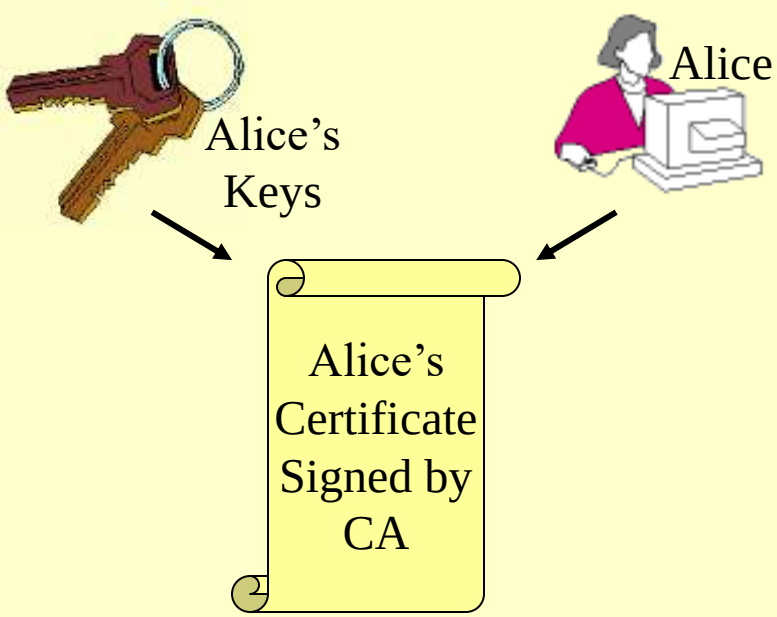
The Certificate Authority

- In a Public Key Infrastructure, the CA component is responsible for issuing certificates.
- A certificate ***binds*** key pair and its owner...

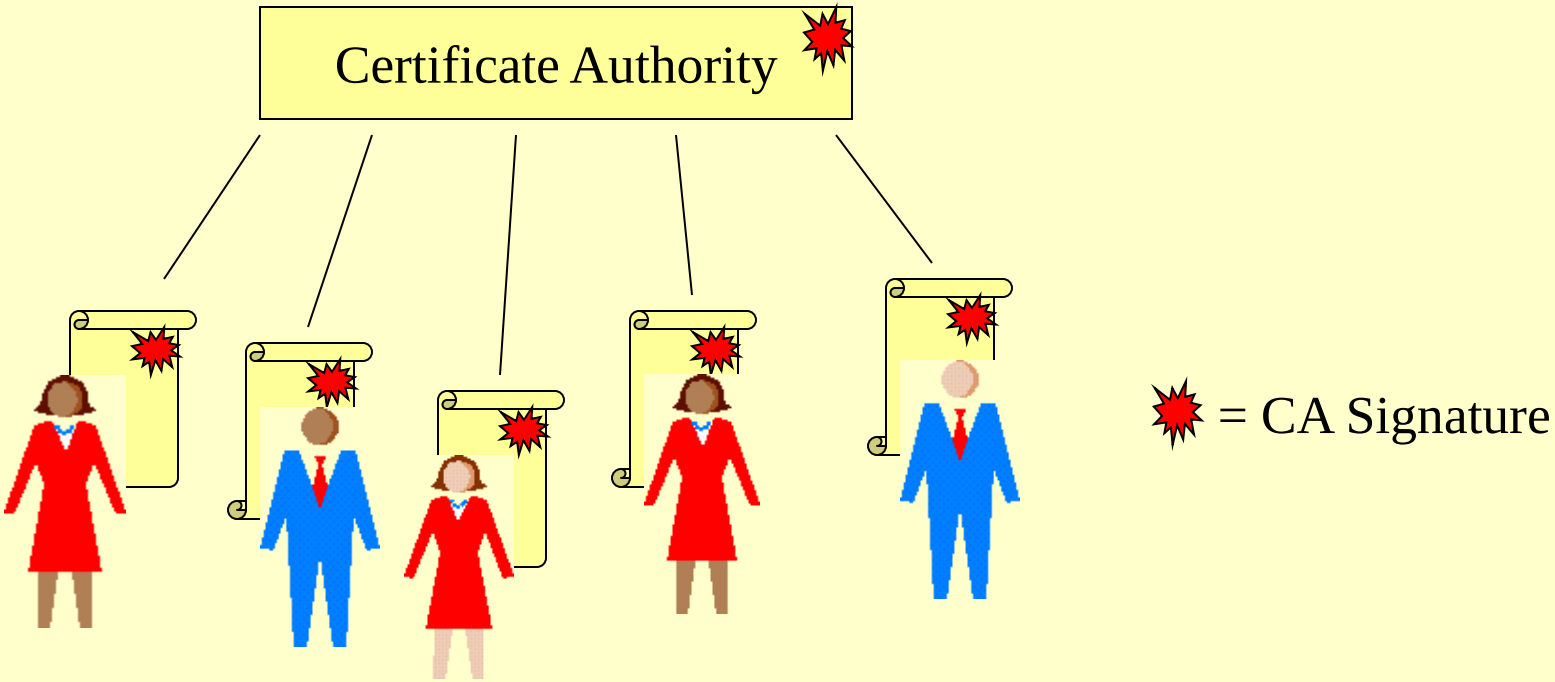


CA Trust Hierarchy

- The CA is the root of all trust in a PKI.
- There can exist multiple sub-CAs, all signed by the Root Certificate Authority.
- All certificates are traceable back to the Root CA.
- All certificates issued within a particular CA hierarchy, or topology, conform and must adhere to the same policies.

Certificates and Trust

- Once users trust the Root Certificate Authority, they can trust all certificates signed by the CA or sub-CAs.



Certificates - A Closer Look

- We must check to ensure:
  - We have the right certificate
  - The key is still valid
  - The key is still trusted

Certificates - A Closer Look

- For interoperability, the certificates conform to standards.
- The X.509 Certificate contains data attributes set by the ITU-T.
- The Net Tools PKI Server generates certificates that are X.509 compliant.

Security Policy

- The security of any public key crypto-system relies heavily on policies and procedures
- The *conduct* of PKI Administrators and users impacts the effectiveness and security of the system
- Comprehensive policies must support information security *and* business objectives

Security Policy

PKI Administrators will perform many critical tasks, including:

- Certificate Authority creation
- Defining Certificate Attributes
- Verifying Identity of Certificate Users
- Certificate Lifecycle Event processing

Security Policy

PKI users will perform many critical tasks, including:

- Keeping their passwords secure
- Keeping their private key(s) secure
- Knowing when/how to trust other's keys
- Treating information in accordance with the information security policy

Security Policy

- Policies should not inhibit business objectives or day-to-day responsibilities
- Policy-makers should seek global standards within organization
- All policies should explicitly define *procedures* for proper incorporation
- All policies and procedures must be readily available for those who ask

Net Tools PKI Server

PKI Server Components

- The Net Tools PKI Server application contains the following components:
  - Certificate Authority (CA)
    - Web-based Administration interface
    - Web-based Enrolment interface
    - A Secure Server Enrolment interface
  - LDAP Directory Certificate Server

Net Tools Certificate Authority

Certificate Authority

The Net Tools CA is used to...

- Implement a CA topology
- Define a directory schema
- Manage certificate lifecycle events

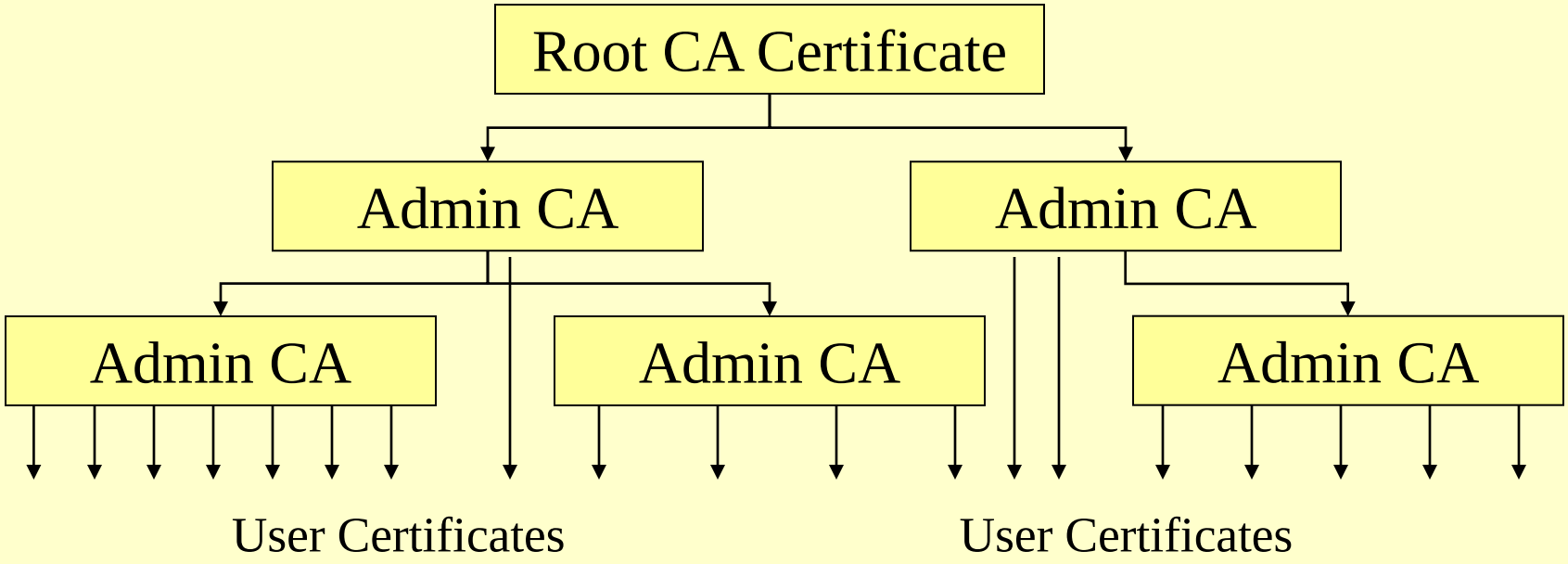
CA Topology

- The CA Topology is also known as a “CA hierarchy” or “PKI hierarchy”
- A Root CA exists at the “top” of the topology
- If needed by an organization, Admin CAs (a.k.a. “sub-CAs”) can be created to develop a hierarchy.

See the following diagrams

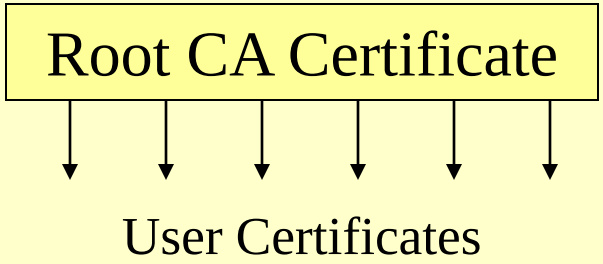
CA Topology

A multi-level CA Topology:



CA Topology

- A Flat CA Topology:



This could represent a smaller organization without a need to distribute the certificate management process.

CA Topology

- The Net Tools Certificate Authority initially generates a Root Key.
- The Root CA will then sign and issue:
  - Active Security Certificates
  - User Certificates
  - Admin CAs
  - Other application certificates (i.e. SSL certs)
  - Or, a combination of all four.

CA Topology

- Multiple Admin CAs can distribute the certificate management workload
- Multiple Admin CAs can distribute different security policies
- A single CA can be implemented in less complex environments, or where there are limited certificate needs.

Directory Schema

- Each X.509 certificate contains an X.500 or LDAPv3-compliant distinguished name (DN). The values will be defined with the Net Tools Certificate Authority.

C=	country
O=	organization
OU=	organizational unit
S=	state or province
L=	locality
CN=	common name

NOTE: LDAPv3 DN requirements may differ from the X.500 DN requirements

Directory Schema

- X.500 is an ITU-T standard
- X.500 refers to a directory structure standard, and requires a specific naming scheme.
- The Net Tools PKI Server can generate distinguished names that conform to the X.500 standard (the CA administrator must provide the attribute values).

Directory Schema

- Upon installation and configuration of the PKI Server, the schema is defined.
- Subsequent to installation and configuration, certificates issued should be named in accordance with this schema.

The Certificate Lifecycle

- Events in the lifecycle of a certificate include:

1. Certificate Request
2. Verification (End-user and Key identity)
3. Certificate Generation
4. Certificate Publication
5. Certificate Revocation

✓ = discussed thus far

Certificate Request

- End-user entites...
  - Human users
  - Active Security applications
  - Admin CAs (not strictly an “end-user”)
  - Other applications

  …can all request a certificate from the Net Tools PKI Server.

Certificate Request

- The Net Tools Certificate Authority provides the interfaces for end-user requests:

End Entity	Interface	Port
Human	Web Enrollment Server	444
Active Security and other applications	Server Authenticated Enrollment Server	445

NOTE: The default port settings are listed.
These values can be changed.

Active Security Certificate Requests

- The setup of each Active Security component presents an option to:
  - generate a key pair
  - request a certificate from the PKI Server
- The certificate request is completed on the Active Security host machine
- The certificate issuance is completed on the PKI Server admin page

The Certificate Lifecycle

- Events discussed thus far:

1. Certificate Request
2. Verification (End-user and Key identity)
3. Certificate Generation
4. Certificate Publication
5. Certificate Revocation

= discussed thus far

Verification

- A critical responsibility of the Certificate Authority administrator is verifying…
  - the identity of the requester
  - the association of the public key and private key.
- Because a Certificate binds the key owner to a key pair, the Verification process is the foundation of certificate validity.

Verification

- Even for Active Security components, the CA Administrator should confirm component host machine relationships:
  - The host name and IP address
  - The installed Active Security component
  - The key pair was generated by said machine

Verification

- The level of required verification will vary with the amount of trust required in the system, however great detail must be given to the following:
  - Minimum verification requirements
  - Separation of verification and issuance duties
  - Educating responsible parties
  - Documenting verification policies and procedures in writing

The Certificate Lifecycle

- Events discussed thus far:

1. Certificate Request
2. Verification (End-user and Key identity)
3. Certificate Generation
4. Certificate Publication
5. Certificate Revocation

= discussed thus far

Certificate Generation

- The Net Tools Certificate Authority provides a web-based PKI Administrator page (port 443)
- This is used, among other tasks, to…
  - check pending certificate requests
  - issue approved certificates
  - generate additional CA certificates

Certificate Generation

- Using the PKI Administrator page, data is entered to generate a certificate
  - Review information provided by requester
  - Distinguished name (following schema)
  - Other identifying attributes
  - V3 Extension values

Certificate Generation

- Upon generation, the PKI Server Administrator page is used to issue the certificate.
- Issuance includes:
  - **Notifying** the end-user on how to retrieve the certificate
  - **Publishing** the certificate to the LDAP directory

The Certificate Lifecycle

- Events discussed thus far:

1. Certificate Request
2. Verification (End-user and Key identity)
3. Certificate Generation
4. Certificate Publication
5. Certificate Revocation

= discussed thus far

Certificate Revocation

- On occasion, a certificate will need to be revoked
- Situations might include:
  - Loss of trust in certificate for any reason
  - Compromise of private key
  - Compromise of private key password
  - Removal of entity from PKI

Certificate Revocation

- Using the PKI Server Administrator page…
  - certificates can be revoked
  - Certificate Revocation Lists (CRL) are generated
- CRLs can be manually updated
- CRLs can be automatically updated according to a pre-set schedule

Certificate Revocation

- This certificate lifecycle event deserves attention to:
  - Educating Administrators and end-users on how to recognize the need for revocation
  - Escalation procedures for the revocation process
- The policies and procedures of revocation should be documented in writing.

The Certificate Lifecycle

- Events discussed thus far:

1 Certificate Request

2 Verification (End-user and Key identity)

3 Certificate Generation

4 Certificate Publication

5 Certificate Revocation

= discussed thus far