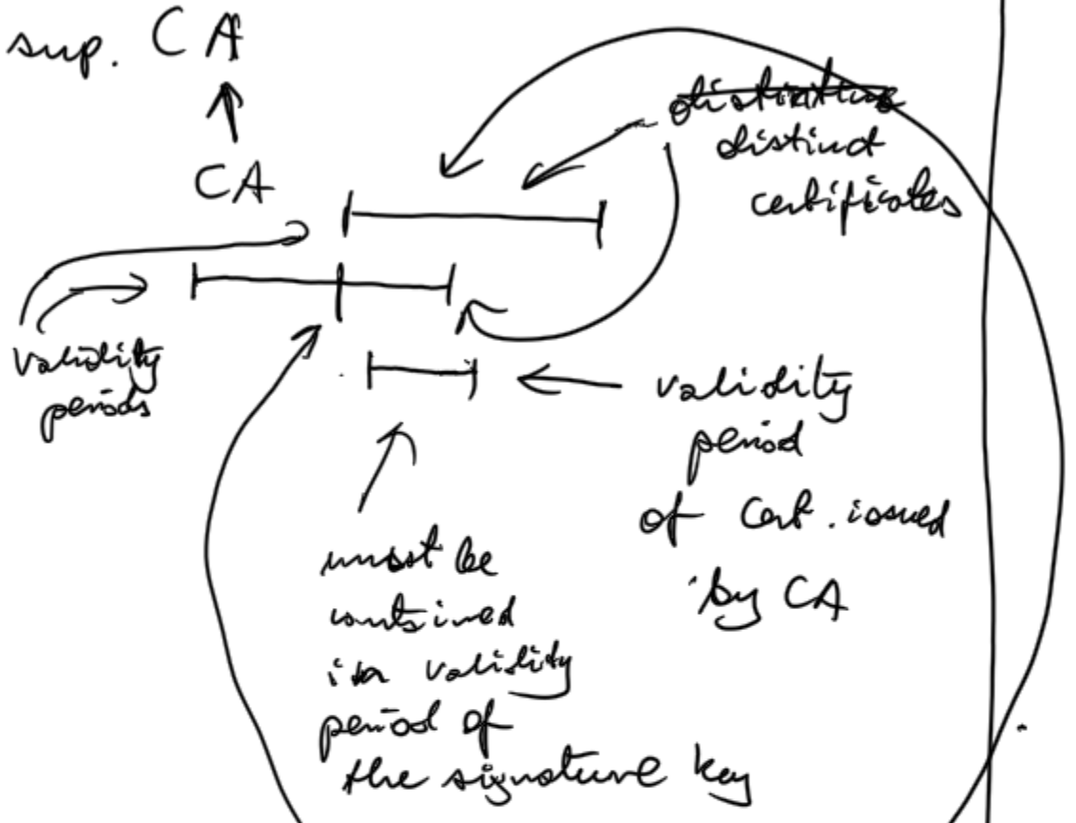
privateKeyUsagePeriod



good practice: generate a new key for that certificate

Sup. CA may enforce CA to request for a new cert. for a new key at this time by setting privateKeyUsagePeriod extension

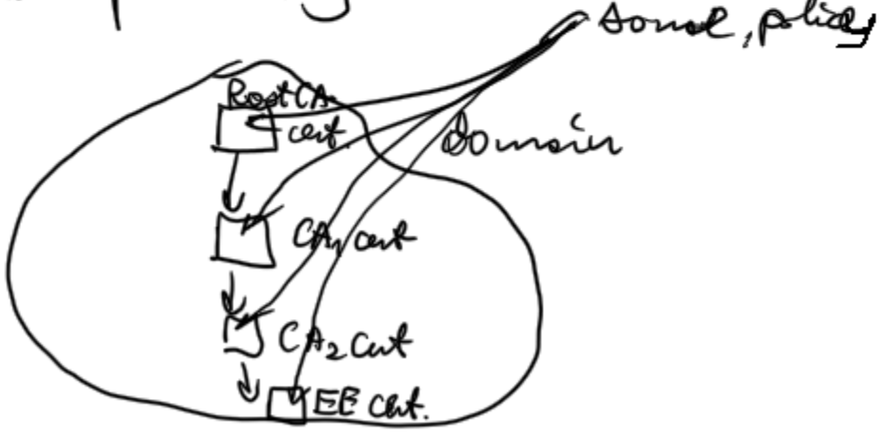
simple case

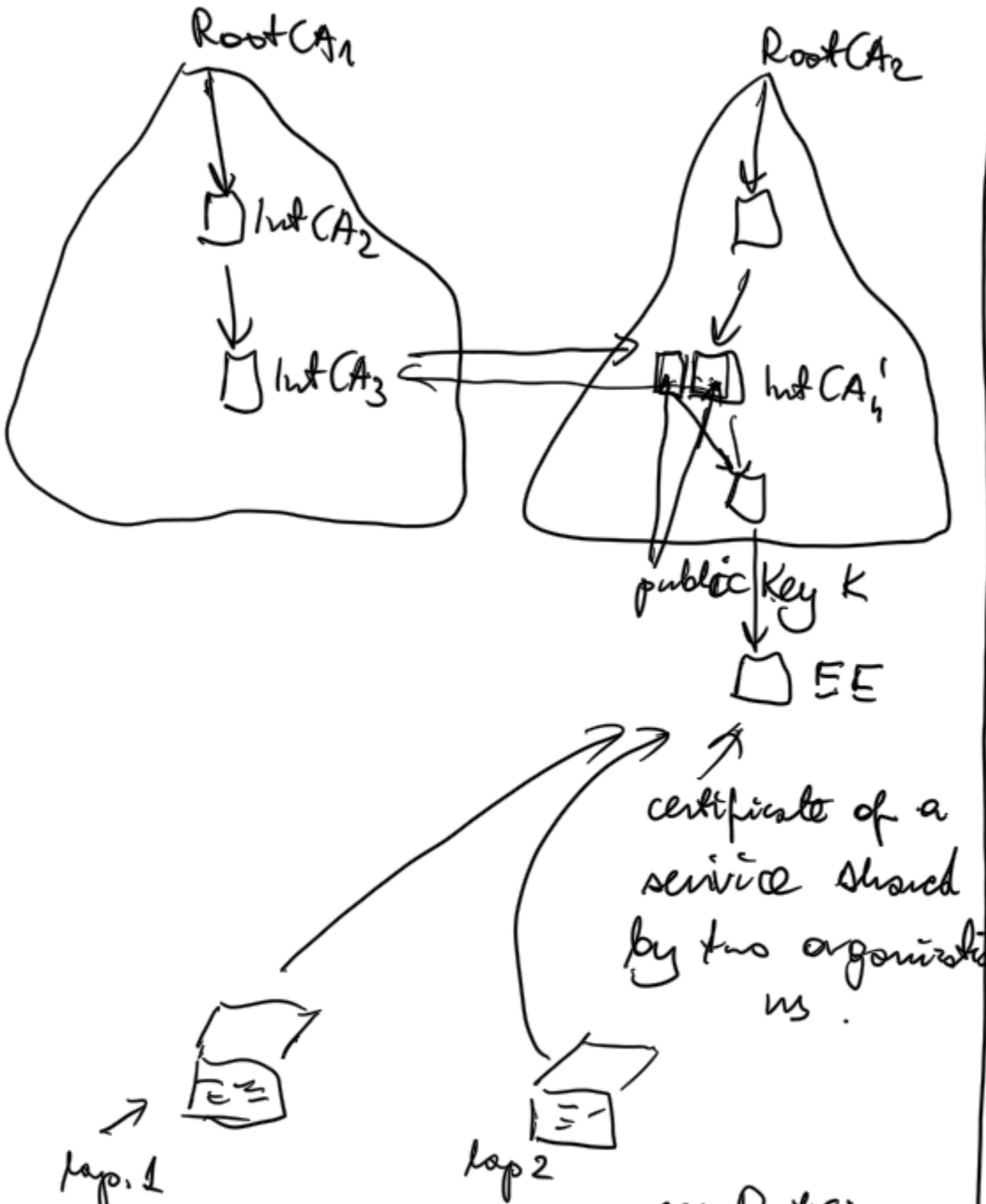
Certificate Policies - describes:

- the means taken to verify subject's identity
- the value of transactions allowed for a certificate class,
- type of storage required for private key material

RFC 3647

identified by OID





to build alternative certificate chain. Int CA_4' requests for a new certificate for a key K to Int CA_3.

Policy mapping extension

Assume that in organization 1 the policy is 1.5.6.7 and the parties agreed that in organization 2 the requirements of the policy 1.5.6.7 are satisfied by the policy 1.4.3.2.

So issuing the certificate for Int CA_4' the authority Int CA_3 writes in the certificate

the policy mapping extension must

1.5.6.7 → 1.4.3.2

↑

from now on in the chain of certificates this policy is required

There is a special anyPolicy OID which is interpreted as a wildcard

Subject Alternative Name

multiple hostnames can be represented in a single cert. (the same host).

SAN[0] = DNSName: finanzas.santander.com
SAN[1] = DNSName: fin.santander.com
SAN[2] = DNSName: finweb.santander.com

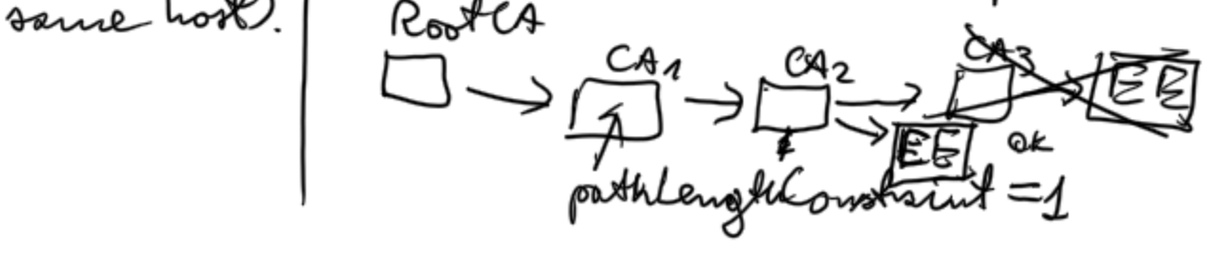
a few extensions of this type are present in the cert.

Issuer AlternativeName should be equal to the SAN of the issuer.

BasicConstraints — critical extension

CA - true or false?

pathLengthConstraint is meaningful only for CA certificates



Name Constraints

↳ see the example (link in the main document)

KeyUsage Extension : not verified

↳ Signature → ec-key (ecdsa)

KCi (key Compromise impersonation)

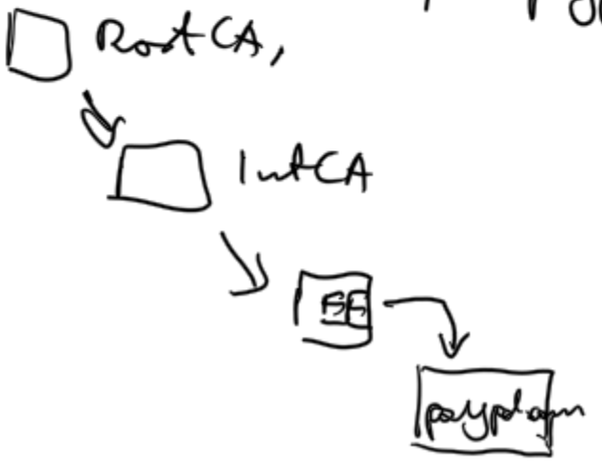
~2015

Not verified basic constraint

CA = true?

2009 - some implementation did not check that condition

EE has issued a certificate for paypal.com



Hacker breaks into clients computer and ~~steal~~ put there a private key c, and the public key g^c and a self signed certificate for g^c.