

PKI

Part 2: Components and Architectures

Kjell Jørgen Hole
NoWires Research Group
Department of Informatics
University of Bergen

last changed September 27, 2010

Outline

- PKI components:
 - Registration Authority (RA)
 - Certification Authority (CA)
 - Repository
 - Archive
- PKI architectures:
 - simple architectures
 - enterprise architectures
 - hybrid architectures

RA

- Assume that each user shows up in person at RA
- The RA first verifies the information presented by a user requesting a certificate:
 - driver's license
 - passport
 - employee badge with picture
 - credit limit
 - signature authority

Key generation

- User initiates the generation of a key pair (e.g. inside a tamper resistant smart card)
 - the private key is kept secret
 - the public key is given to the RA
- In some cases the keys are generated by the RA and the private key is given to the user
- It must be possible for the CA to verify that a user owns a particular key pair

RA ...

- Finally, the RA initiates the certification process with a CA on behalf of the user
- observe that the RA does not issue any certificate, this is only done by the CA

RA's responsibility:
verify information needed by
a CA to issue a certificate

5

CA

- A CA maintains a list of RAs it trusts
- The CA performs two functions:
 1. issuing certificates
 2. maintaining **CRLs (Certificate Revocation Lists)**

6

1. Issuing certificates

- A CA issues certificates to users and, in some cases, other CAs
- *The CA guarantees that the entity named in a certificate has the private key corresponding to the public key in the certificate*
- The CA also asserts that any additional information, e.g. policy and contact information, in the certificate is valid

7

1. Issuing certificates ...

- When a CA issues a certificate to another CA, it (the first CA) asserts that the certificates issued by the other CA are trustworthy
- The issuing CA inserts its name in every certificate and CRL it generates, and signs them with its private key
- Users verify the signature of the certificates and CRLs using the issuing CA's public key

8

1. Issuing certificates ...

- The CA's digital signature is the basis of trust for all issued certificates
- If an attacker can obtain the CA's private key, then users will trust certificates generated by the attacker

CA's *primary* responsibility:
protect private key from disclosure

9

Cryptographic modules

- The CA's private key is often stored in a **cryptographic module**
- A **hardware** cryptographic module performs cryptographic operations on an external processor
- because these operations are not done in the CA's memory, the security is less dependent on the CA's OS

10

NIST requirements

- The National Institute of Standards and Technology (NIST) developed FIPS 140-2, **Security Requirements for Cryptographic Modules**
- FIPS 140-2 describes four increasing levels of security
- Accredited third-party laboratories perform validation testing of modules

11

Certificate profile

- A CA has a **certificate profile** defining the types of information to include in the certificates
- **Example:** If a CA specifies that it only issues e-mail certificates, it cannot issue a certificate for contract signing

12

Certificate profile ...

- The CA must
 - ensure that every certificate conforms to the profile
 - protect the profile by restricting access to CA components

CA's second responsibility:
ensure that all certificates and CRLs
conform to its profile

2. Maintaining CRL

- A CRL may contain the information:
 - list of revoked certificates
 - the date each certificate was revoked
 - the reason why each certificate was revoked

CA's third responsibility:
accurately maintain the list of certificates
that should no longer be trusted

Repository

- A **repository** accepts certificates and CRLs from one or more CAs
- It provides these certificates and CRLs upon request
 - requests based on name of user or CA
- A user accepts the certificates and CRLs because they are signed by a trusted CA

15

Repository ...

- Note that the distribution of certificates and CRLs is about availability and performance, not security

**Repository's responsibility:
distribute certificates and CRLs**

16

Archive

- An **archive** maintains information to identify the signer of an old document based on an **expired** certificate
- must keep information to identify the person named in the certificate
- prove that the person requested the certificate
- show that the certificate was valid at the time the document was signed

17

Archive ...

**Archive's responsibility:
maintain sufficient information to
establish the validity of certificates
after they have expired**

18

Outsourcing?

- The CA must be operated in a secure manner
 - an organization not used to operating a secure facility should consider outsourcing
- An organization's RA should probably not be outsourced because an organization knows its members best
- The repository and archive can most easily be outsourced

19

PKI architectures

- We now consider different PKI architectures and discuss their trust relationships
- We first consider two simple PKI architectures:
 - single CA
 - CA trust list

20

Single CA

- A single CA provides all certificates and CRLs for a community of users
- Users trust all certificates and CRLs from CA
- All certificates are user certificates, except the root certificate
- **Problems:**
 1. the architecture does not scale well
 2. CA represents a **single point of failure**

CA trust list

- Users maintain lists of trusted CAs
 - there are no trust relationships between CAs, i.e., no CA certificates are used
- Users can modify lists
 - they accept only certificates and CRLs from CAs in their trust list

CA trust lists ...

- **Problems:**
 1. a user tends to add new CAs to list without investigating the CAs
 2. it is difficult for a user to discover a CA compromise since there is no direct relationship between the user and a CA

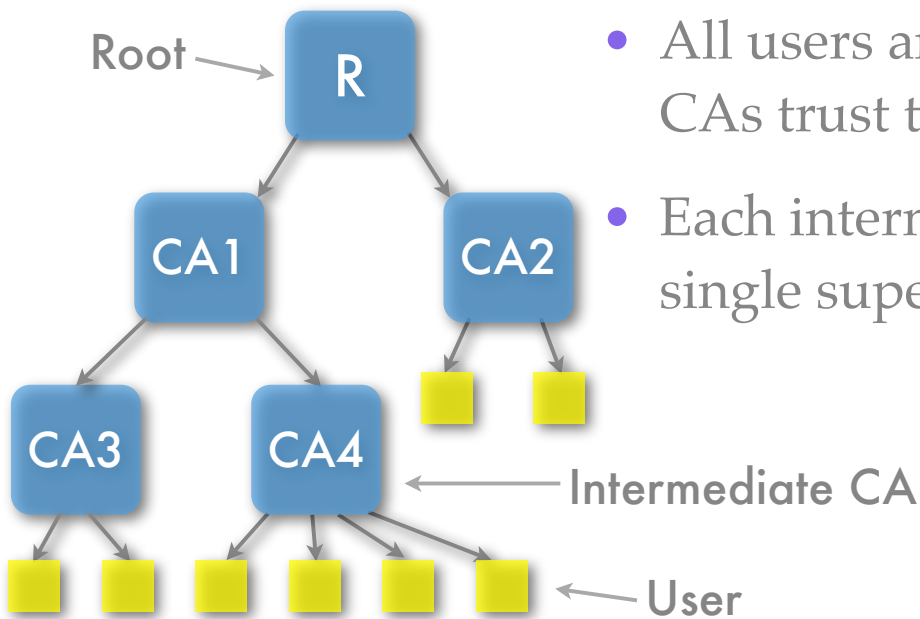
23

Enterprise architectures

- Next, we consider two enterprise PKI architectures:
 - hierarchical PKI
 - mesh PKI
- In these architectures, the CAs establish trust relationships with other CAs from the same enterprise

24

Hierarchical PKI



- All users and intermediate CAs trust the **root CA**
- Each intermediate CA has single superior CA

25

Establishing hierarchy

1. A root CA and a (self-issued) root certificate are established
2. The root CA certifies zero or more intermediate CAs
3. Each of those CAs certifies zero or more intermediate CAs immediately below it
4. At the second-to-last level the CAs certify users

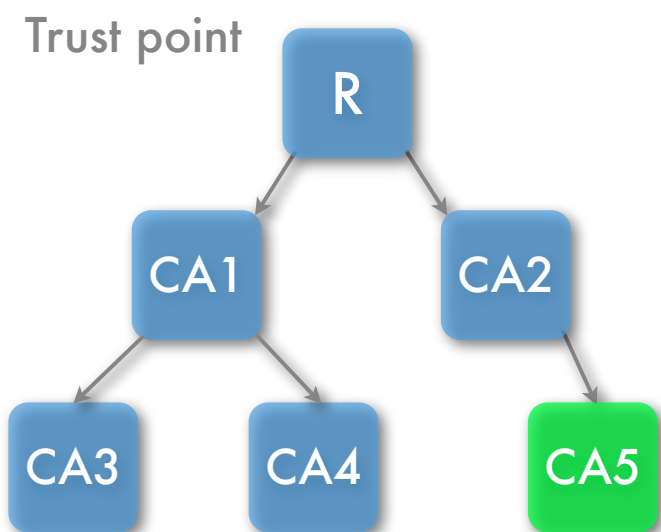
26

Establishing hierarchy ...

- Each entity in the hierarchy must be supplied with a copy of the root CA's public key
 - this must be accomplished in a secure, out-of-band fashion
- Note that while users are certified by the CA immediately above them, their trust point is a different CA (the root)

27

Adding new CA



- CA2 issues certificate to CA5
- Simple deterministic trust paths
- Single trust point at the root

28

Compromise of single CA

- Assume that a single CA (not the root CA) is compromised:
 1. the superior CA revokes the compromised CA's certificate
 2. once the compromised CA has been reestablished it issues new certificates to all its users
 3. the superior CA then issues a new certificate to the reestablished CA

29

Compromise of root CA

- When a non-root CA is compromised only a part of the PKI is compromised
- The complete hierarchical PKI is compromised when the root CA is compromised
- the root CA should operate offline, significantly reducing the risk of key compromise

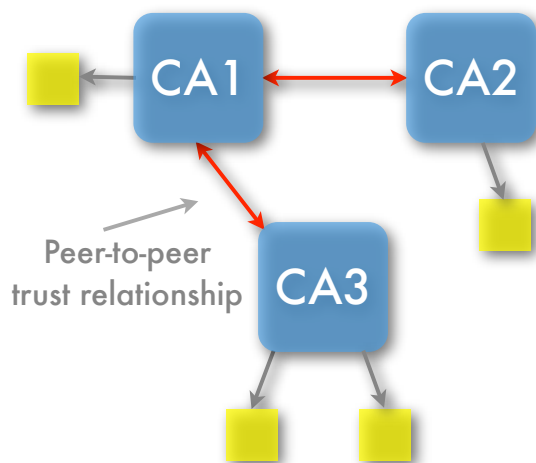
30

Mesh PKI

- The mesh PKI architecture is also referred to as the **network PKI** or a **web of trust**
- Multiple CAs are related through **peer-to-peer** relationships
- Each user trusts a single CA, but this CA is not the same for all users

31

Mesh PKI ...



- Users trust the CA that issued their certificates
- CAs issue certificates to each other
- bidirectional trust relationships are defined by pairs of certificates

32

New CA

- A new CA can easily be added to a mesh PKI
- the new CA exchanges certificates with at least one CA that is already a member of the mesh

33

Compromise of CA

- Mesh PKIs are resilient because there are **multiple** trust points
- Compromise of single CA cannot bring down complete PKI
- CAs that issued certificates to compromised CA revoke these certificates
- users associated with other CAs will still have a valid trust point

34

Certification paths

- **Problem:**
 - construction of a certification path is difficult because there may be multiple choices
 - some path choices lead to
 - a valid path
 - useless dead-ends
 - endless loops

35

Hybrid PKI architectures

- PKI-based applications may cross boundaries between communities or enterprises
- Hybrid architectures can be used to connect community and enterprise PKIs
 - extended trust list
 - cross-certified enterprise PKIs
 - bridge CA architecture

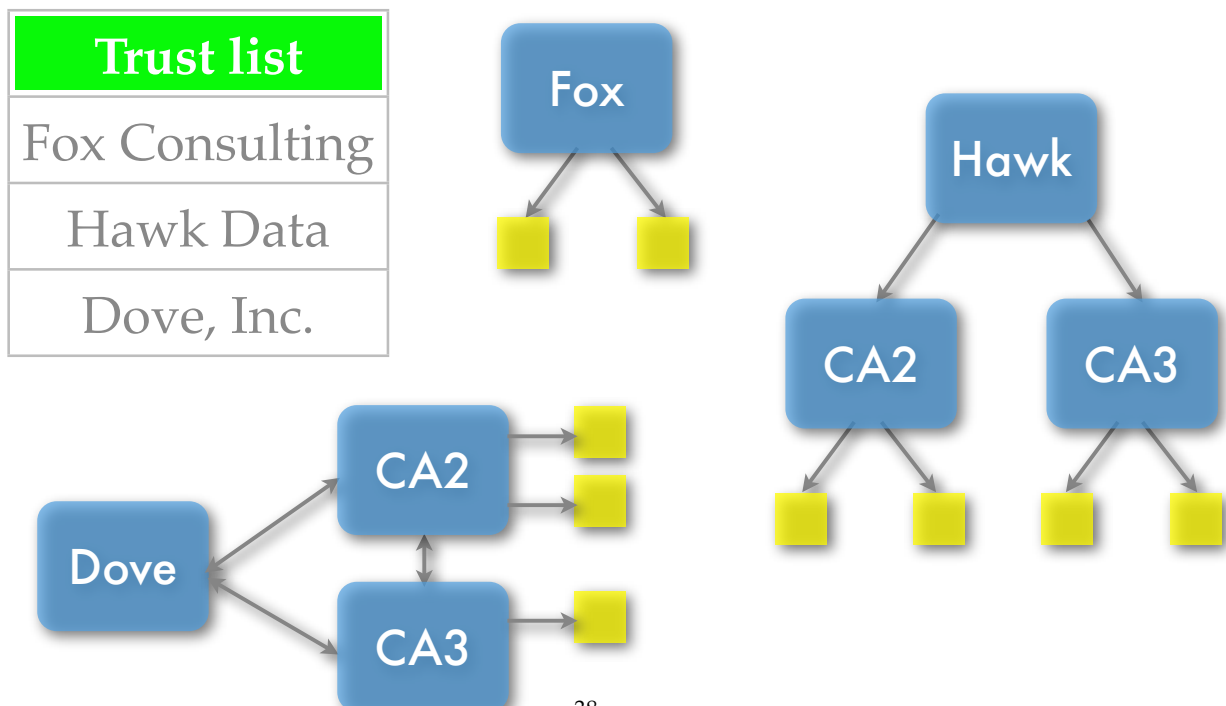
36

Extended trust list

- Each user maintains a list of trusted CAs
 - each trust point in the list is a single CA, a hierarchy, or a mesh
 - a user trust any certification path that starts with a trust point in the list
- **Problems:** the architecture does not solve problems of list management, CA verification, and CA compromise notification

37

Example



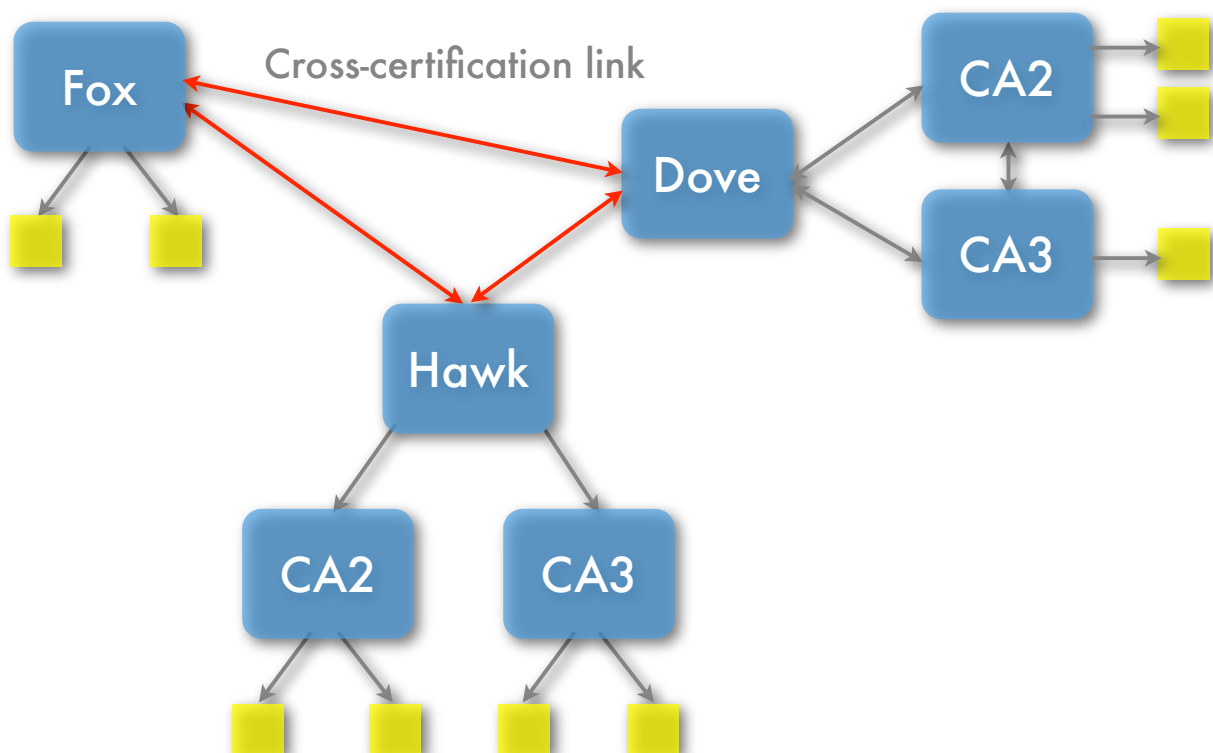
38

Cross-certified enterprise PKIs

- A cross-certified enterprise PKI establishes peer-to-peer trust relationship
- Each user maintains a single trust point, the CA that issued the certificate
- **Problem:** building of certification paths may be complex

39

Example

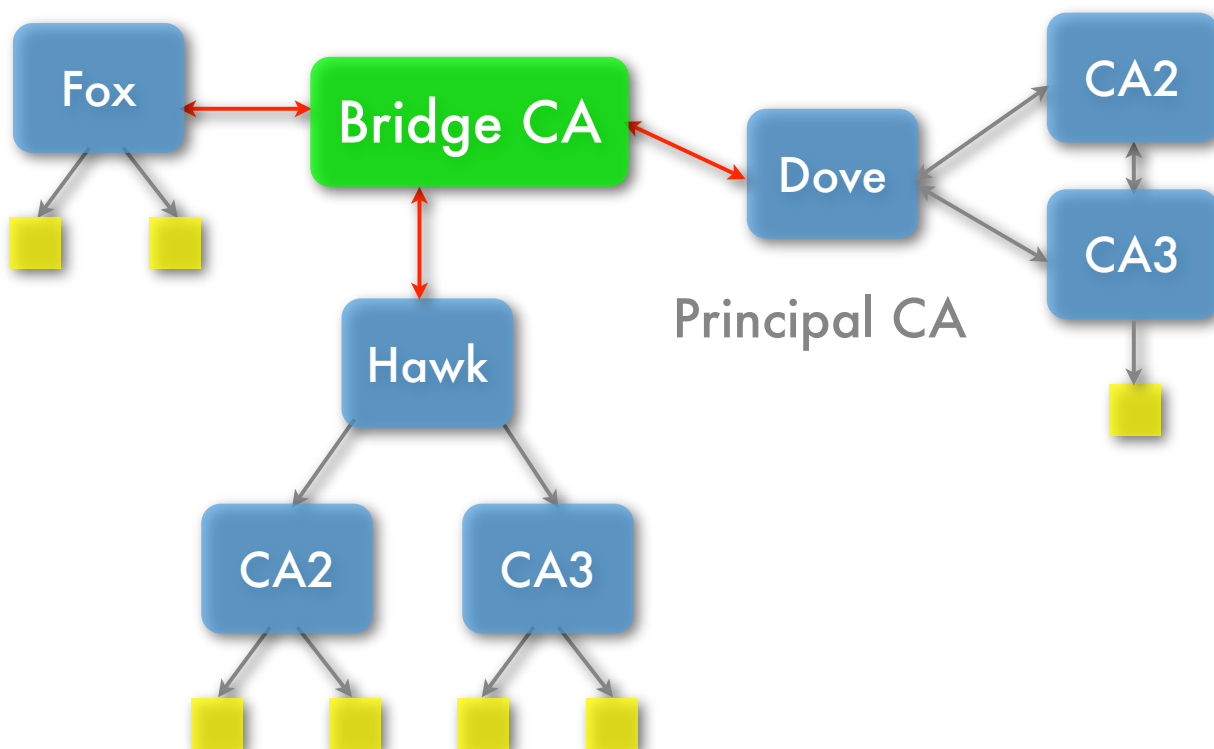


Bridge CA

- A special CA, called the **bridge CA**, is an intermediary that establishes peer-to-peer relationships with enterprise PKIs
- A CA that enters into a trust relationship with the bridge CA is termed a **principal CA**
- **Problem:** Certification path construction is complex

41

Example



Summary

- A PKI consists of one or more RAs and CAs, a repository, and an archive
- There exist a several different PKI architectures

43

Sources

- C. Adams and S. Lloyd, [Understanding PKI](#), 2nd Edition, Addison Wesley, 2003
- W. Ford and M. S. Baum, [Secure Electronic Commerce](#), 2nd Edition, Prentice Hall, 2001
- R. Housley and T. Polk, [Planning for PKI](#), Wiley, 2001

44

