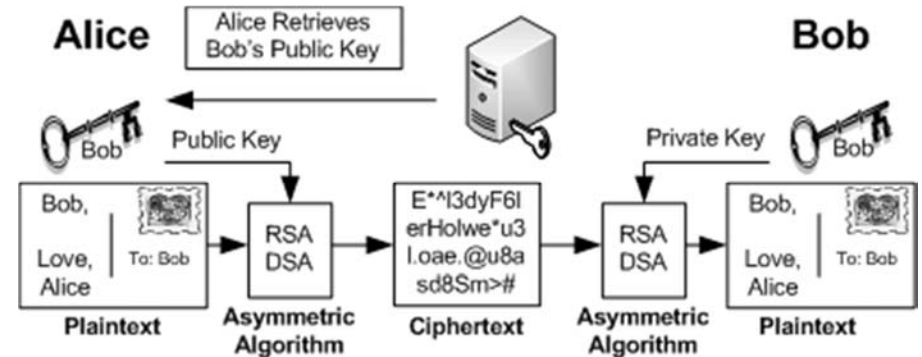
Symmetric Key Cryptography



5

Copyright © 2011 M. E. Kabay. All rights reserved.

Public Key Cryptosystem



6

Copyright © 2011 M. E. Kabay. All rights reserved.

Advantages of PKC over SKC

- PKC requires fewer keys to manage
 - ❑ Total keys $2n$ (Cf SKC with $\frac{1}{2}n(n-1) \approx \frac{1}{2}n^2$)
- Can focus on authenticating only public keys
- No secret keys transmitted over networks
 - ❑ Not susceptible to compromise even if public keys must be changed
- Public keys can be used to encrypt temporary session keys for one-time use
- Session keys allow PKC to encrypt message for multiple recipients easily

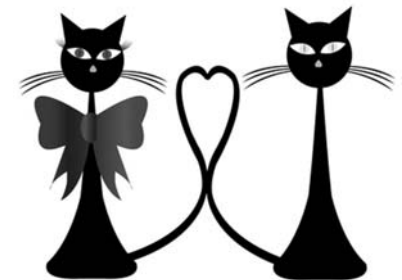


7

Copyright © 2011 M. E. Kabay. All rights reserved.

Combination of the Two

- Usual implementation of PKC uses symmetric algorithm for session key
 - ❑ Computationally less onerous
 - ❑ Encrypt session key with asymmetric key
- Digital signing uses similar method
 - ❑ Encrypt secure hash of document
 - ❑ Decrypt encrypted hash to verify data integrity and authenticity of text



8

Copyright © 2011 M. E. Kabay. All rights reserved.

Need for PKI

- Everything in PKC depends on trustworthiness (authenticity) of the public key (certificate)
 - ❑ If someone posts a public key in victim's name, can
 - ✓ Intercept encrypted content intended for spoofed victim
 - ✓ Issue fraudulent content in victim's name
- Similar problems with Secure Sockets Layer (SSL) v2
- Develop *chain of trust* for certificates (value signed by public keys)



Copyright © 2011 M. E. Kabay. All rights reserved.

Public Key Certificate (1)

- Certification authority (CA) issues signatures for public keys
- Standard is ANSI X.509 (IETF RFC 5280)
 - ❑ Described in Abstract Syntax Notation (ANS.1)
 - ❑ Often encoded in MIME (Multipurpose Internet Mail Extensions) to use only ASCII characters
- Trust the root & you can trust the issued keys



Copyright © 2011 M. E. Kabay. All rights reserved.

Public Key Certificate (2)

Every CA's certificate has list of key info:

- Version #
- Certificate serial #
- Algorithm
- CA name
- Validity period for certificate
- Subscriber name
- Subscriber public key, PK algorithm, parameters
- CA unique ID (optional)
- Extensions (optional)
- CA's digital signature



Copyright © 2011 M. E. Kabay. All rights reserved.

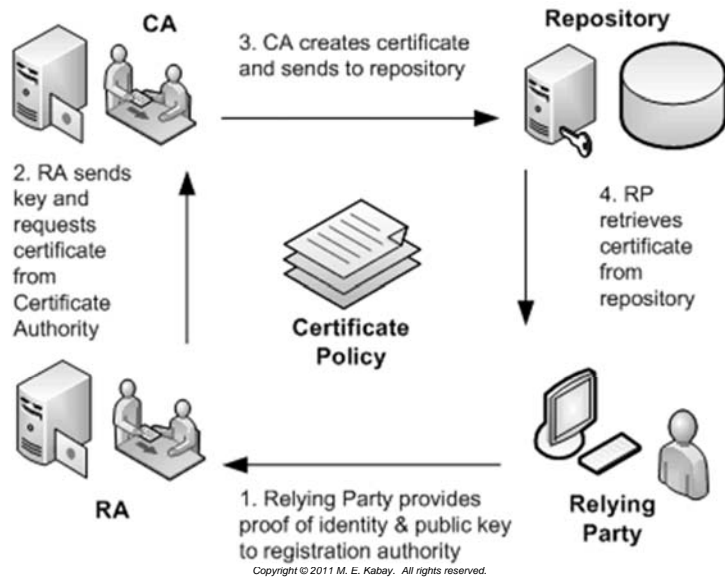
Certificate Revocation List

- CRL is list of revoked certificates
- Must check CRL before trusting public key
- X.509v2 CRL contains
 - ❑ Version # of CRL standards
 - ❑ Algorithm & parameters for CA signature
 - ❑ CA name
 - ❑ CRL issuance time
 - ❑ Next CRL issuance time (optional)
 - ❑ List of revoked certificates with each
 - ✓ Certificate serial #
 - ✓ Time CA notified of revocation
 - ✓ Extensions (optional)
 - ❑ Extensions related to CRL (optional)
 - ❑ CA's digital signature



Copyright © 2011 M. E. Kabay. All rights reserved.

Enterprise Public Key Infrastructure

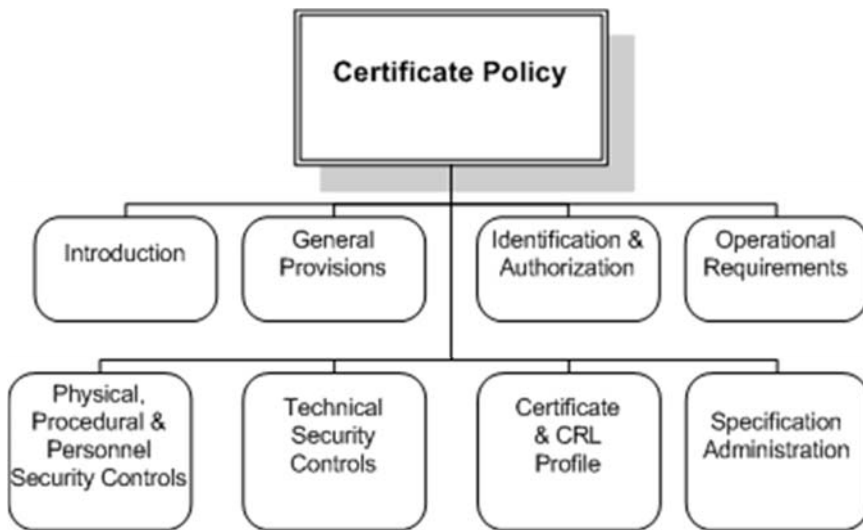


Certificate Policy (1)

- Private keys must be
 - Kept confidential
 - Used only by owners of keys
- *Trust anchors'* public key integrity must be assured
- Initial authentication of subscriber
 - Must be strong
 - Must prevent identity theft at time of certificate creation
- CA & RA (Registration Authority) computer systems must be protected against tampering
- Requirements for level of trust must be defined



Certificate Policy (2)



Global PKI

- Levels of Trust
- Proofing
- Trusted Paths
- Choosing a PKI Architecture
- Cross-Certification
- PKI Interoperability



Levels of Trust

- OMB M04-04 §2.1 basic levels of trust:
 - ❑ Level 1: Little or no confidence in asserted identity's validity
 - ❑ Level 2: Some confidence
 - ❑ Level 3: High confidence
 - ❑ Level 4: Very high confidence

EXHIBIT 37.6 Trust Level Determination

| Category | Required Trust Level | | | |
|---|----------------------|-----|------|----------|
| | 1 | 2 | 3 | 4 |
| Inconvenience or distress | Low | Med | High | High |
| Financial loss | Low | Med | Med | High |
| Harm to agency programs or public interests | N/A | Low | Med | High |
| Personal safety | N/A | N/A | Low | Med/high |
| Civil or criminal violations | N/A | Low | Med | High |
| Information classification | | | | |
| Confidentiality | Low | Med | High | High |
| Integrity | Low | Med | High | High |

Proofing

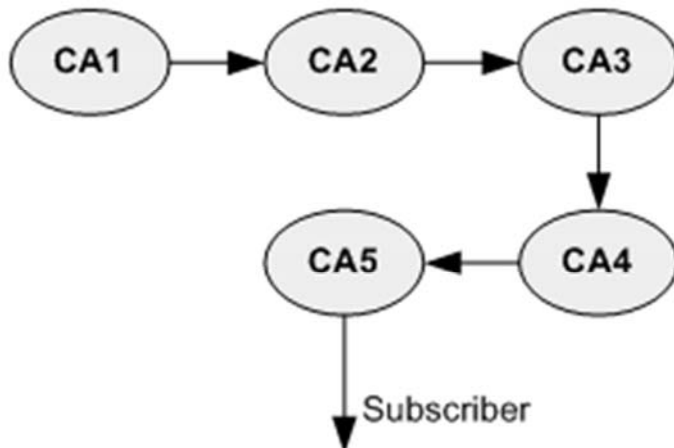
- Vetting (proofing) requires increasingly thorough background checking of identity

EXHIBIT 37.7 Trust Levels and Proofing

| Level | Title | Proofing | Authentication |
|-------|-------------------|--|----------------------|
| 1 | Default | Anonymous allowed. | None |
| 2 | Basic | Simple assertion — may be online. | Password |
| 3 | Medium (software) | 1-9 employment eligibility verification and authorization. Must be in person. | Software certificate |
| 3 | Medium (hardware) | 1-9 employment eligibility verification and authorization. Must be in person. Biometrics may be captured. | Hardware certificate |
| 4 | High | National agency check or local agency check, background investigation, and authorization required. Final proofing must be in person. | Hardware certificate |

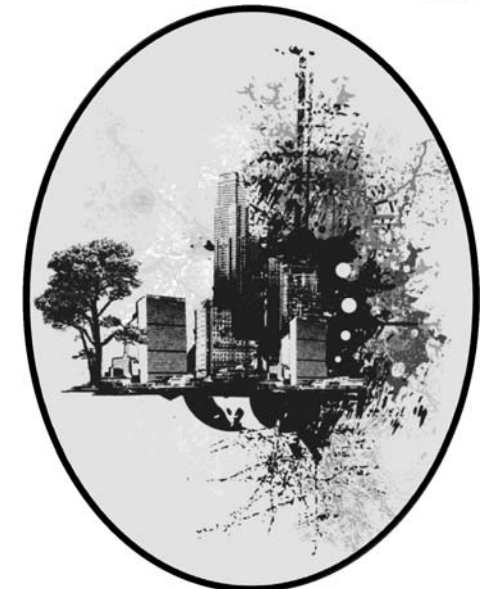
Trusted Paths

Relying Party
Trust Anchor

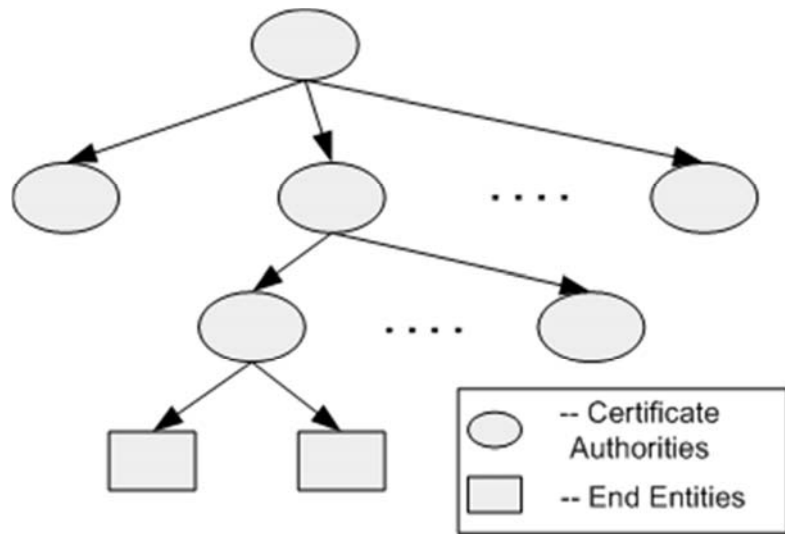


Choosing a PKI Architecture

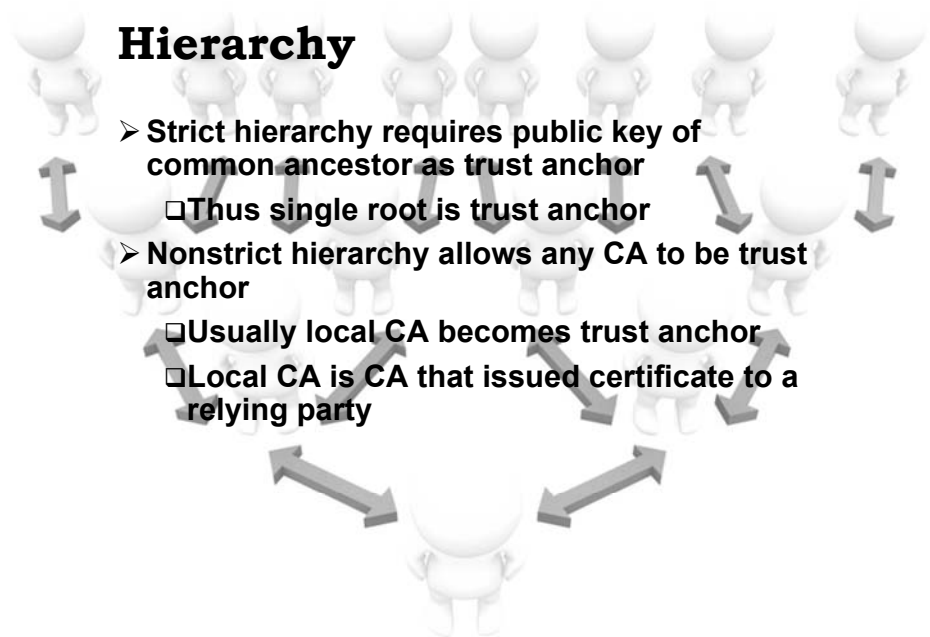
- Strict Hierarchy
- Hierarchy
- Bridge
- Multiple Trust Anchors
- Mesh (Anarchy, Web)
- Making a Choice



Strict Hierarchy

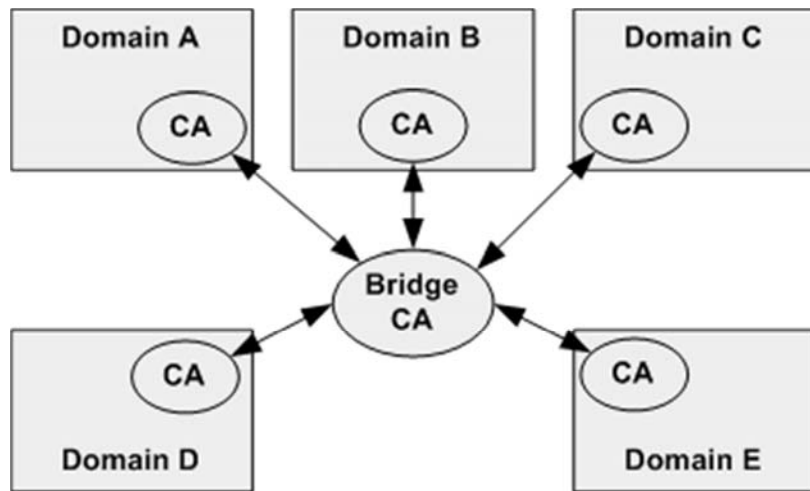


Hierarchy



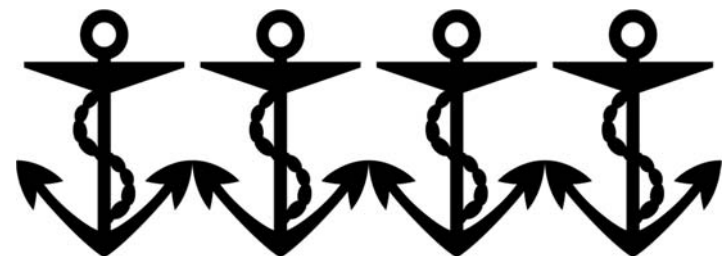
- Strict hierarchy requires public key of common ancestor as trust anchor
 - ❑ Thus single root is trust anchor
- Nonstrict hierarchy allows any CA to be trust anchor
 - ❑ Usually local CA becomes trust anchor
 - ❑ Local CA is CA that issued certificate to a relying party

Bridge



Multiple Trust Anchors

- Relying party obtains public keys of many CAs
 - ❑ Must use secure method
 - ❑ Each key becomes a trust anchor
- Helpful for situations where CAs cannot cross-certify each other



Making a Choice

- Factors
 - Management culture
 - Organizational politics
 - Certification path size
 - Subscriber population size
 - Subscriber population distribution
 - Revocation information
- Often end up with multiple CAs



26

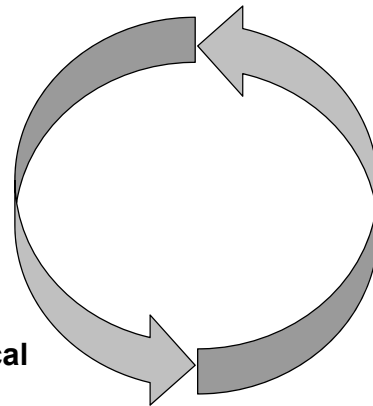
Copyright © 2011 M. E. Kabay. All rights reserved.

Mesh (Anarchy, Web)

- Web of trust
- Any CA can trust any other
- Original concept underlying PGP
- Not scalable (WHY NOT?)

Cross-Certification (1)

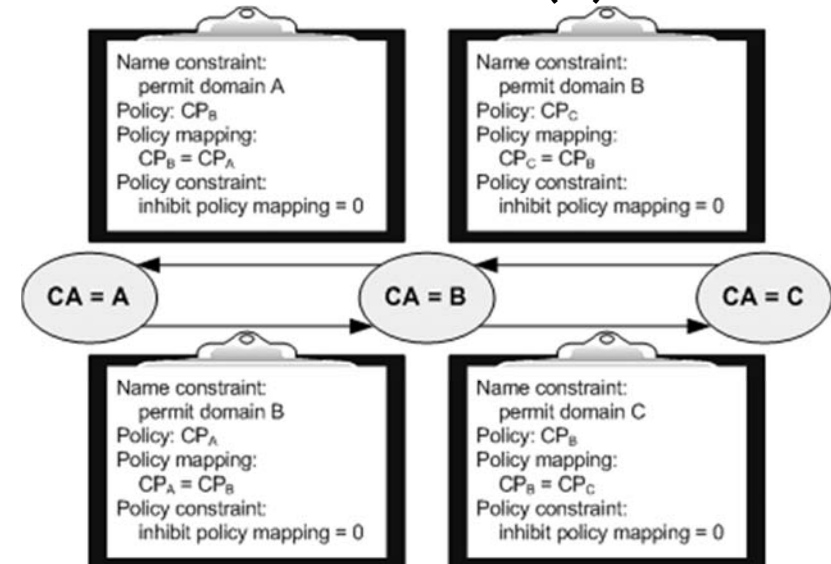
- Simplest case:
 - Two CAs grant the other a certificate
- Problems
 - Incompatible PKI products
 - Incompatible certification policies
 - ✓ Must review policies
 - ✓ Need equivalent, not identical policies
 - Use name constraints extension in X.509v3 certificates
 - ✓ Trust each others' domain names



27

Copyright © 2011 M. E. Kabay. All rights reserved.

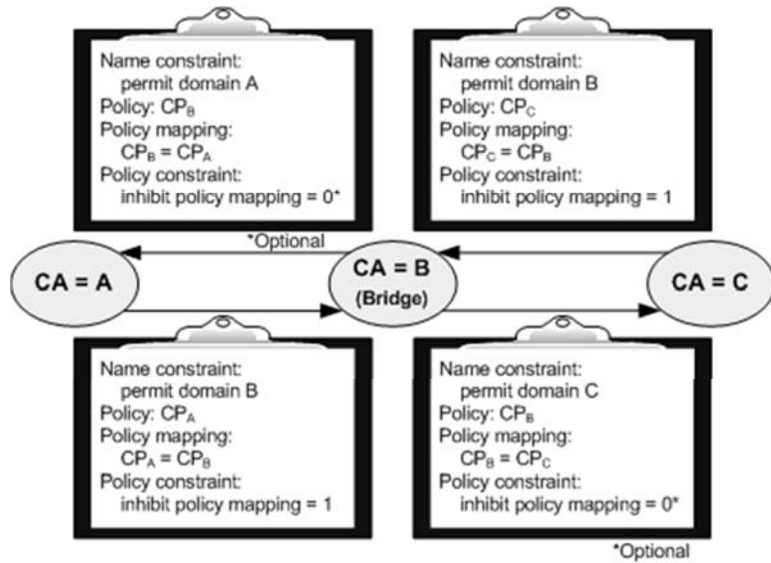
Cross-Certification (2)



28

Copyright © 2011 M. E. Kabay. All rights reserved.

Cross-Certification (3)



PKI Interoperability

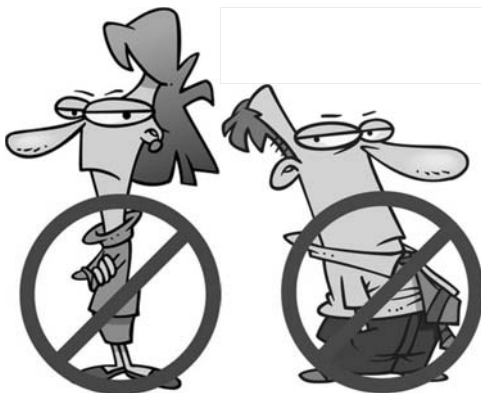
Factors

- Trust Path
- Cryptographic Algorithms
- Certificate & CRL Formats
- Certificate & CRL Dissemination
- Certificate Policies
- Names



Forms of Revocation

- Types of Revocation-Notification Mechanisms
- Certificate Revocation Lists & Variants
- Server-Based Revocation Protocols
- Summary of Recommendations



Types of Revocation-Notification Mechanisms

- Concerns about CRLs have led to variations for checking validity of certificates
- Online Certificate Status Protocol (OCSP)
 - ❑ RFC 2560
- Directory-based verification & revocation
- B-tree revocation lists



Certificate Revocation Lists & Variants

- Most versatile, effective & recommended
- Variations
 - ❑ Full & complete CRL (rare)
 - ✓ All certificates, revoked and valid
 - ✓ Most CRLs have only recent revocations
 - ❑ Authority revocation list (ARL) – usually short
 - ✓ Revocations only for CAs
 - ✓ Don't use X.509v1 ARL – only X.509v2, which distinguishes between CRL & ARL
 - ❑ Distribution-point CRL: allows partitions for shorter lists
 - ❑ Delta CRL: changes only since last CRL



33

Copyright © 2011 M. E. Kabay. All rights reserved.

Server-Based Revocation Protocols

- Servers provide revocation info; e.g.,
 - ❑ On-Line Certificate Status Protocol (OCSP)
 - ❑ Simple Certificate Validation Protocol (SCVP)
- Flaws
 - ❑ Need to secure channel to server
 - ❑ Computationally intensive digital signature generation makes system difficult to scale
 - ❑ Need trusted servers
- Useful when need to
 - ❑ Have thinnest possible PKI clients
 - ❑ Generate revenue for CA services
 - ❑ Check changing credentials
 - ❑ Update changing credentials



34

Copyright © 2011 M. E. Kabay. All rights reserved.

Summary of Recommendations for CRLs

- Use combination of
 - CRLs
 - Replication of CA directory entry for fast access
 - ARLs & their consolidation
 - Consolidation of reason-codes of key compromise in a domain
 - ❑ Use Distribution Point extension
 - ❑ Issue CRL frequently
 - Partition routine revocation info using Distribution Point CRLs if CRLs become too large
 - Store plaintext CRLs for fast searching
 - Eliminate private information to eliminate need for authentication when searching CRLs

35

Copyright © 2011 M. E. Kabay. All rights reserved.



"Sure, I'll be glad to give your management recommendations a chance."

Rekey

- Public key certificates eventually expire
 - ❑ Thus need new PK certificates
- Don't use PKs longer than estimated time for brute-force cryptanalysis
 - ❑ *Cryptanalysis threat period*
 - ❑ Shortens all the time as computational power increases
- Current estimates
 - ❑ 1024 bit RSA key → 25 years for now
 - ❑ Therefore worthwhile recertifying keys
 - ✓ Reduce number of keys necessary to access or validate older files/messages



Why?

37

Copyright © 2011 M. E. Kabay. All rights reserved.

Key Recovery (1)

- Distinguish between *signing keys* & *data encryption keys*
 - ❑ Signing keys must *never* be subject to key recovery!
 - ❑ Data encryption keys *may* be protected by key recovery
- *Key escrow*
 - ❑ Provide private decryption key to *key recovery agent (KRA)*
- *Key encapsulation*
 - ❑ *Encrypt* private decryption key using KRA's public key



38

Copyright © 2011 M. E. Kabay. All rights reserved.

Key Recovery (2)

- Avoiding giving KRA control
- May not want KRA to have unfettered access to decryption key
- So can
 - ❑ Superencrypt
 - ✓ Encrypt using 2 keys
 - ✓ Requires collaboration to get key
 - ❑ Split the key: *Shamir's n out of m rule*
 - ✓ Send parts of key to *m* recipients
 - ✓ Require at least *n* recipients to collaborate in restoring key



39

Copyright © 2011 M. E. Kabay. All rights reserved.

Privilege Management

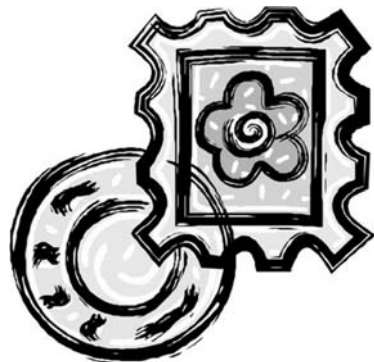
EXHIBIT 37.14 Privilege Management

| Alternative | Pros | Cons |
|----------------------------------|---|---|
| Application-based access control | Easy to implement. Does not require additional infrastructure, so saves cost. | Need to manage privileges on an application-by-application basis. Synchronization of privileges may be hard as applications increase and as they are distributed. Security may be compromised if privileges are not removed from all applications. Higher operational costs. |
| Public Key Certificate | Easy to add to PKI. Privileges can be managed easily by revoking certificate. | Changes in privileges require revocation of identity certificate. Sometimes this is a small price to pay for savings that result from not having to deploy and operate a separate privilege management infrastructure (PMI). Parties issuing identity certificate may not have authority to bestow privileges. |
| Attribute Certificate | Privileges can be managed easily by revoking attribute certificates. Change in privilege does not require revocation of public key certificate. | Cost of privilege management infrastructure (PMI). |

40

Trusted Archival Services & Trusted Time Stamps

- PKI does not prevent alteration or spoofing
 - ❑ Merely detects them
- Could also challenge digital signature after expiry of cryptanalysis threat period
- But can use trusted archival services
 - ❑ Need to provide storage of signed materials
 - ❑ Trustworthy assurance of error-free transcription from medium to medium over time as media degrade & technologies change
 - ❑ Can add functions of trusted time stamps



41

Copyright © 2011 M. E. Kabay. All rights reserved.

Cost of PKI

- Compare costs of PKI with costs of not having PKI!
 - ❑ Scalability is key factor:
 n vs n^2 keys
- Consider consequences of untrusted digital communications
 - ❑ Continued dependence on trust



M. E. Kabay's question to Norwich University authorities who resisted digital signatures on documents sent by e-mail:

How is depending on pigment smeared through a hole in the end of a stick onto compressed fibers from dead plants supposed to engender more trust in the authenticity and integrity of a document than cryptographically sound digital signatures?

42

Copyright © 2011 M. E. Kabay. All rights reserved.

DISCUSSION

43

Copyright © 2011 M. E. Kabay. All rights reserved.