
EJBCA training!

Training overview

1. X509v3 review → LAB install raw test CA & issue self-signed certificates

2. PKI & EJBCA. The plan I →LAB Small PKI

3. PKI & EJBCA. The plan II →LAB Advanced PKI

4. The CWA 14167 Qc PKI

Public key cryptography

Certificate

FLOREAT·RVGBEIA

BOROUGH OF RUGBY

Second Class Certificate

Awarded to ANDREW PETCHER

Age 12 *years, for satisfying the examiner of his* ABILITY TO SWIM *a distance of 100 yards by means of the Breast-stroke, and 33⅓ yards by means of the Back-stroke.*

Mrs Dick *Examiner*

Chairman of the Baths Committee

Town Clerk

Certificate

Issuer

Subject

An assertion/affirmation

Issuer signature

Certificate

Issuer: Goverment of spain

Subject: Adrià Massanet

An assertion/affirmation: Adrià has a private key

Issuer signature: electronic signature

Certificate in smartcard

- Posession of the key
- Key is generated inside the cryptoprocessor
- Key cannot be extracted but can be used sending the data to the chip
- The certificate of posession is public and is stored inside the chip, also

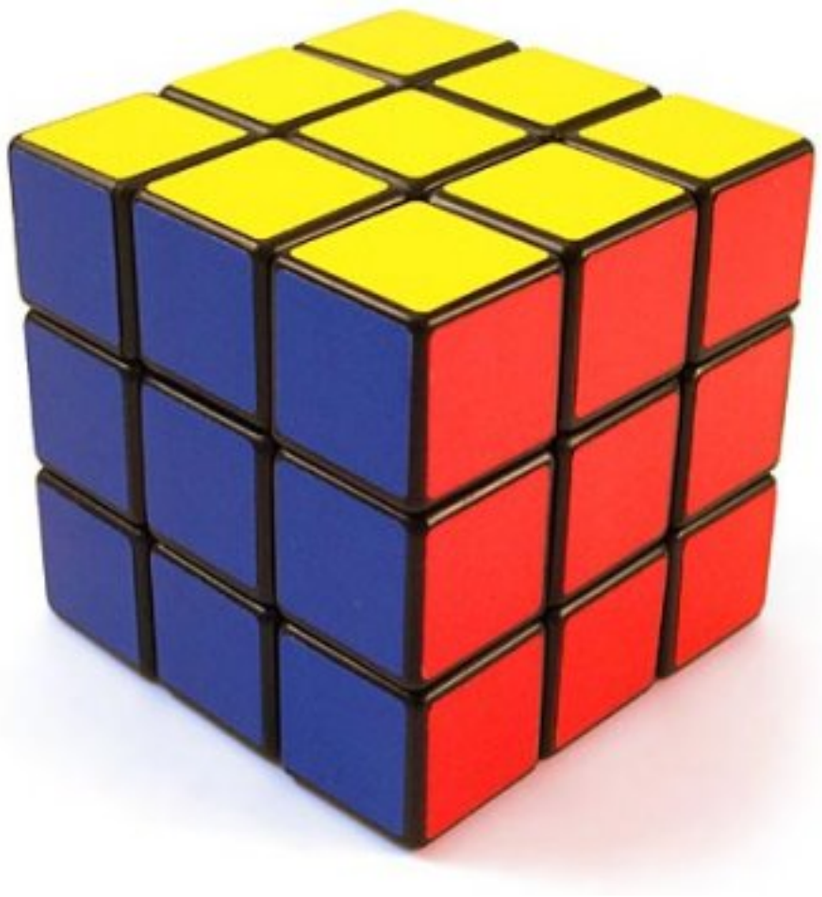
Public key cryptograhy is used

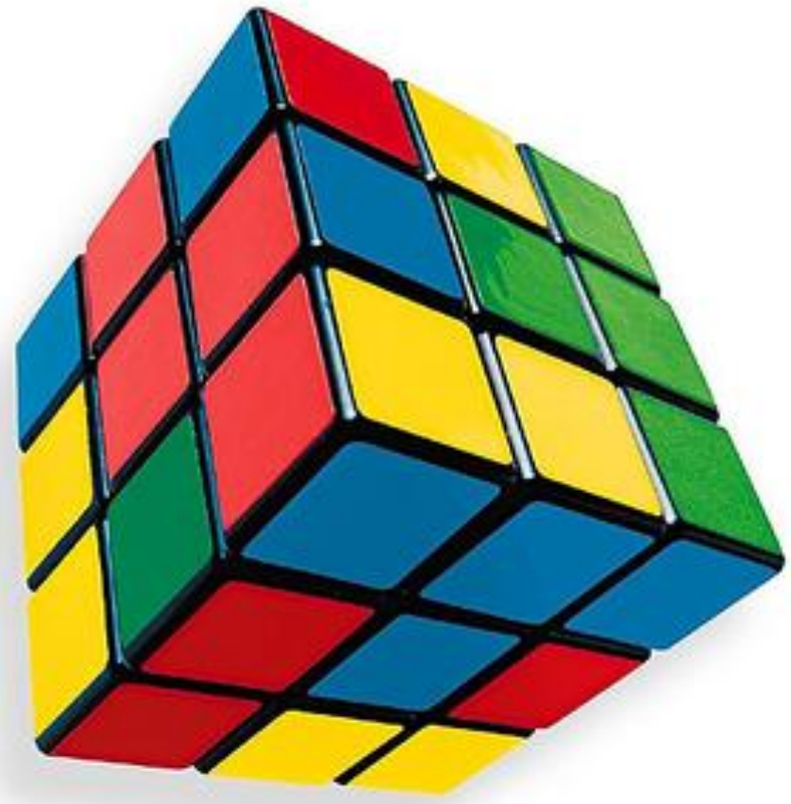
- Authentication
- Digital signature
- Encryption

Secure communications

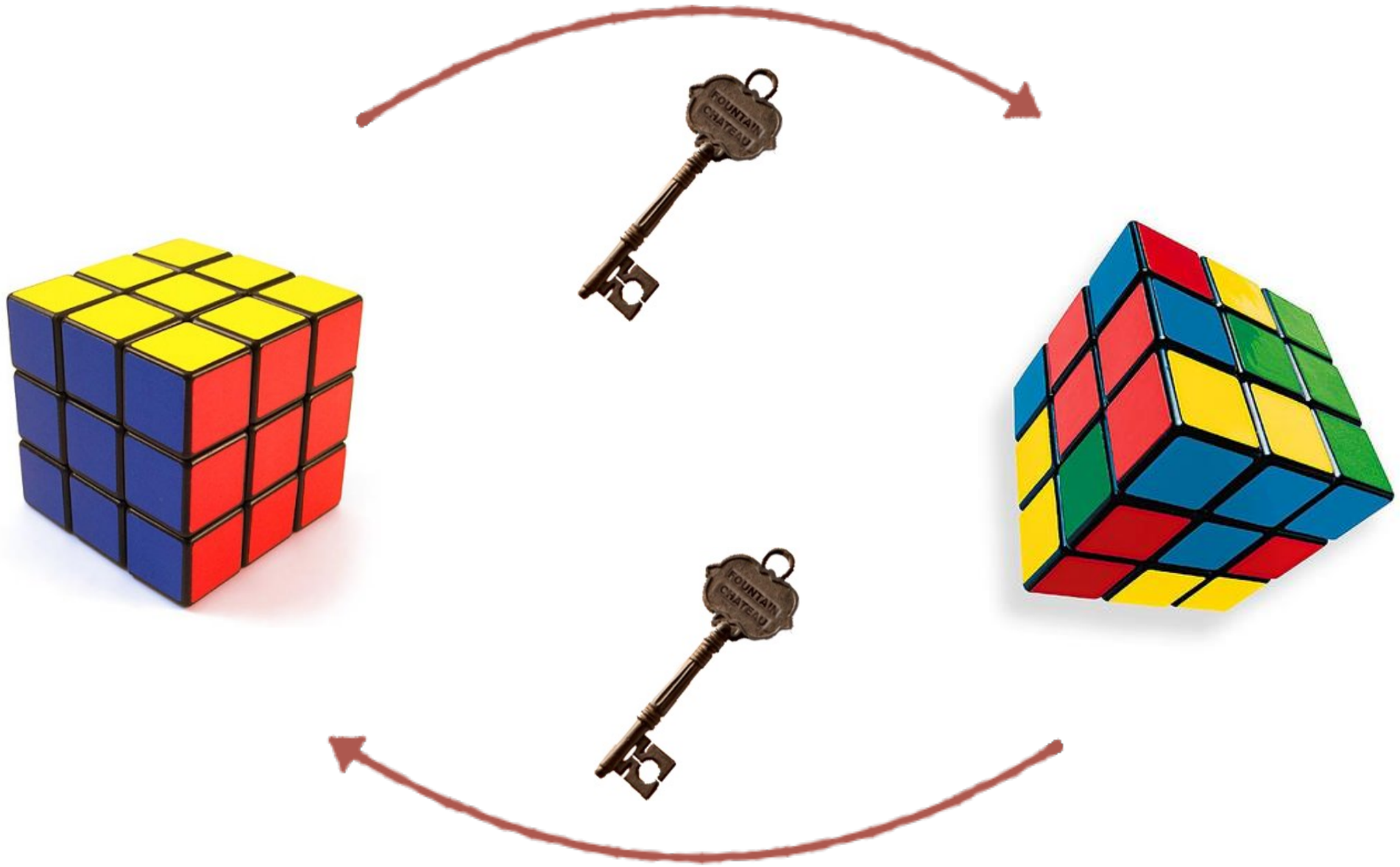
- Authentication
- Integrity
- Confidentiality
- Non repudiation

Cipher



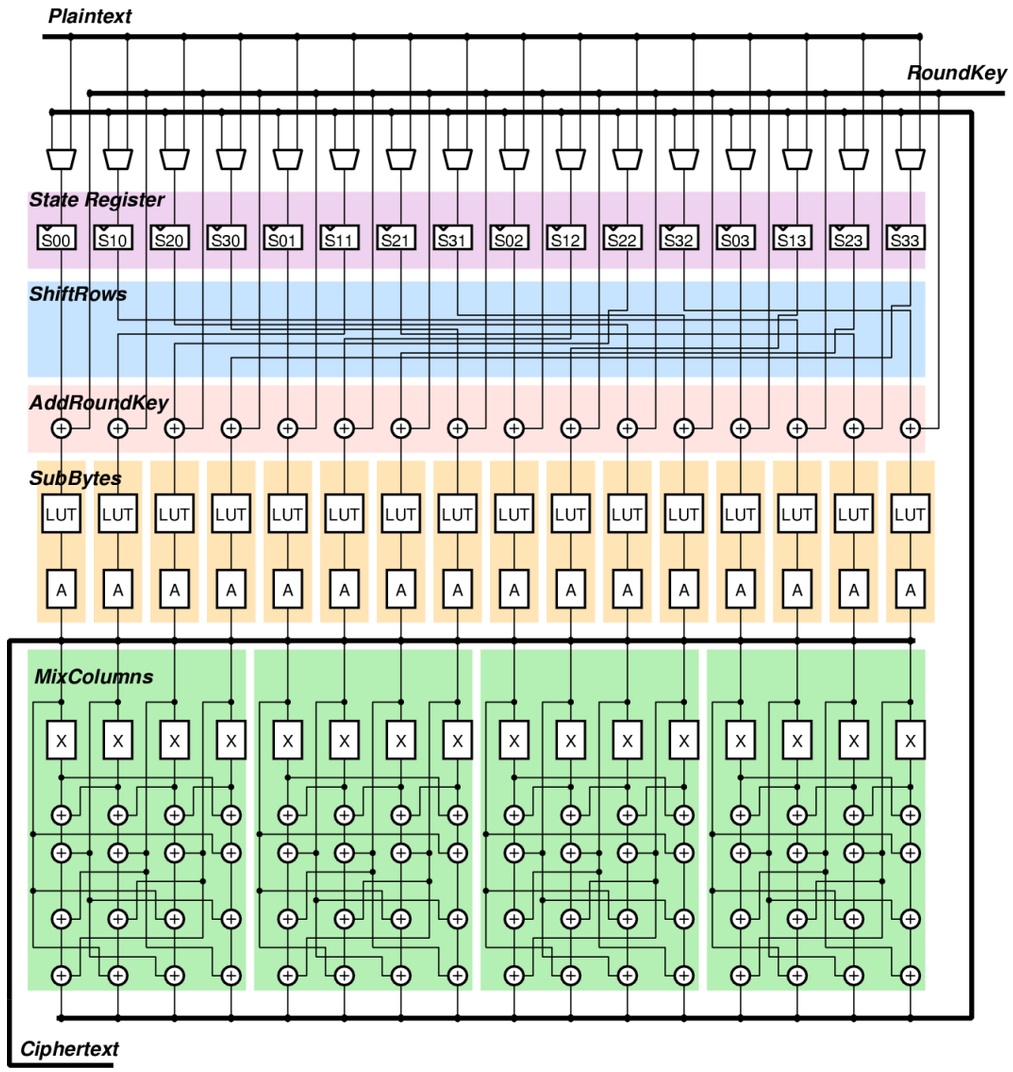


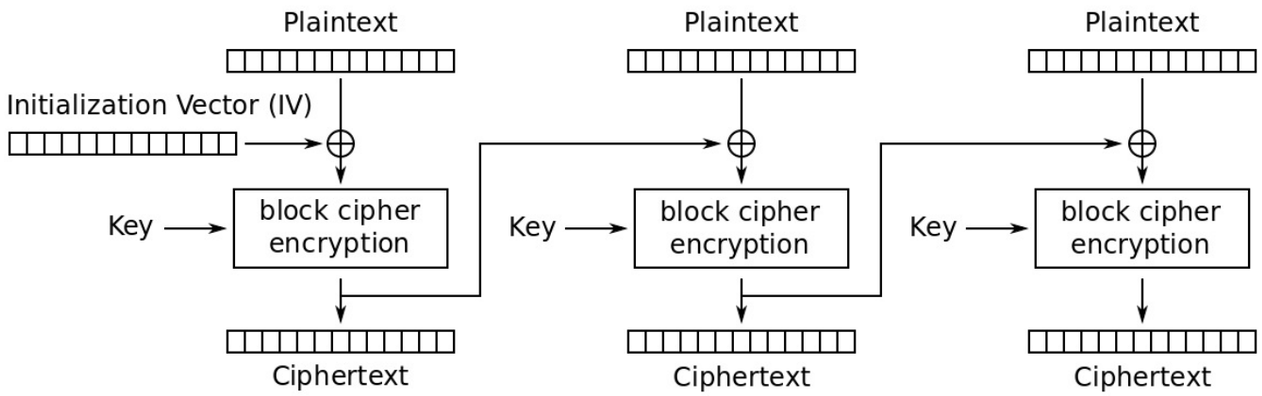
Symetric cipher



Symetric cipher

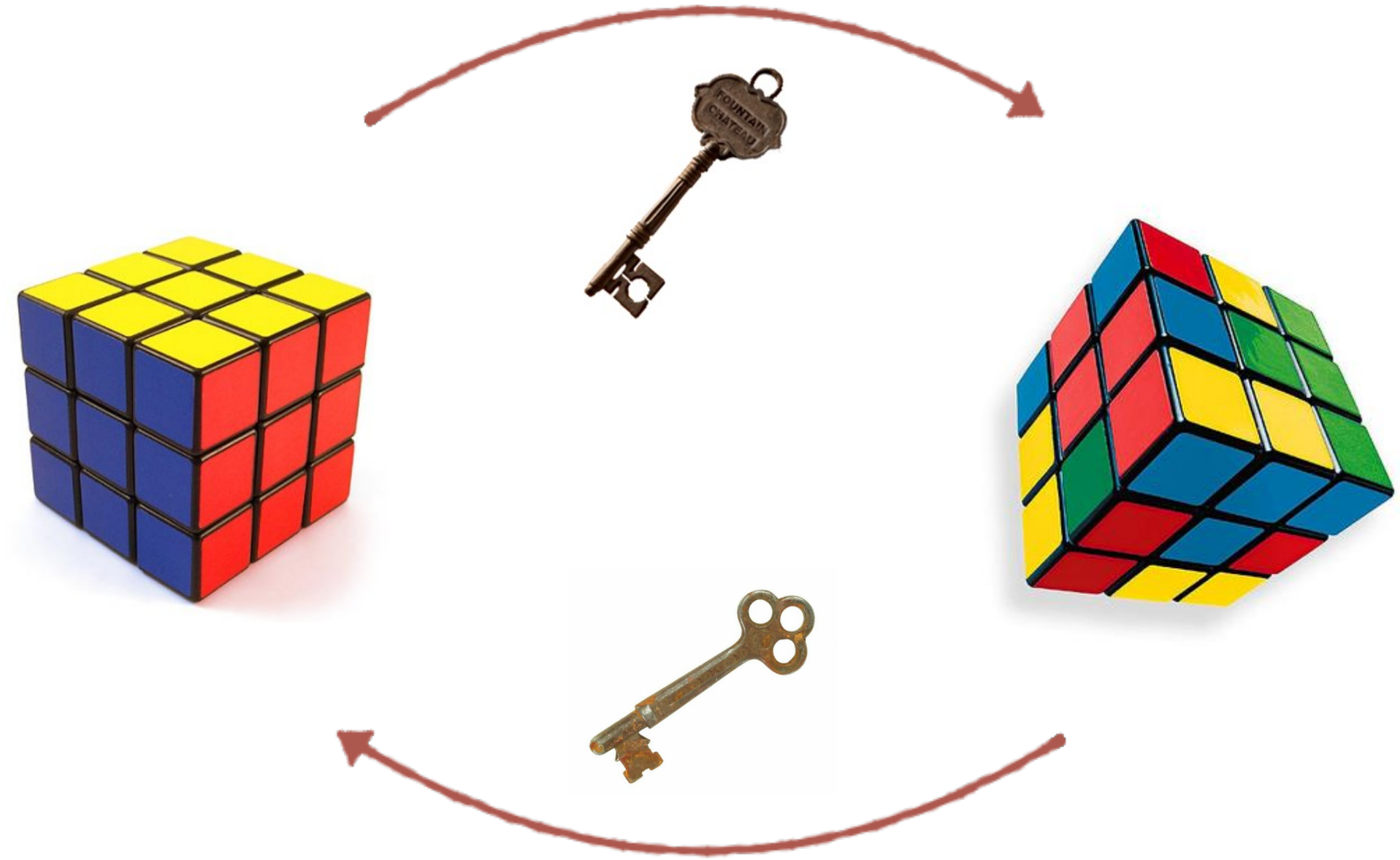
- AES-CBC
- 3DES-CBC



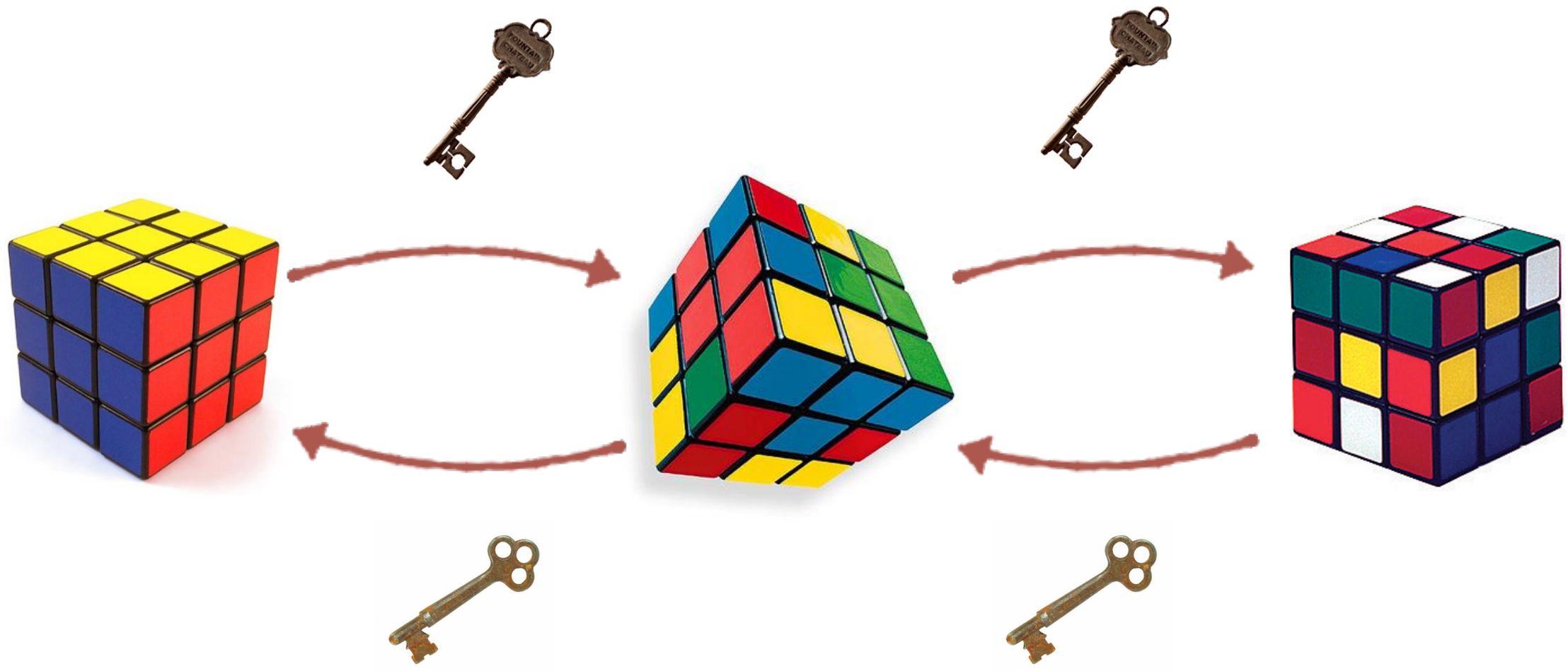


Cipher Block Chaining (CBC) mode encryption

Asymmetric Cipher



Asymmetric Cipher



Asymmetric Cipher

Asymmetric Cipher

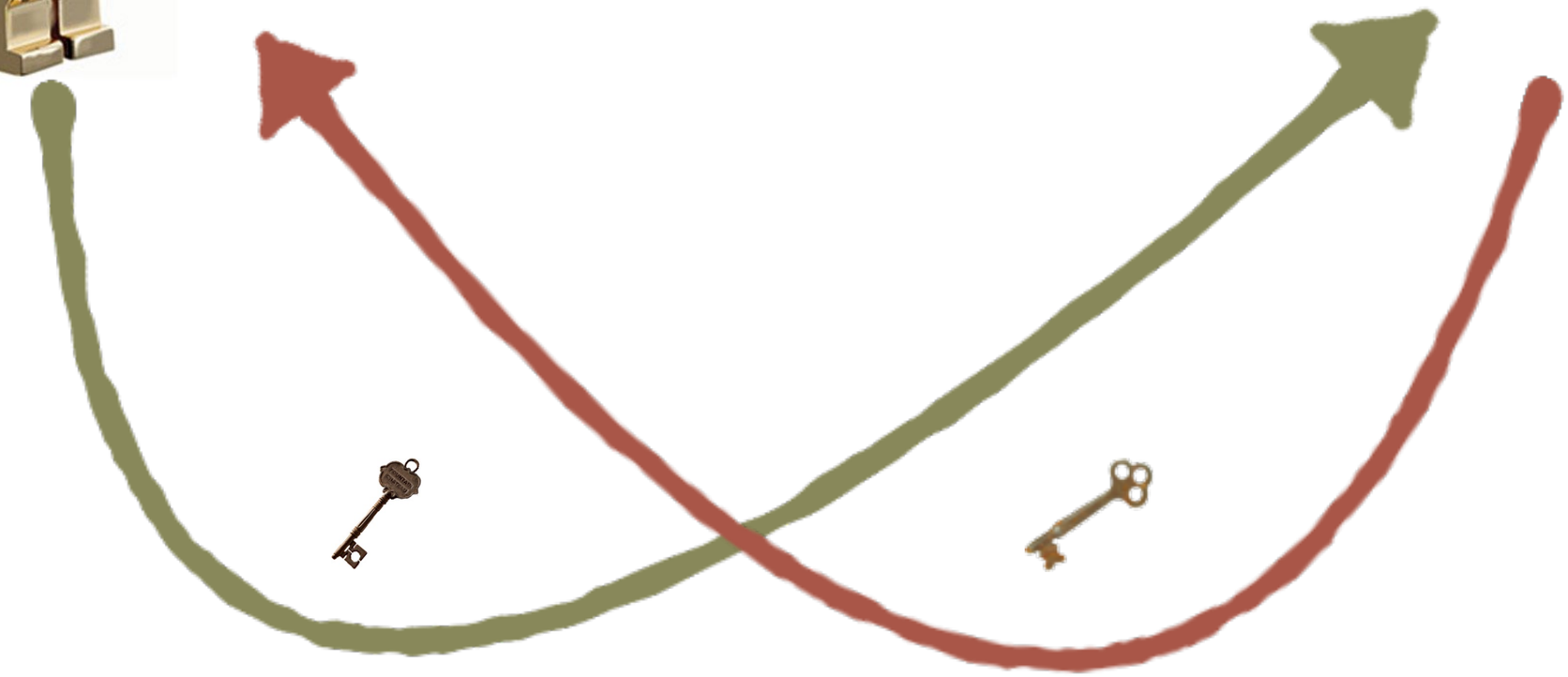
Asymmetric Cipher

Public Key Cryptography

Asymmetric signature

Asymmetric signature

Asymmetric signature & cipher



Algorithms

- RSA
- DSA
- #Message < #key

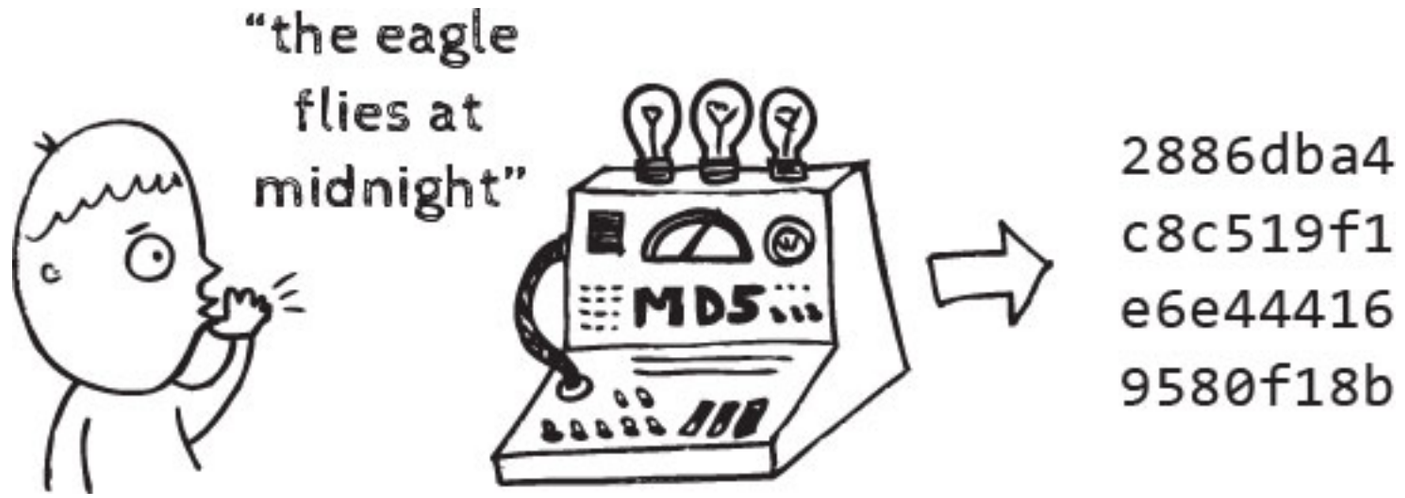
SSL Performance		
	Commodity Hardware	
Key Length	**32-bit**	**64-bit**
1024	525 TPS	1570 TPS
2048	96 TPS	273 TPS
4096	15 TPS	38 TPS

Hash functions

43444861T

43444861|61

Hash functions



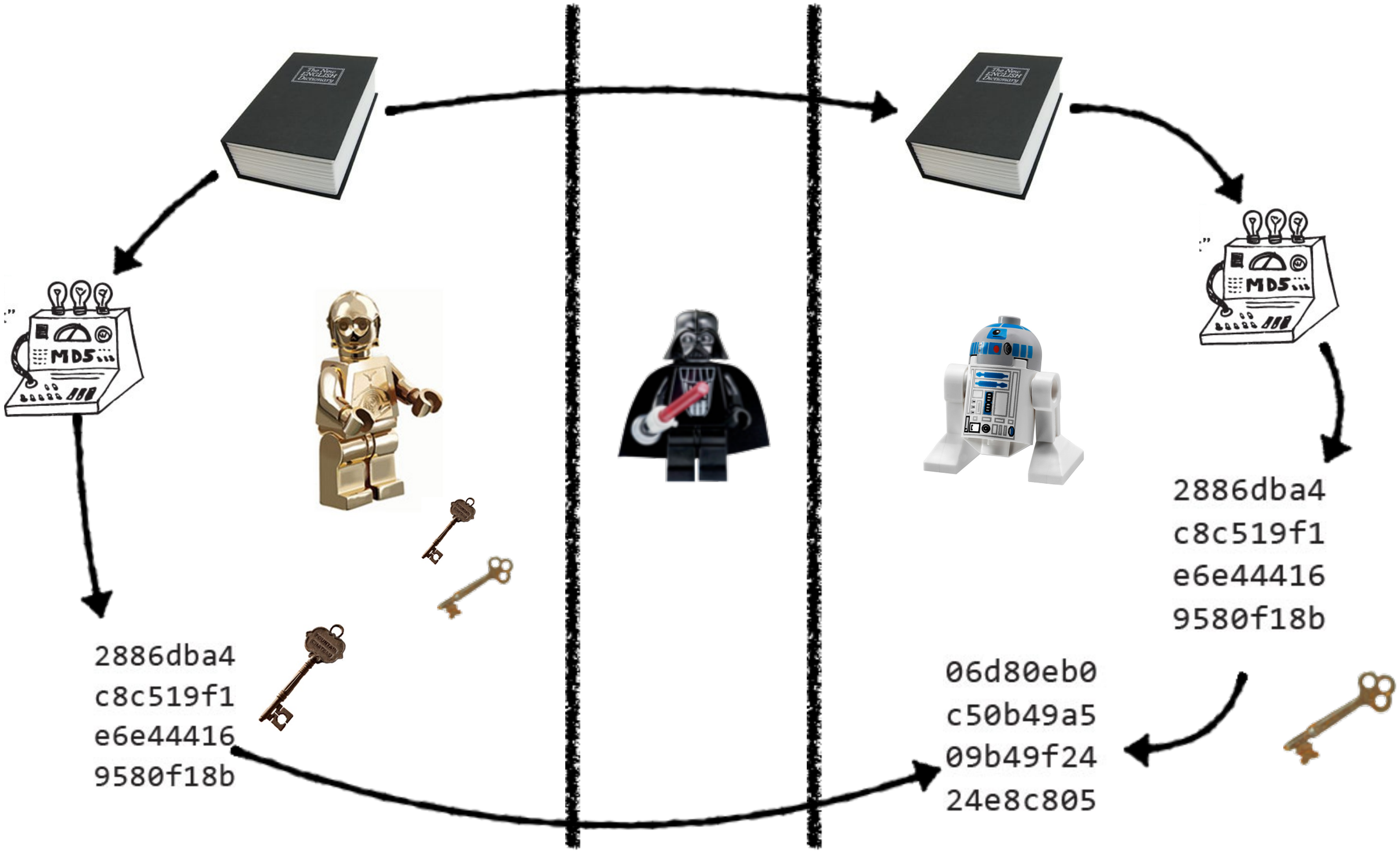
Criptographic hash functions

- **Pre-image resistance**: Given a hash h it should be difficult to find any message m such that h = hash(m). This concept is related to that of one-way function. Functions that lack this property are vulnerable to preimage attacks.

- **Second pre-image resistance**: Given an input m1 it should be difficult to find another input m2 such that m1 ≠ m2 and hash(m1) = hash(m2). Functions that lack this property are vulnerable to second-preimage attacks.

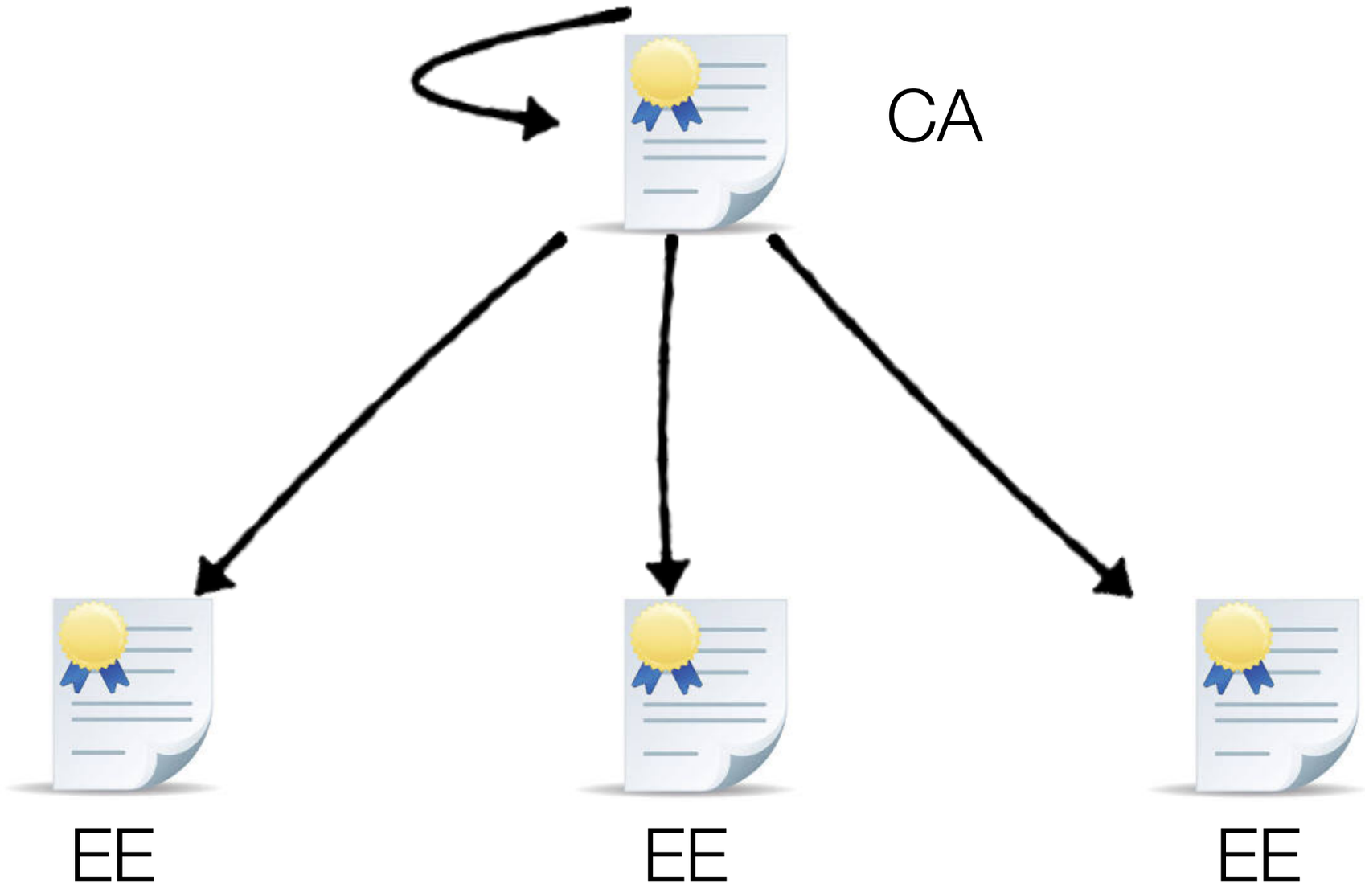
- **Collision resistance**: It should be difficult to find two different messages m1 and m2 such that hash(m1) = hash(m2). Such a pair is called a cryptographic hash collision. This property is sometimes referred to as strong collision resistance. It requires a hash value at least twice as long as that required for preimage-resistance; otherwise collisions may be found by a birthday attack.

Electronic signature

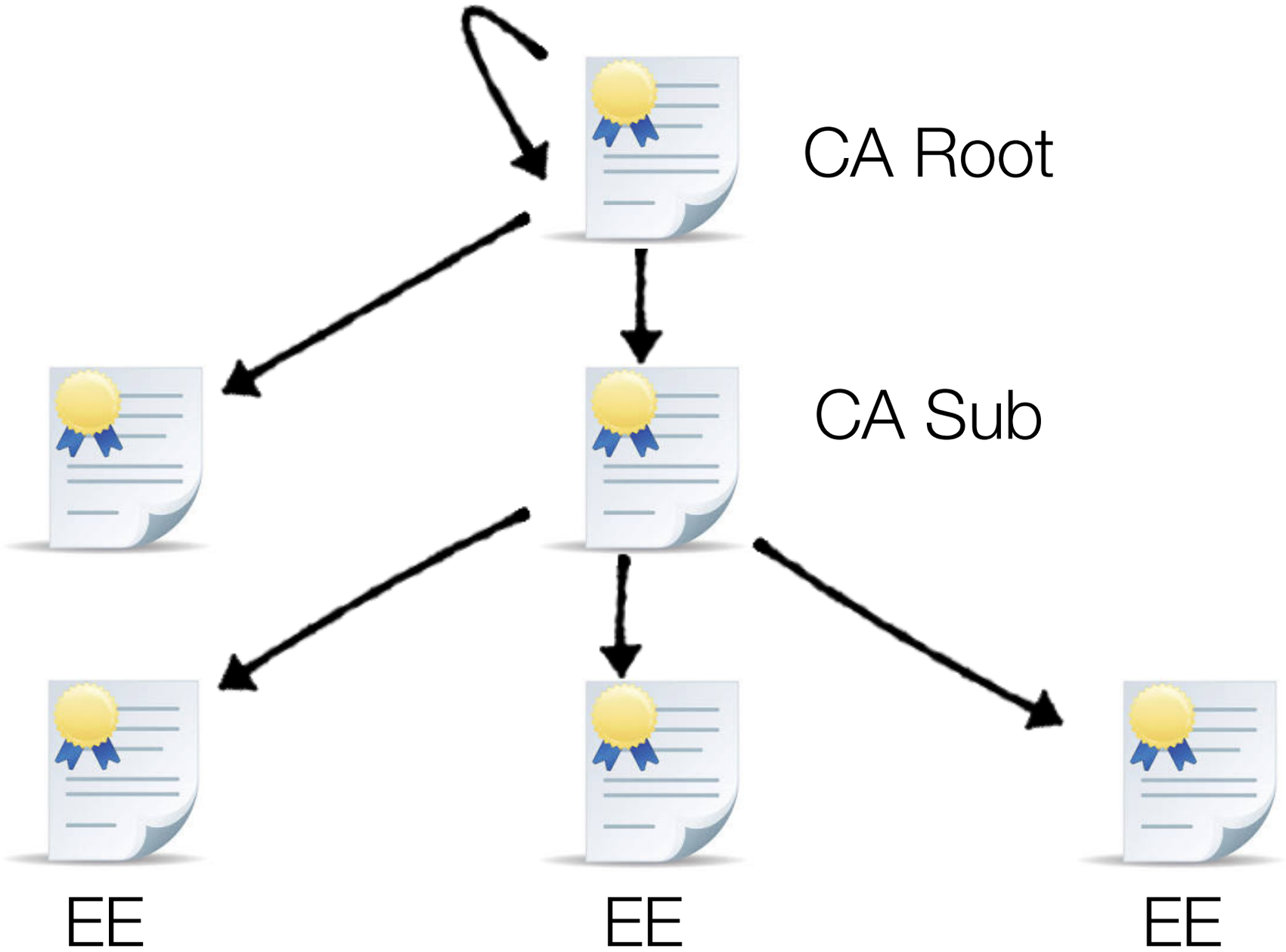


Public Key Infraestructure

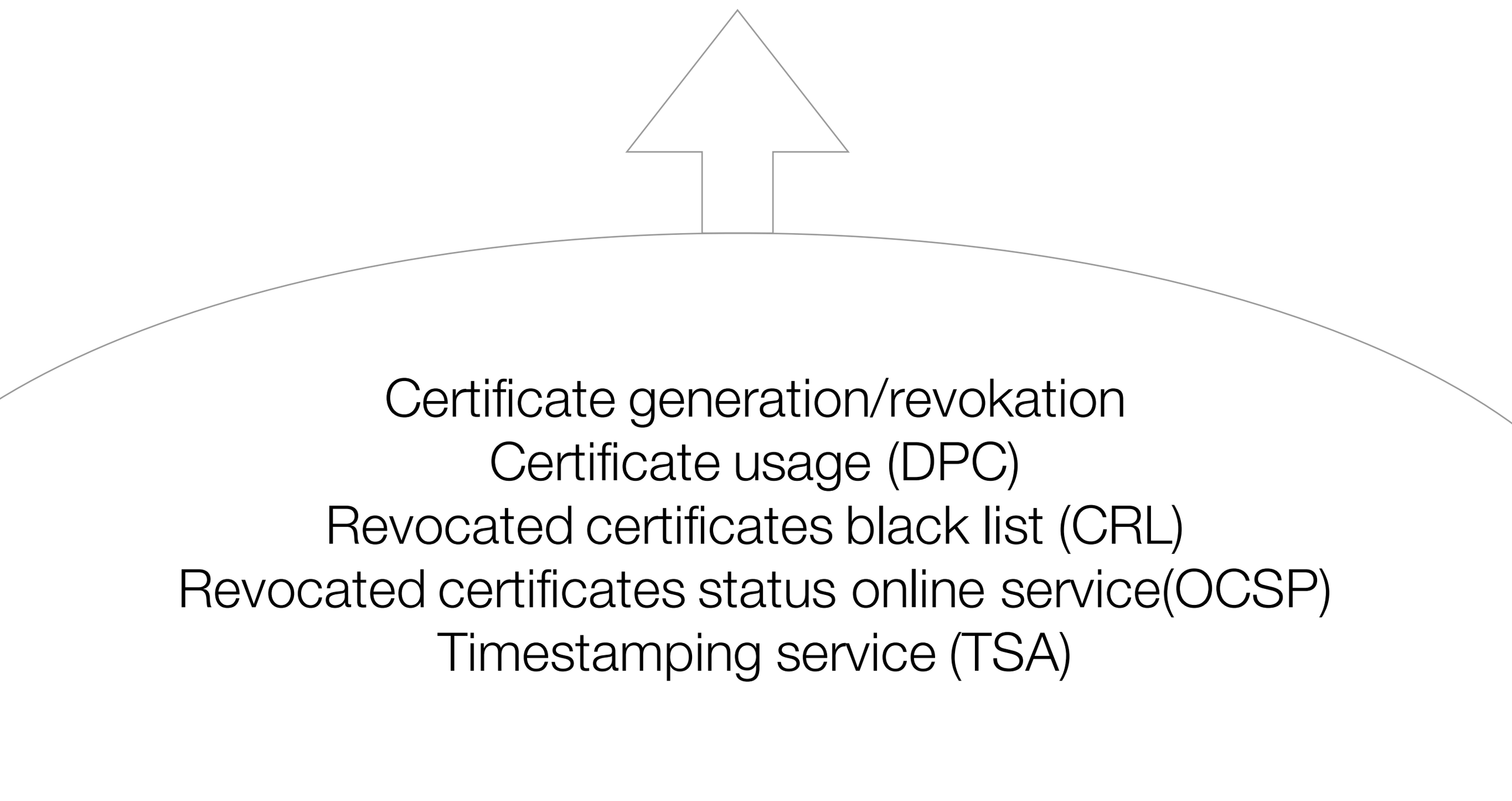
CA/EE



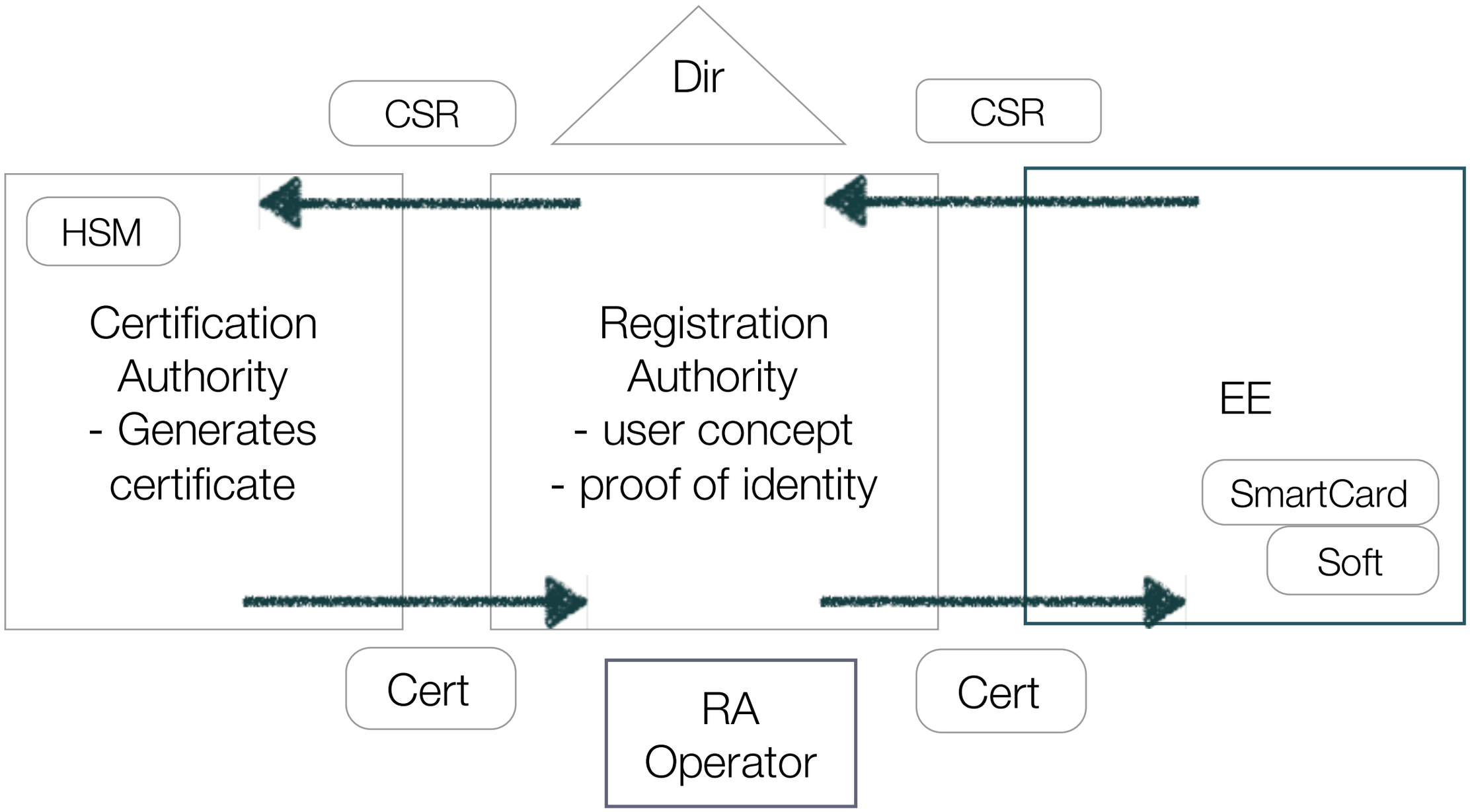
CA/EE



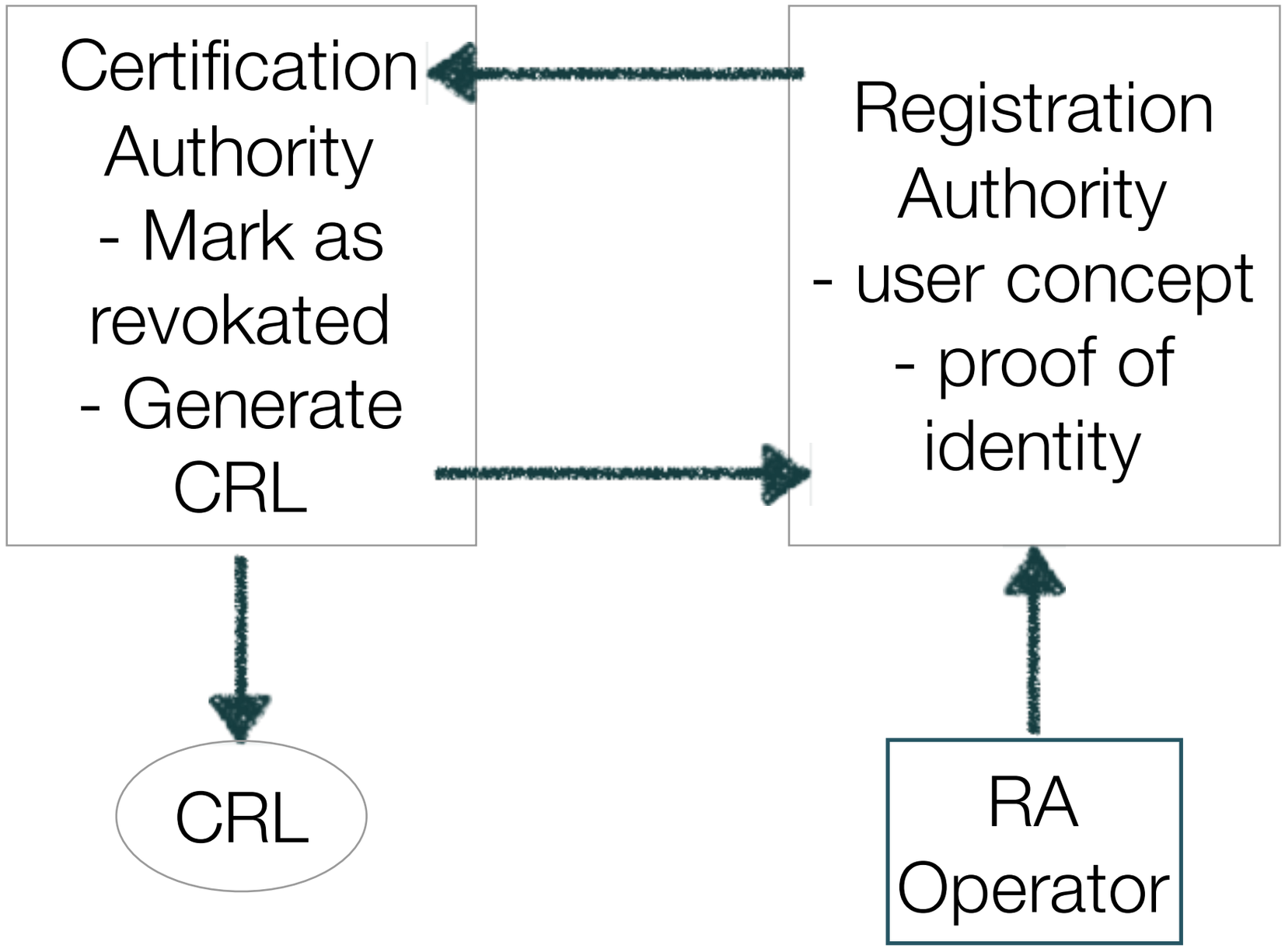
Certificate Service Provider



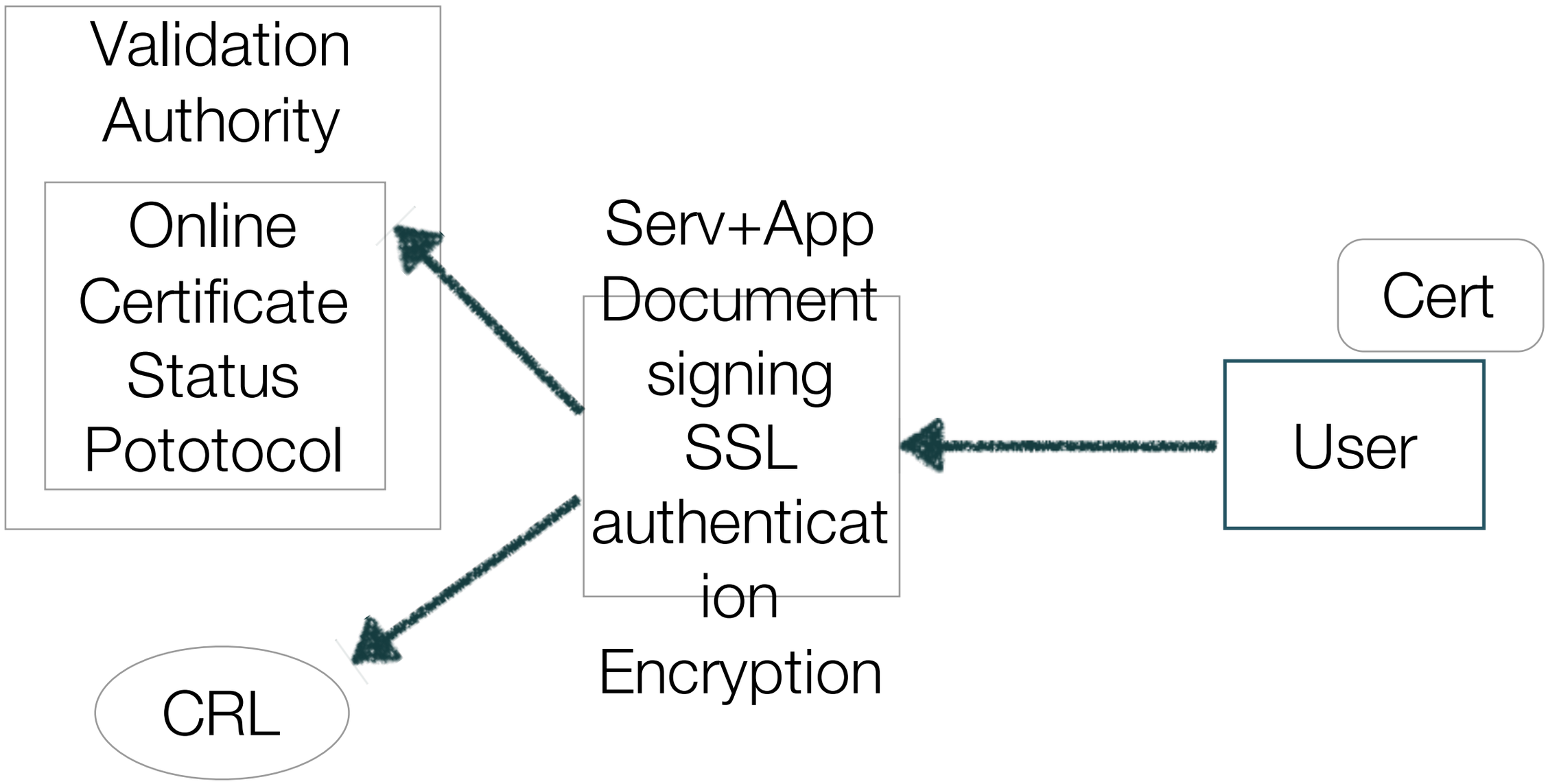
EE creation process



EE revocation process



EE certificate usage



Hands-on

Use MS cert viewer to inspect DNIe certificate, SSL certificates

PKI infrastructure

CA Admin

RA Admin

Certification Authority

HSM

CRL

Registration Authority

Validation Authority

Timestamp Authority

Dir

Serv+App
Document signing
SSL authentication
Encryption

Soft

HSM

Users

Browser

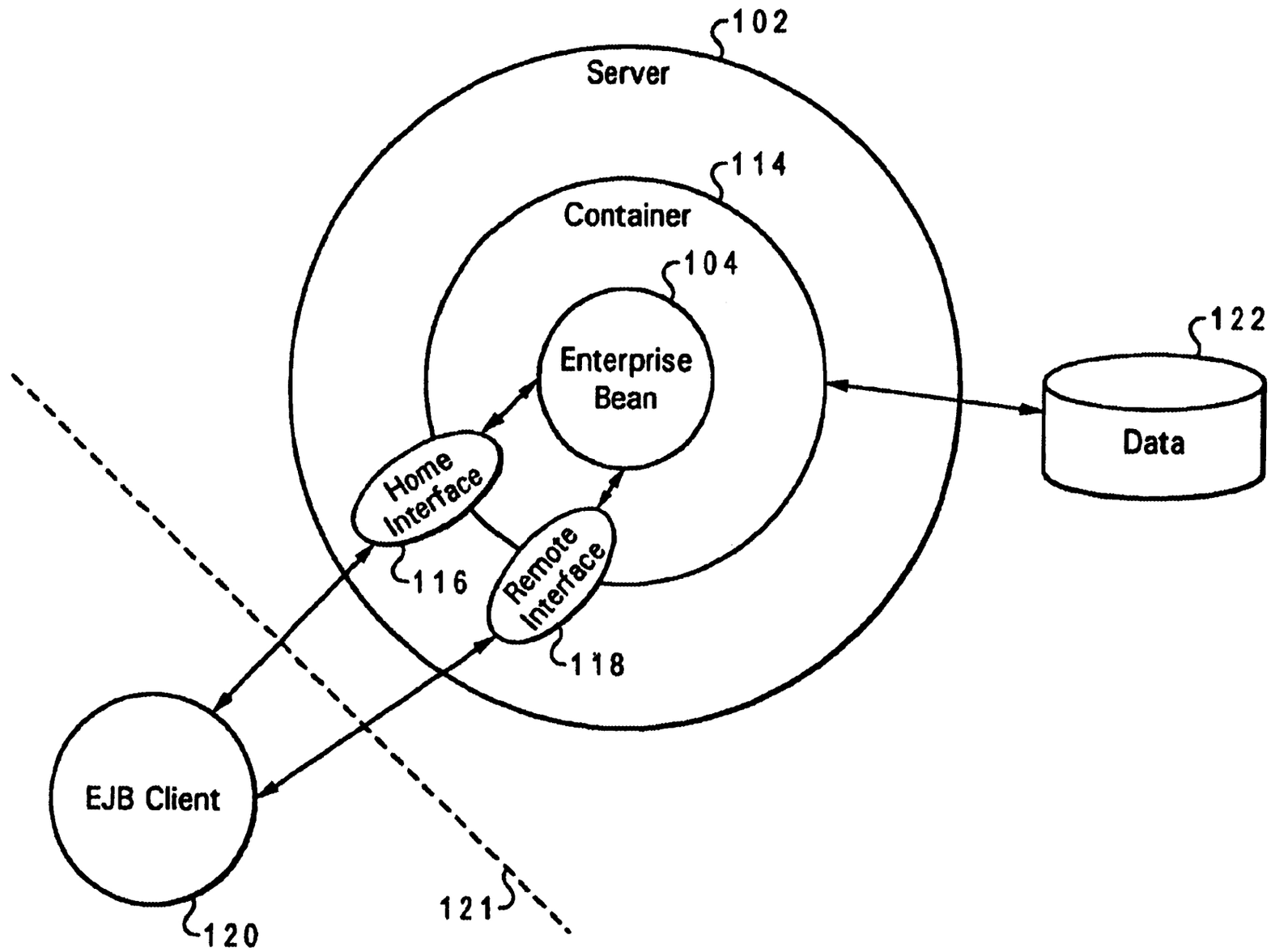
SmartCard

Cert

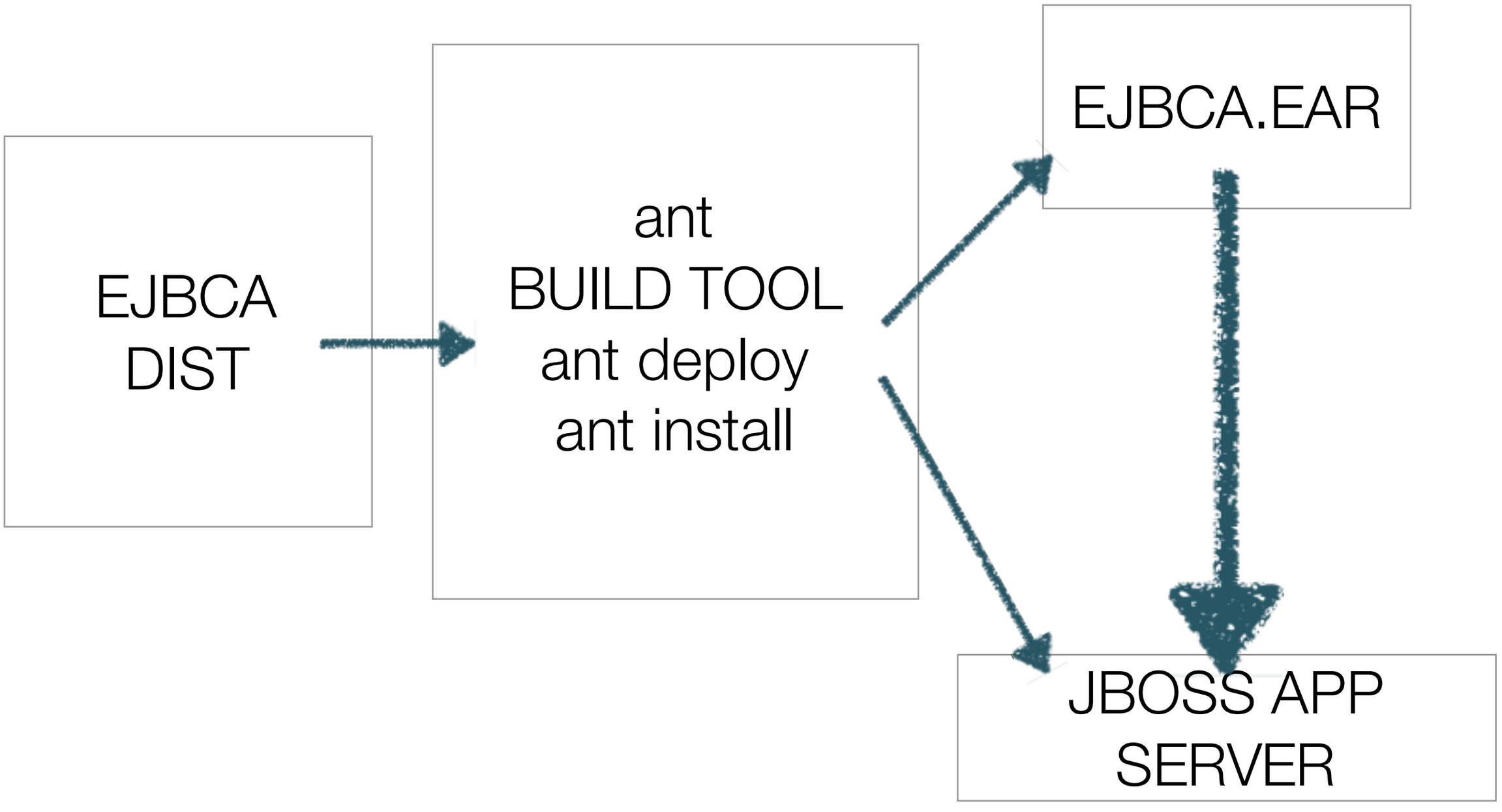
Certification policy declaration under applicable laws

Enterprise Java Beans Certificate Authority

Enterprise Java Beans



EJBCA static

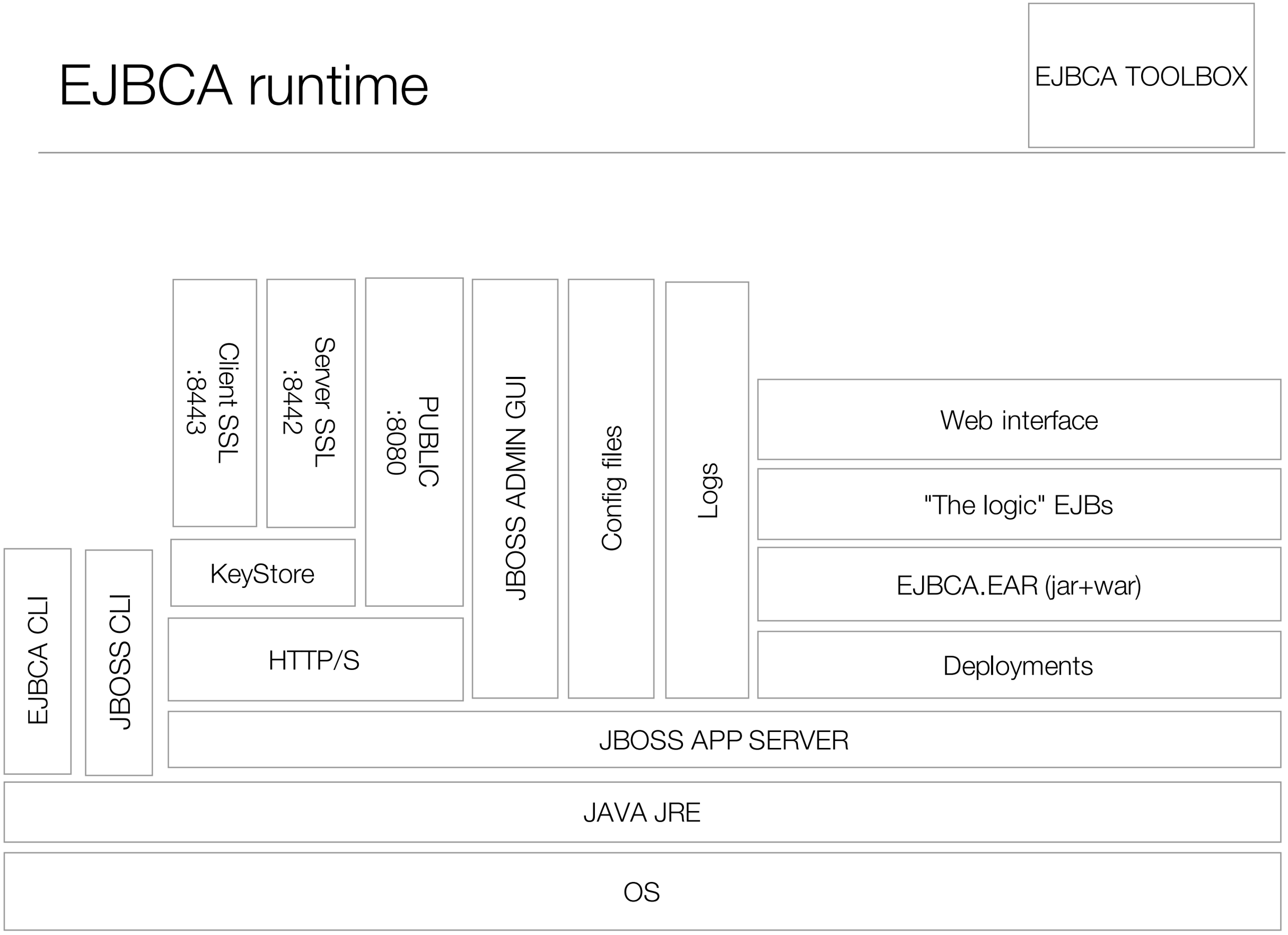


Hands-on

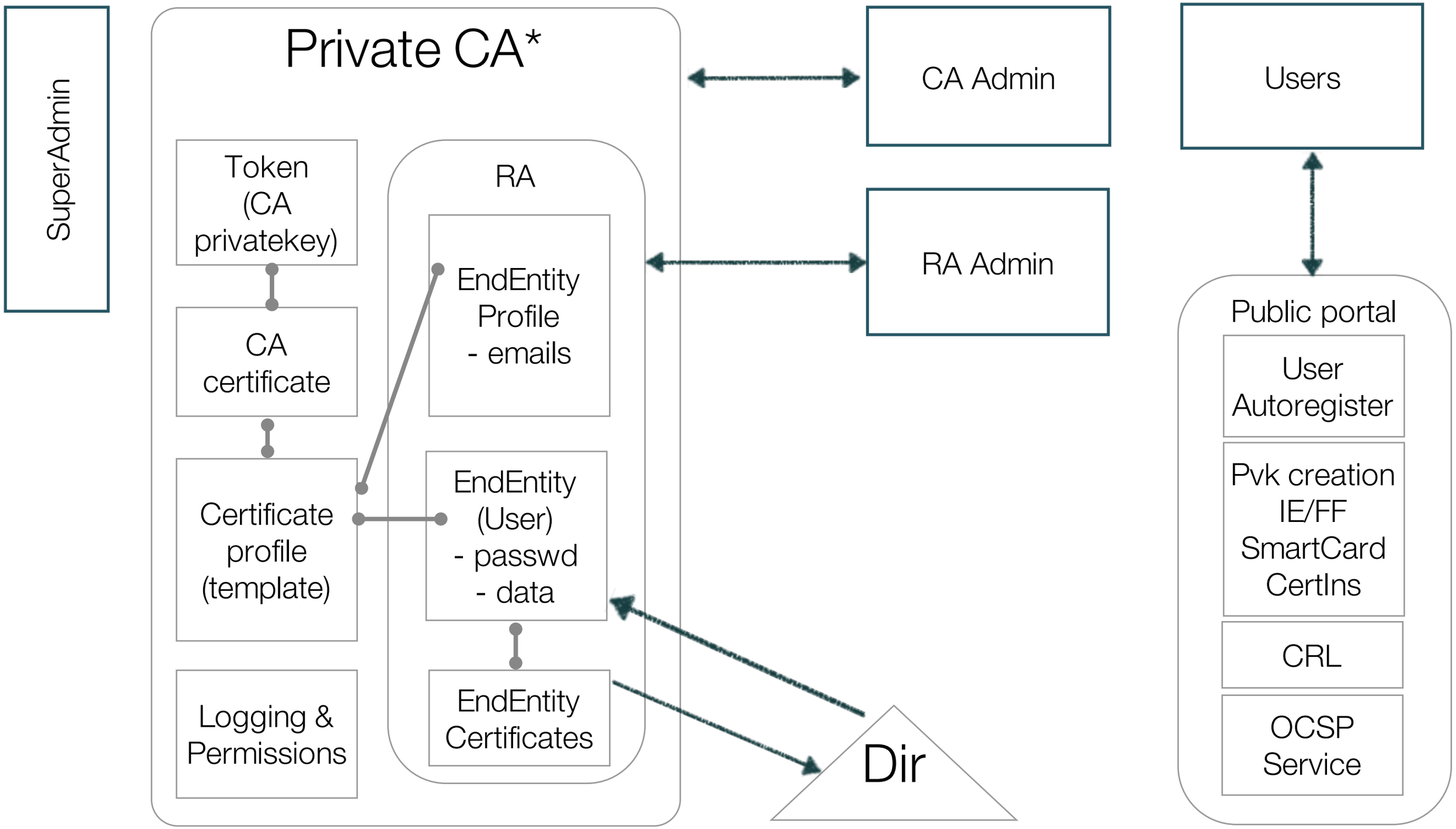
Build EJBCA from scratch

Issue self-signed certificates with EJBCA

EJBCA runtime



EJBCA


SuperAdmin
Private CA*
Token (CA privatekey)
CA certificate
Certificate profile (template)
Logging & Permissions
RA
EndEntity Profile - emails
EndEntity (User) - passwd - data
EndEntity Certificates
CA Admin
RA Admin
Dir
Users
Public portal
User Autoregister
Pvk creation IE/FF SmartCard CertIns
CRL
OCSP Service

The plan I

Management
CA Root

SuperAdmin

ROOT
CA

ClientSSL

ServerSSL

CSR

Hands-on

The plan I

The plan II

CA Root

SuperAdmin

Remot
e
access

CA Sub
Admin

CA Administrators

EJBCA server SSL

Email

CA Sub
Issuer

SelfEnrolled ClientSSL

RA Administrators

LDAP
Publish

Privileged ClientSSL (2 approv)

Hands-on

The plan II

CWA 14167 Qc PKI

CWA

CEN

WORKSHOP

AGREEMENT

CWA 14167-1

June 2003

ICS 03.120.20; 34.040

Supersedes CWA 14167-1:2001

English version

Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements

CWA

4.4 Security Levels

The certificates produced by a CSP fall into the following categories:

1. Non-Qualified Certificates (NQCs):

    - Used for Electronic Signatures, meeting [Dir.1999/93/EC], Article 5.2
    - Used for Electronic Signatures in internal tasks of the TWS

2. Qualified Certificates (QCs):

    - Used for Advanced Electronic Signatures (AES) which are created by a Secure-Signature-Creation Device (SSCD), meeting [Dir.1999/93/EC], Article 5.1
    - Used for Advanced Electronic Signatures (AES) which are created by a Signature-Creation Device (SCDev)

CWA

As a minimum, TWSs SHALL provide the following privileged roles:

Security Officers: Having overall responsibility for administering the implementation of the security policies and practices.

Registration Officers: Responsible for approving end entity Certificate generation/revocation/ suspension.

System Administrators: Are authorised to install, configure and maintain TWSs, but with controlled access to security-related information.

System Operators: Are responsible for operating TWSs on a day-to-day basis. Authorised to perform system backup and recovery.

System Auditors: Authorised to view archives and audit logs of TWSs.

[M1.4] – NQC ONLY

TWSs SHALL be capable of ensuring:

- A user that is authorised to assume a Security Officer role is not authorised to assume a System Auditor role.

[M1.4] – QC ONLY

TWSs SHALL be capable of ensuring:

- A user that is authorised to assume a Security Officer or Registration Officer role is not authorised to assume a System Auditor role.
- A user that is authorised to assume a System Administrator role is not authorised to assume a Security Officer or a System Auditor role.

CWA

[KM1.1]

QC/NQC Signing Keys MUST be generated and stored in a secure cryptographic module.

[KM1.2]

This secure cryptographic module of [KM1.1] MUST be evaluated and certified to fulfil the following requirements:

- The module MUST ensure the confidentiality and integrity of the keys during their whole life time;
- The module MUST be able to identify and authenticate its users;
- The module MUST restrict access to its services, depending on the user and his role, to those services explicitly assigned to this user and his role;

[KM1.3]

The secure cryptographic module MUST ONLY generate QC/NQC Signing Keys under at least dual person control.

Note: Dual control of the required function MAY be achieved either directly by the secure cryptographic module or by the TWS implementing suitable dual controls.

QC/NQC

The QC/NQC Signing Key of the Certificate Generation Service may be stored and backed up only when additional security mechanisms are in place. For instance, this may be accomplished using m of n techniques, where m component parts out of a total of n component parts are required for successful key initialisation. For recovery from failure purposes, it is RECOMMENDED that m ≥ 60% * n (i.e. if n = 3, then m = 2. If n = 4, then m = 3, if n = 5, then m = 3, etc.)

[AA5.1]

TWSs SHALL prohibit all user read access to the audit records, except those users that have been granted explicit read access (e.g. those with System Auditor role).

[AA7.1] – QC ONLY

TWSs MUST ensure the integrity of the audit data.

To achieve this, TWSs SHOULD provide a Digital signature, keyed hash or an authentication code with each entry in the audit log, computed over the entire audit log or over the current entry and the cryptographic result of the previous one.

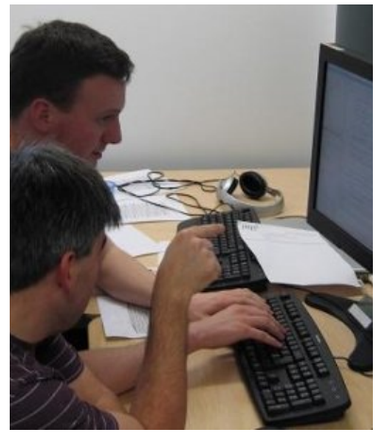
TWSs MUST also provide a function to verify the integrity of the audit data.

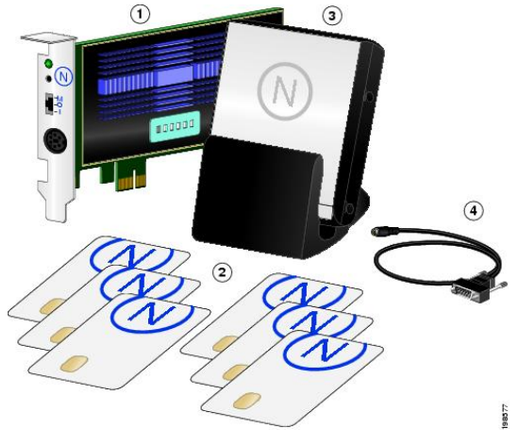
CWA

[BK2.1] – QC ONLY

Backups SHALL be protected against modification through use of digital signatures, keyed hashes or authentication codes.

Structure for QC/WebTrust





DPC

ENTRANCE

Security airlock

Dual-control operation

Smartcard & HSM

Gràcies

adriamassanet@gmail.com