

Issues In PKI

- *PKI for Future Wireless Networks*
 - *Weaknesses in PKI*

A. Public Key Infrastructure for Future Wireless Networks

*Ed Dawson and Selwyn Russell
Information Security Research Centre
Queensland University of Technology*

Outline

- *Introduction and PKI Overview*
- *Lessons from X.509 & Internet*
- *Wireless is different from Internet*
- *Security Architecture*
- *Design of Efficient Certificates*
- *Summary*

Need for PKI

- *Secure transactions between two unrelated strangers*
- *Key exchange problem*
- *Public Key Cryptography gives solution*
- *Digital Signatures*
- *What is your public key?*

Digital Certificates

- ***Means of conveying public key***
- ***Requires:***
 - key management
 - certificate management
 - user management
 - directory management
- ***Needs (wireless) infrastructure so strangers can use simply***

PKI Overview

- ***Create certificates***
- ***Store certificates***
- ***Assist users***
- ***Facilitate inter-operation***
- ***Enables PK services C, I, A & NR***

PKI Components

- *Registration Authority (RA)*
- *Certification Authority (CA)*
- *Certificates*
- *On-line databases or files*
- *Certificate Revocation List (CRL)*
- *Users*

PKI Components (2)

- *Key generators*
- *Key storage (e.g. tokens)*
- *Policies*
- *Auditors*
- *Other trusted components*

Lessons from X.509

- *Open Systems Interconnection model 1980s*
- *X.500 Directory “strong authentication” for login*
- *Certificate specified in X.509*
- *OSI not widely adopted*
- *X.509 of limited value without X.500*
- *No PKI*

Lessons from the Internet

- *Internet public access and growth has led to commercial transactions on Internet and interest in security*
- *X.509 provided basis but was limited in content*
- *1996 version 3 to allow infinite extensions*

X.509 Limitations

- *DER encoding gives platform independence*
- *Not needed on wireless*
- *Identities as OSI network addresses*
- *Lacks telephone address*

Problems with Version 3

- *So flexible that probably incompatible*
- *IETF sought to limit content*
- *Developed special profile for Internet use*
- *Currently being revised*

IETF Certificates

- *Basically 2 philosophies*
- *PKIX, all in one certificate*
- *Extensions for users of Internet*
- *SPKI, many simple certificates*
- *Longer = slower*
- *No PKI*

Internet vs Wireless Requirements

- *Both provide wide area data services*
- *Easy to assume wireless PKI is extension of Internet PKI*
- *Important differences between them*

Internet - Wireless Differences

- *Heterogeneous platforms vs relatively standard*
- *Telephone networks more reliable than Internet*
- *Telephone users accustomed to no delays*
- *Internet service quality unpredictable*
- *Internet users accept long delays*

Internet - Wireless Differences (2)

- *Low storage*
- *Low power processor*
- *Small battery life*
- *Low speed wireless link*
- *Pocket telephone should have short delays*

Factors in Delays

- *Algorithms & computation*
- *Chaining of certificates*
- *Decoding of certificates*
- *Need short transmissions*
- *Need minimum processing*

Internet ISP

- *Different suppliers*
- *Desktop from non-carrier*
- *Modem by different supplier*
- *Carrier line to ISP*

Internet ISP (2)

- *User has connection to Internet via ISP*
- *Carrier and ISP often not related*
- *Choice of ISP if not carrier*
- *Certificate provided by another party*

Wireless ISP

- ***Subscriber obtains handset and account from NO (or agent)***
- ***NO issues SIM/UIM***
- ***All internet access via NO***
- ***Close relationship with NO for all services***
- ***No other parties needed***

Security Architecture

- ***NO as Registration Authority***
- ***NO as Certification Authority***
- ***NO issues certificate in SIM / UIM***
- ***no chaining for subscribers of the NO***

Certificate Design

- *Minimize content size*
- *Optimize encoding*
- *Minimize chaining*

General Requirements

- ***Simplest content for application***
- ***No encoding***
- ***Small size***
- ***Easy to process***

ASPeCT Certificate

- ***Used by subs and CAs***
- ***Similarities to X.509:***
 - single multi-purpose design
 - standard fields + optional fields
 - allows for chains
 - has cross certification attributes

ASPeCT Differences

- *Adds map field to tell contents*
- *Fixed length fields*
- *No encoding*
- *Two options for identifier*
 - either binary or plain
 - no other options
- *Public or private key*

A More Specialised Design

- ***Individuals most common users of e-commerce in wireless***
- ***Use special high efficiency certificate***
- ***Can eliminate inapplicable fields***
- ***No need for features which apply to CAs only***

Efficiency Features

- ***Fixed length fields***
- ***No encoding***
- ***Version number for easy upgrades***
- ***Identities tailored for mobiles:***
 - mobile network address, or
 - UIM/SIM related

Revocation Assistance

- ***Checking is a performance problem***
- ***Add revocation source(s) for fast revocation checking***
 - number of CRL distribution identifiers
 - list of CRL distribution identifiers
- ***Mobile contacts source(s) directly***

Summary

- ***Wireless is different to Internet***
- ***NO as Registration Authority***
- ***NO as Certification Authority***
- ***Certificates in SIM / UIM***
- ***Simpler certificate for smaller latency***
- ***Special case of individuals***

B. Weaknesses in Public Key Infrastructure

¹M. Henderson and ¹E. Dawson,
²M. Burmester and ³E. Okamoto

¹ Queensland University of Technology

² Royal Holloway College, Uni of London

³ Toho University

Sponsored by Telecommunications Advanced
Organization of Japan (TAO)

Outline

- * Public Key Infrastructure (PKI)
- * PKI Topologies
- * PKI Stress Points
- * Towards Secure PKIs

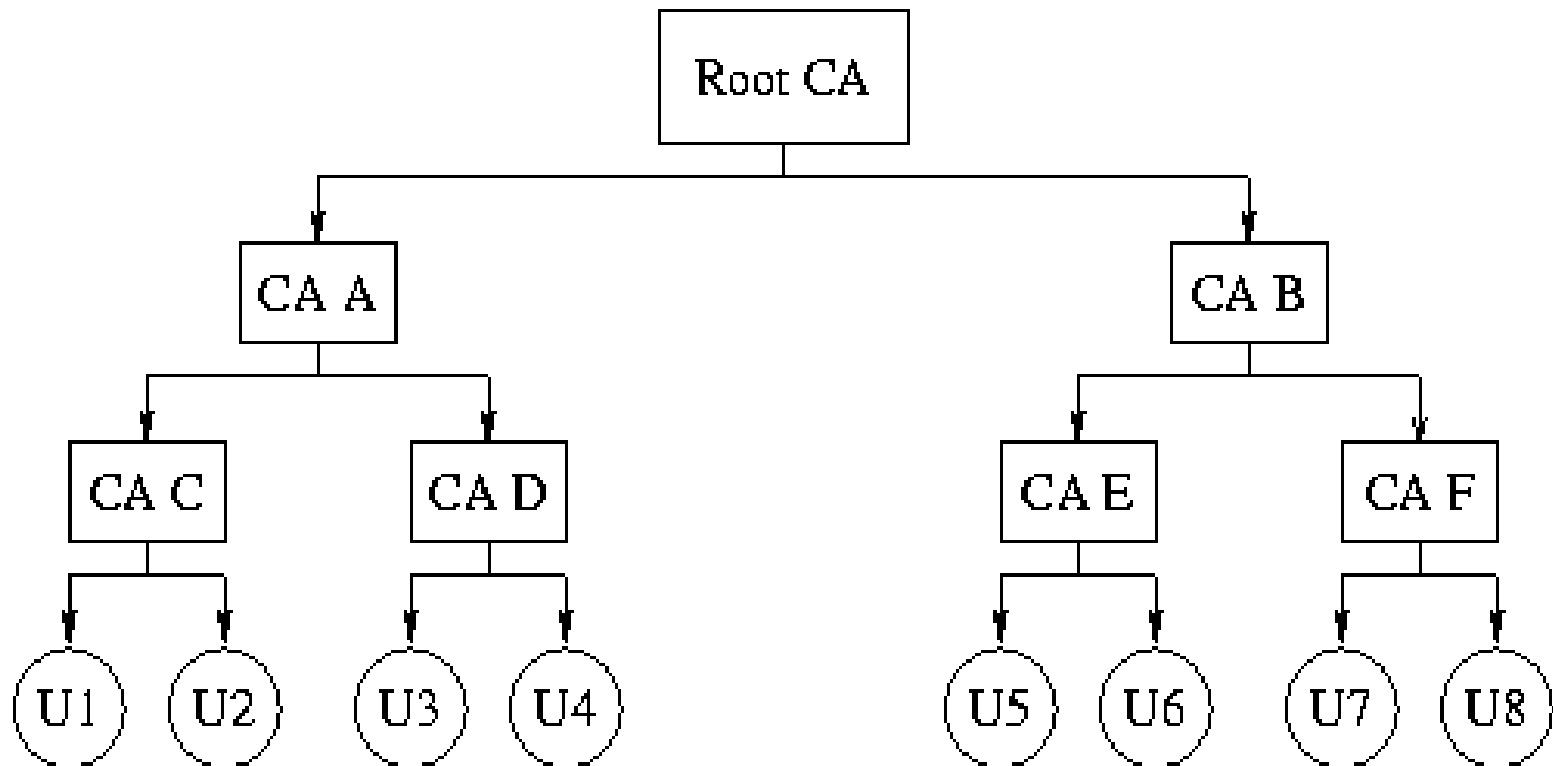
Public Key Infrastructure

- * Certificates
- * Certificate Authorities (CAs)
- * End Entities (EEs)
- * Trust-path
- * Trust Graph

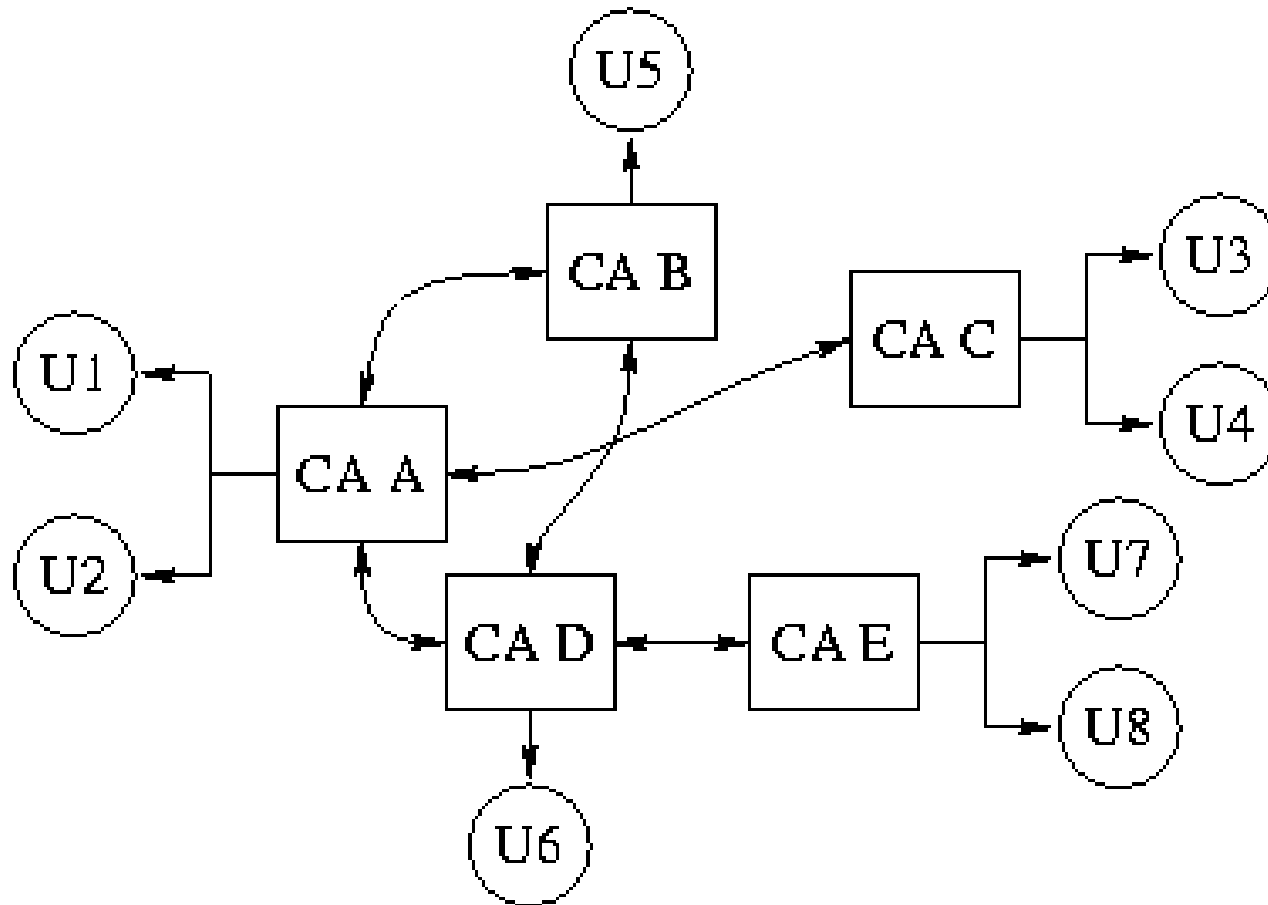
PKI Topologies

PKIs can be structured in different ways. PKI structuring determines the trust relationships (how trust is transferred from one entity to another).

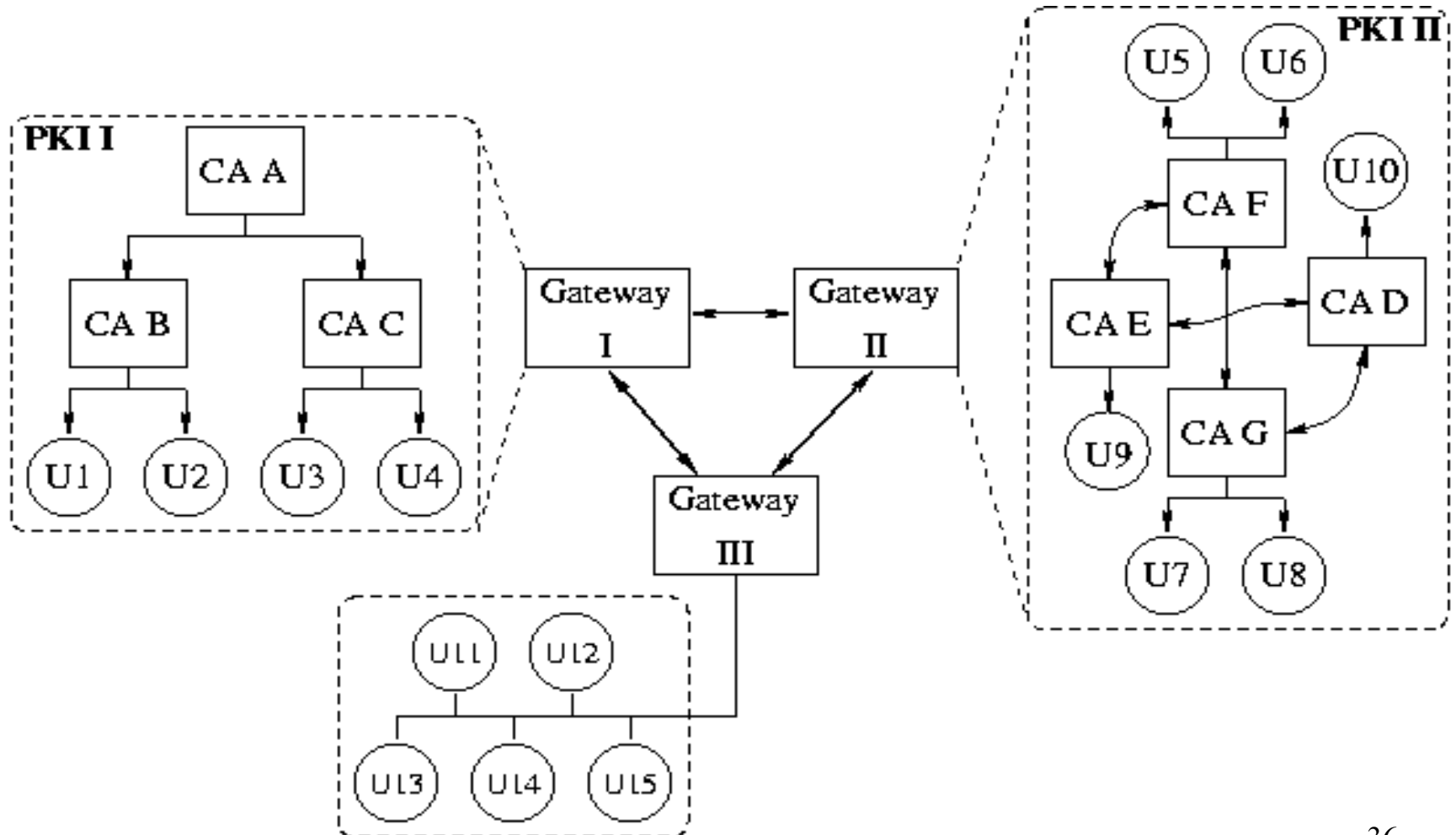
Hierarchical Structures



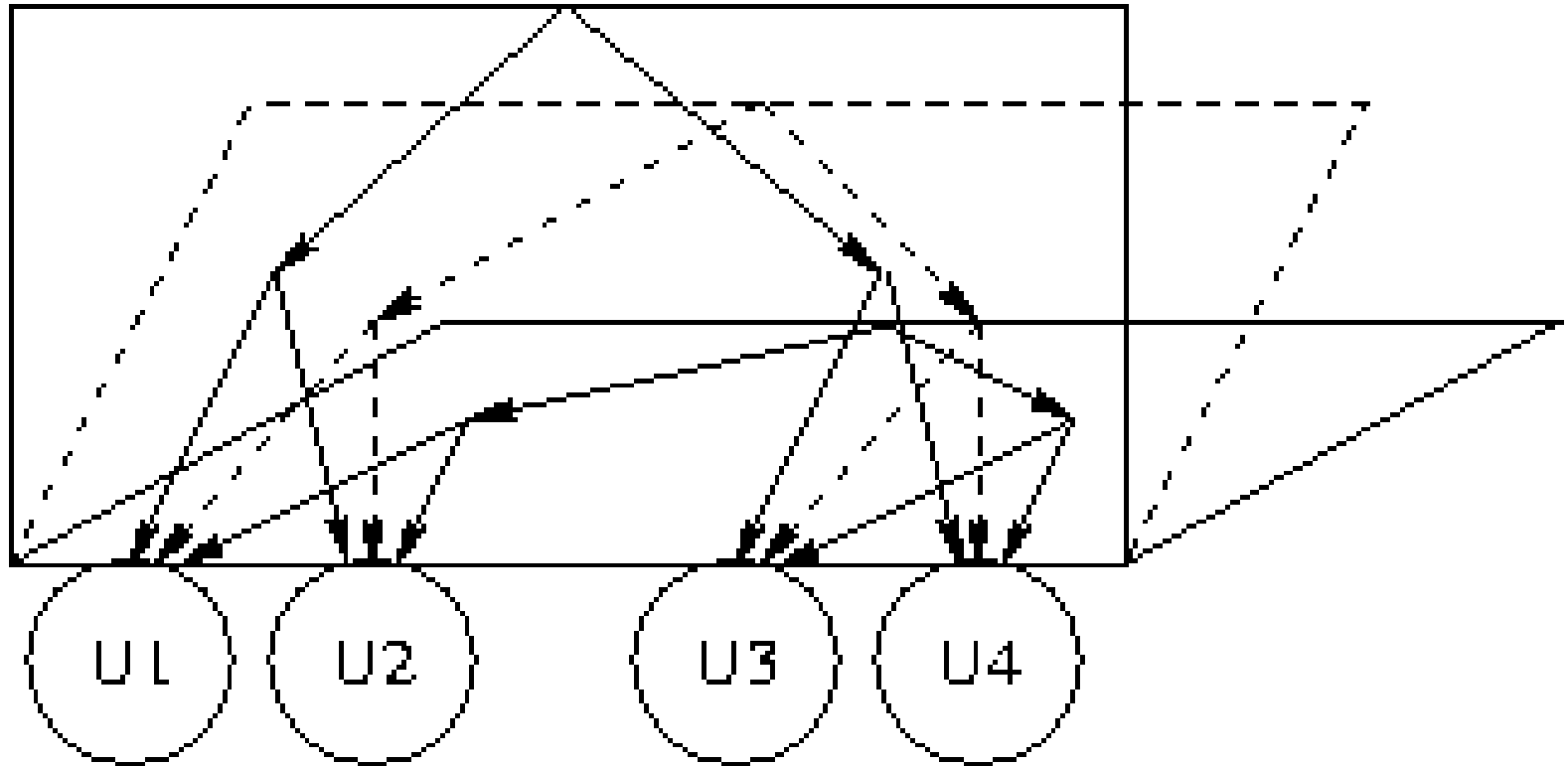
Mesh Structures



Gateway Structures



Multiple Platform Structures



PKI Stress Points

We analyse the PKI stress points at each of the following PKI components:

- * Certificate Authorities
- * Certificates
- * Certificate Users (EEs and verifiers)

Certificate Authorities

Separation of Certification and

Registration: use of Unmanaged CAs

(black box CAs) with RAs exposes the CA
to attacks on the RA.

Unmanaged CAs: with an unmanaged CA recovery from compromise is degraded while exposure to compromise is increased.

Lost or Compromised Keys: replacement of defunct CA keys can trigger a domino effect when the CAs private key is lost or compromised (all certificates issued with the certificate will need to be revoked and so on). This impacts PKI operation.

Compromised Signing Device: access to the signing device allows creation of certificates so it must be controlled.

Three components are involved in certificate creation:

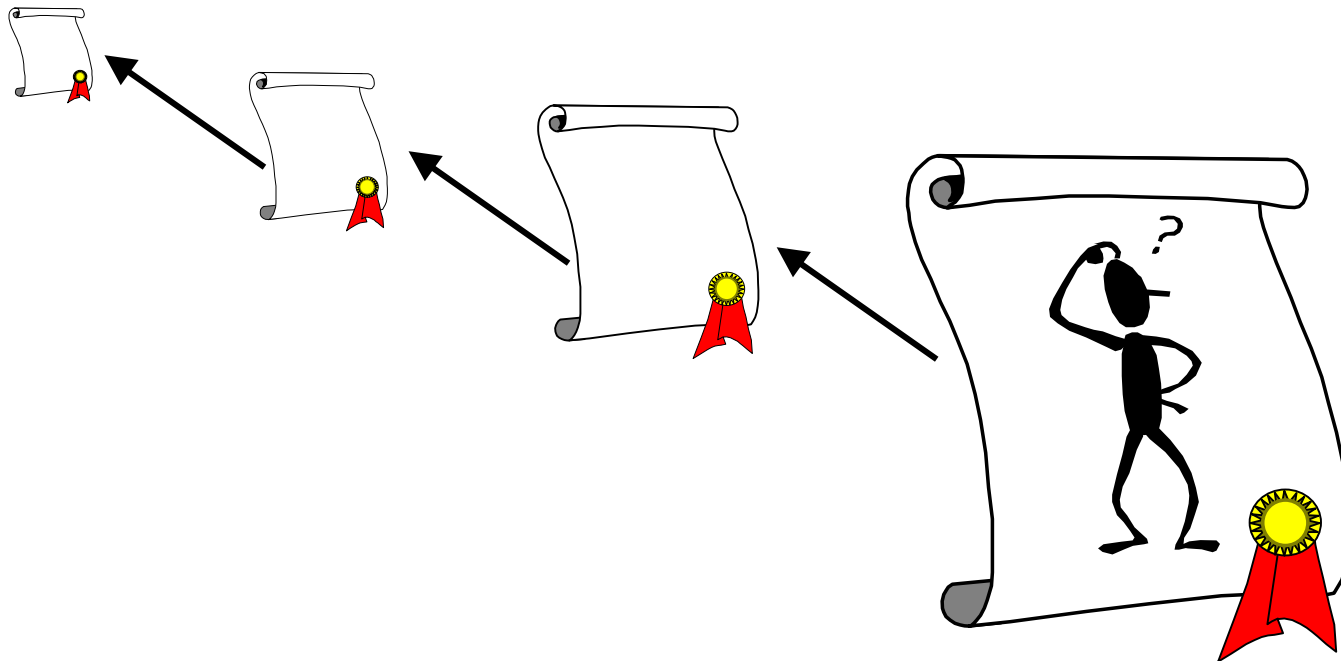
1. the private key of the CA
2. the algorithm
3. the data to be signed.

Certificates

Certificates are protected by the signature of the CA so that any changes to the certificate can be detected.

Problems can arise when certificates are processed.

Path Processing Implementation: a path of certificates may need to be checked to verify the required certificate



Most algorithms are based on X.509

- * X.509 version 3 certificate path processing is complicated.
- * Standards have been changing (sometimes to fix identified errors).
- * Implementations can contain errors.
- * Processing can result in security violations.

Certificate Users

Authentication/Encryption keys: the protection properties for private keys are

1. Use of the private key is limited to the certificate owner
2. The private key is never exposed not even to the certificate owner

CA Key Pair Generation: a malicious CA
can keep a copy of the user's private key
degrading non-repudiation

Weak Keys: a user can provide weak keys
and later repudiate transactions

Verifier Processing: even if the processing procedure is correctly implemented it may still not execute correctly due to mis-configuration or virus infection.

Towards Secure PKIs

We outline remedies that can be used to support PKI security.

Remedy 1: Avoid Unmanaged CAs

The security of an unmanaged CA can not exceed their RAs processing security nullifying any advantages. Best practice suggests such configurations should be avoided.

Remedy 2: Minimise Exposure through a Defunct CA Key

A number of methods may be used:

1. Limit the number of certificates issued under one signature key pair
2. Keep a backup copy of the CA's private key
3. Distribute the CA signing service between multiple CAs
4. Distribute the CA service via independent trust paths

Remedy 3: Minimise Exposure to a Malicious CA

Using part three of Remedy 2 limits the exposure to cheating CAs. The fourth method will also limit exposure to attacks from CAs.

Remedy 4: Secure the CA Signing Procedure

Tamper resistant devices can be used to protect the CA's private key and the signing process but does not counter attacks which replace the data to be signed.

Distribution of CA services and re-checking of signatures can help.

Remedy 5: Protect Verifier Against Path Processing Errors

Preliminary efforts aim to improve path processing through the application of formal methods. Path processing should be contained to limit exposure to security violations (buffer overflows etc.).

Remedy 6: Protect the Generation of Key Pairs

The generator of the key pair should take some responsibility for its cryptographic security. Good cryptographic keys require a good source of random bits. Tamper resistant devices can generate keys (but not truly random).

Remedy 7: Protect Private Keys and the Verification/Certification Procedures

Tamper resistant devices may be used to protect keys and to implement verification procedures. These devices must themselves be protected from mis-use by a PIN and/or biometric identification.

Remedy 8: Use Appropriate Architectures

With a hierarchy penetrating any CA will undermine the security of all entities that rely on that CA. Multi-platform can withstand a limited number of penetrations. Gateways can also provide protection from penetration.

Remedy 9: Using Assurance Levels

Assurance levels for certificates can be incorporated into certificates allowing assurance to be combined and assigned to trust paths. Additional paths may be requested if the assurance is not acceptable.

Conclusions

A PKI should be...

- * Robust: survive entity failure, even through malicious attacks
- * Survivable: survive destruction of parts of the PKI through faulty CAs