Elektronický podpis

Marek Kumpošt
Kamil Malinka

Související technologie

- kryptografie – algoritmy pro podepisování dokumentů
- management klíčů – generování klíčů, distribuce, revokace, verifikace implementace
- bezpečnostní politika – definice, ověření dodržování
- administrativní bezpečnosti – přístup k soukromému klíči CA
- fyzická bezpečnost – centrální počítač na velmi bezp. místě
- archivace – dokumentů, certifikátů, revokovaných klíčů ...
- právní úpravy pro použití el. podpisů

Elektronický vs. digitální podpis

- Rozlišní na základě Evropské legislativy
  - el.podpis – jakákoliv informace identifikující odesílatele zprávy, např. prosté podepsání se pod email
  - digitální podpis – podpis založený na kryptografii, splňující určité bezpečnostní požadavky, např. nepadělatelnost

Analogie s ručně psaným podpisem

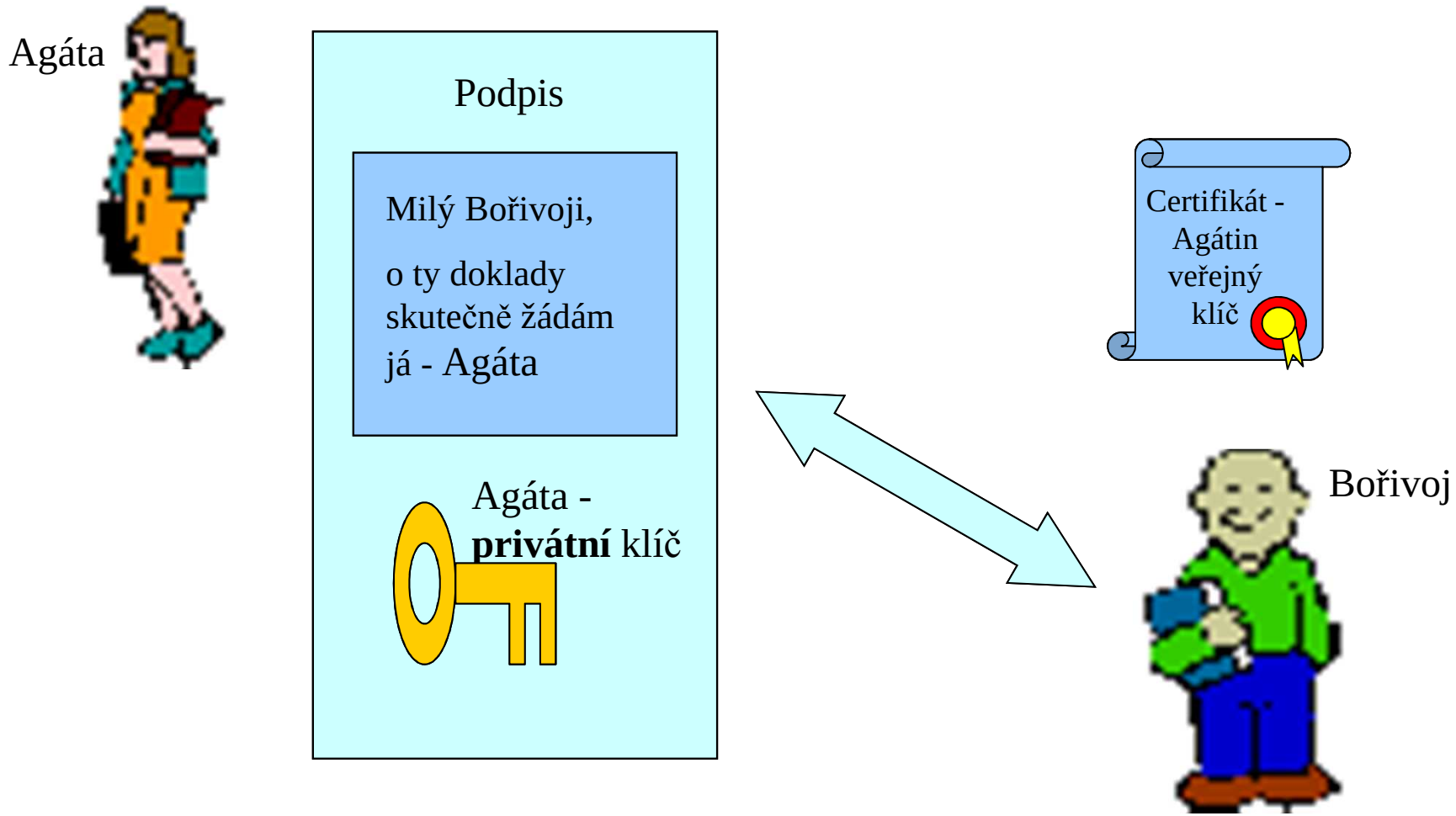
Pojem	**ručně psaný**	**digitální**
zpráva	papír se zprávou	elektronická data
podpis	„škrt“ napsaný rukou	podpis vytvořený krypt. prostředky + samotná zpráva
potřebné k podpisu	schopnost uvažovat, nácvik, schopnost psát	privátní klíč
potřebné pro verifikaci	znalost, zkušenost, zrak, podpisová karta	certifikát veřejného klíče

- vůle člověka podepsat se vlastnoručním podpisem...

Podpis v digitální formě - požadavky

- Musí zajistit autentizaci podepsaných dat.
  - Integrita
  - Prokázání původu dat
- Měl by podporovat ověření data/času podpisu.
- Měl by být ověřitelný i třetími stranami.
- Měl by podporovat mechanismy nepopiratelnosti

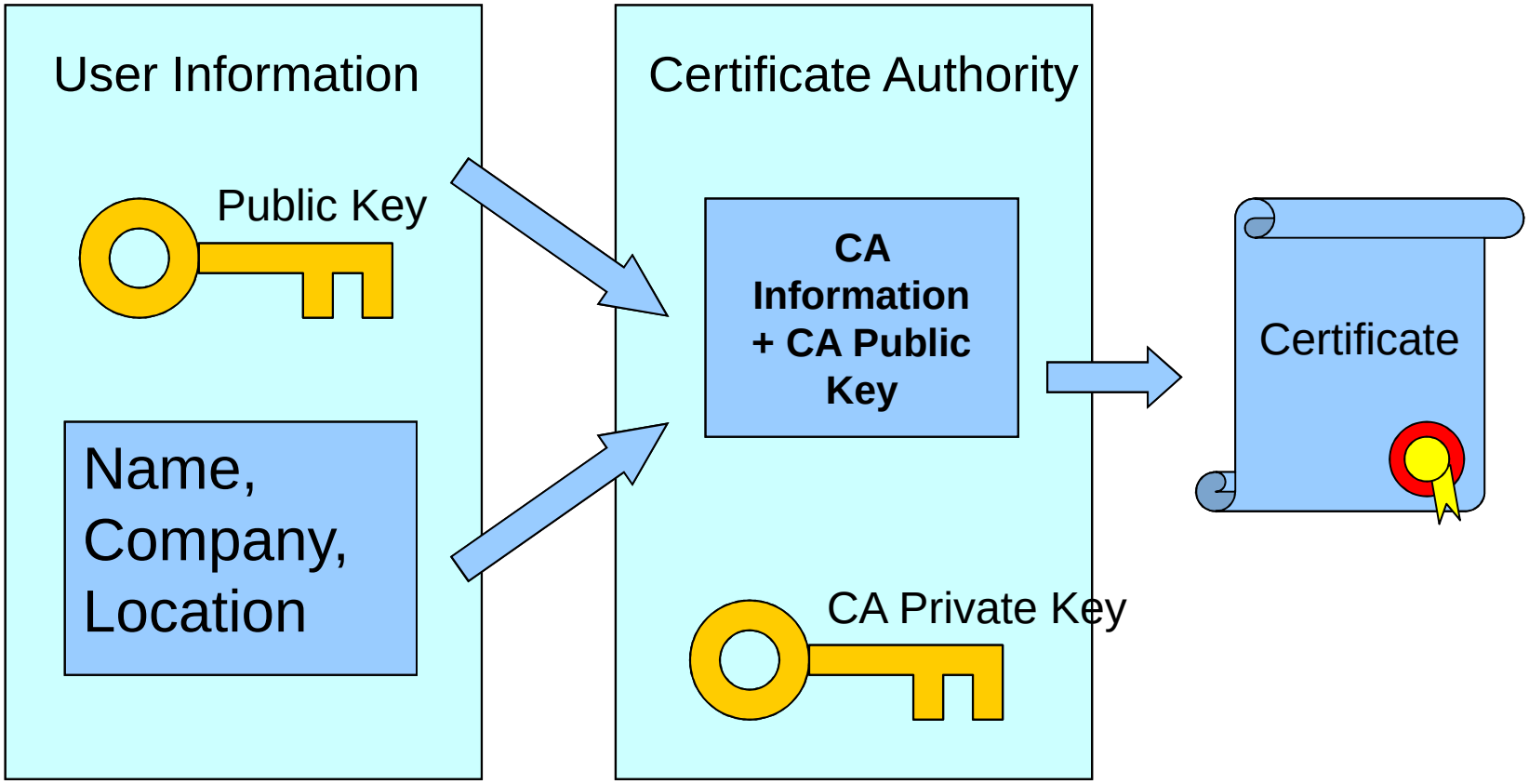
Co je digitální podpis?



Digitální podpis

- Nezajišťuje důvěrnost (šifrování)
- Nejznámější algoritmy – RSA, DSA
- Obecně existují algoritmy
  - s obnovou zprávy (podpis „obsahuje“ podepisovaná data),
  - **bez obnovy zprávy (podpis „neobsahuje“ data)**
- Asym. algoritmy jsou relativně pomalé, proto se podepisuje haš – „otisk dat“
- Fáze postupu:
  - Vytvoření a registrace klíčů (certifikát)
  - Vlastní podepsání
    - Dokument $\Rightarrow$ haš $\Rightarrow$ podpis
  - Ověření podpisu

Co je certifikát?



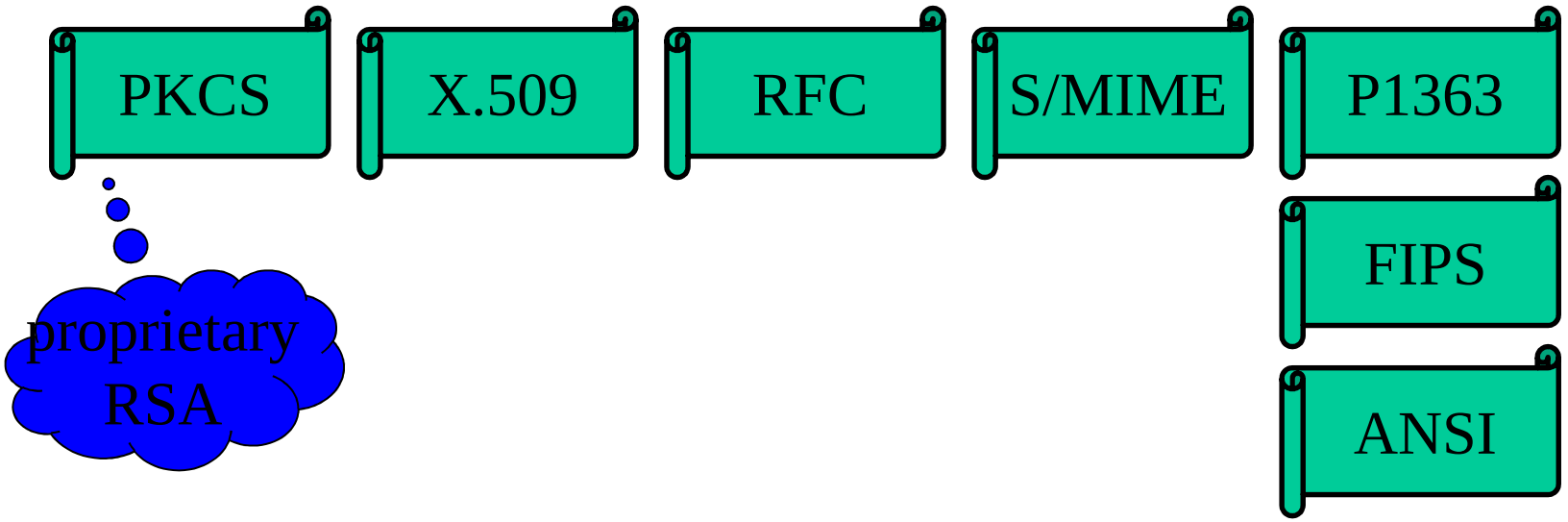
Infrastruktura veřejných klíčů

- komplexní technologie pokrývající problémy správy klíčů ve vztahu k digitálnímu podpisu
- první produkty v devadesátých letech
  - vysoká cena
  - žádná aplikace
  - zpočátku špatně prodejná technologie
- v současnosti existuje několik PKI řešení – Entrust, Verisign, RSA, IBM,
- Česká republika – 1.CA – společnost PVT, většina bank má své PKI řešení

Několik standardů

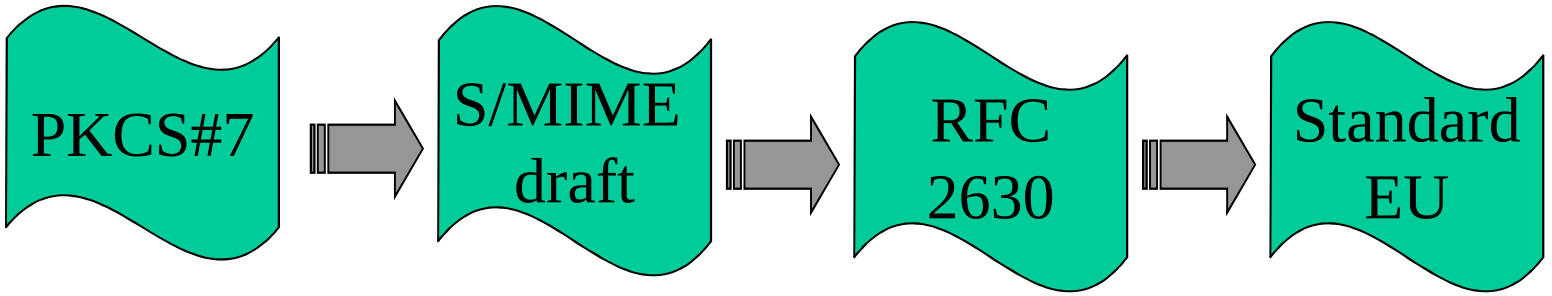
- X.509 – hierarchická stromová struktura
- PGP – každý uživatel má domain of trust
- SPKI/SDSI – jména jsou unikátní pouze ve konkrétním kontextu

X.509 Systémy



Syntaxe šifrovaných zpráv

šifrované a podepsané zprávy



Standardy pro jednotlivé oblasti

- PKI - X.509, PKCS#10, #12 (#6, #9)
- electronický mail - CMS, S/MIME drafts
- algoritmy - PKCS#1, P1363, FIPS, ANSI
- komunikační protokoly - X.509, SSL, RFC, ...

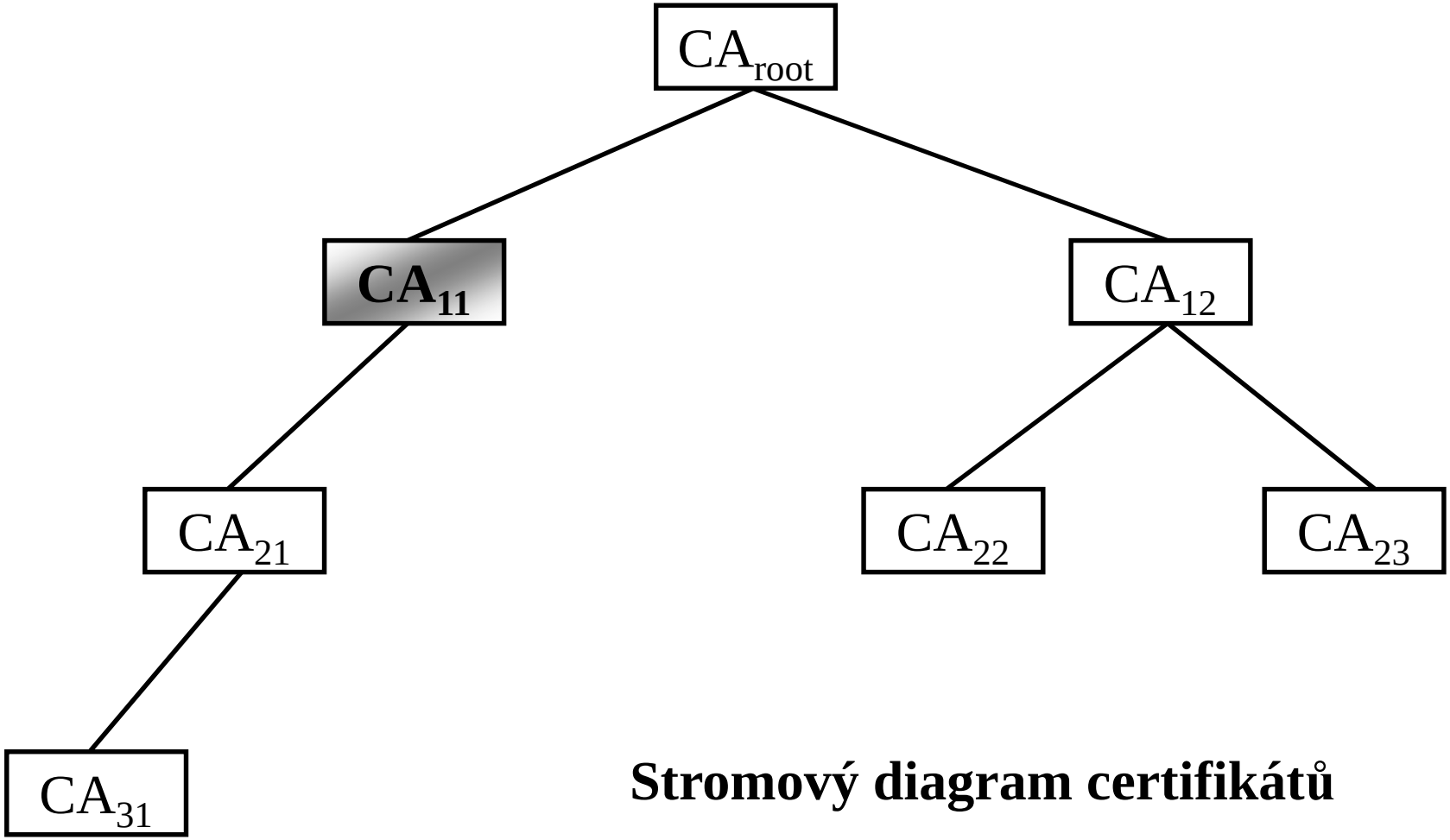
Vývoj designu

- idealistické předpoklady – centrální CA, které všichni věří
  - PEM, X.509
  - jedna CA => jedna politika, certifikáty bez dalších bezp. politik
- realizace - centrální CA nikdy nevznikne
  - PKCS #6, X.509v2, 3
- vytvoření homogenního systému - PKI je rozsáhlá věc
  - nové standardy okolo X.509
- ustanovení národních PKI schémat/struktur

Aktuální stav

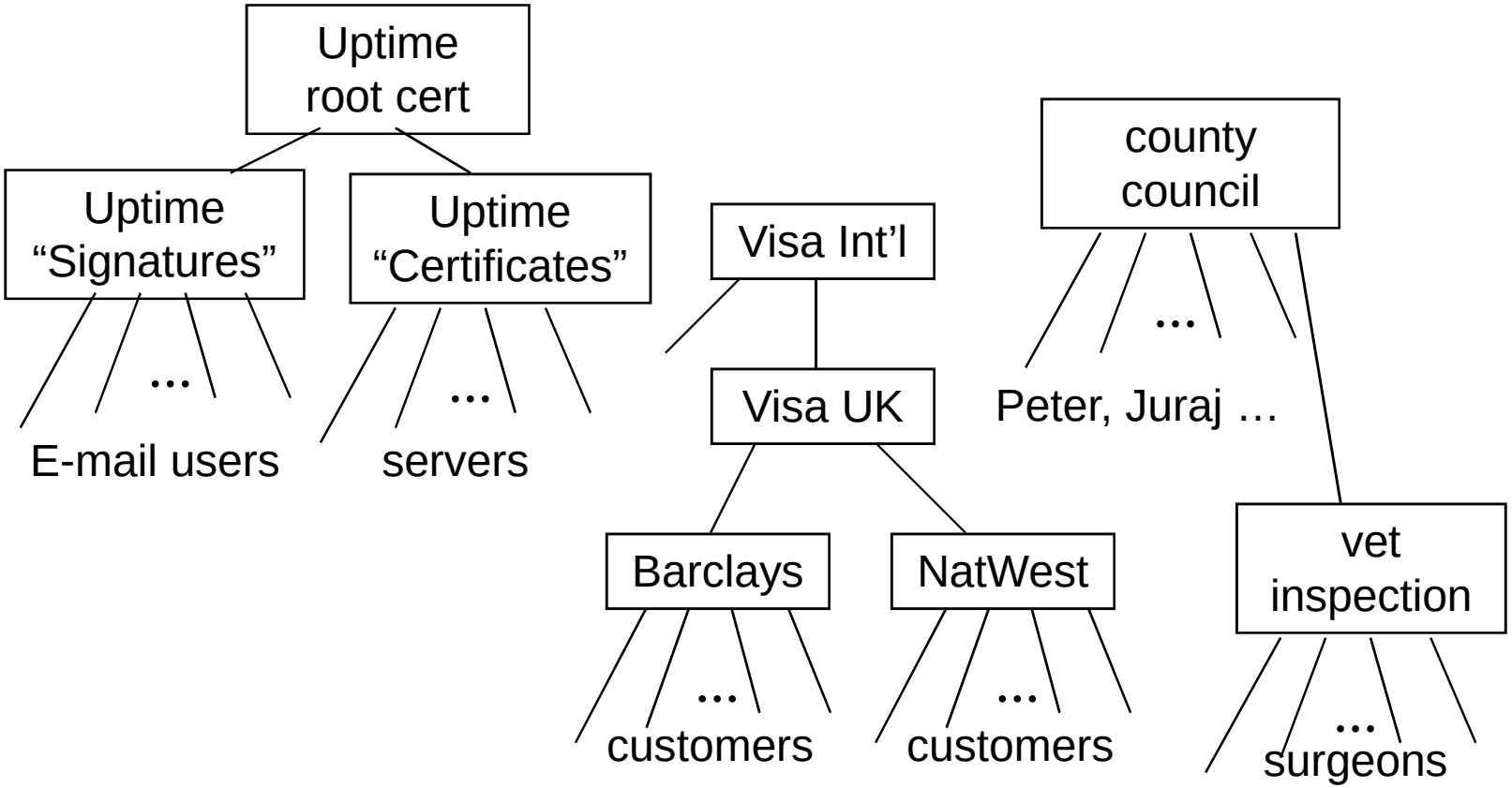
- roztroušenost => nekompletnost, redundance
  - X.509, PKCS #10
  - již dříve definováno, ale velmi komplikované: požadavky na revokaci, požadavky na certifikáty pouze pro RSA, nepředpokládá se další využití klíčů (např. podpis, šifrování)
- Jednotný model
  - založený na žádosti o certifikát (CRMF) umožňující veškeré bezpečnostní vlastnosti
  - definice kompletní množiny zpráv pro management PKI
  - nové koncepty a jejich podpora v nových protokolech

PKI – vysokoúrovňový pohled

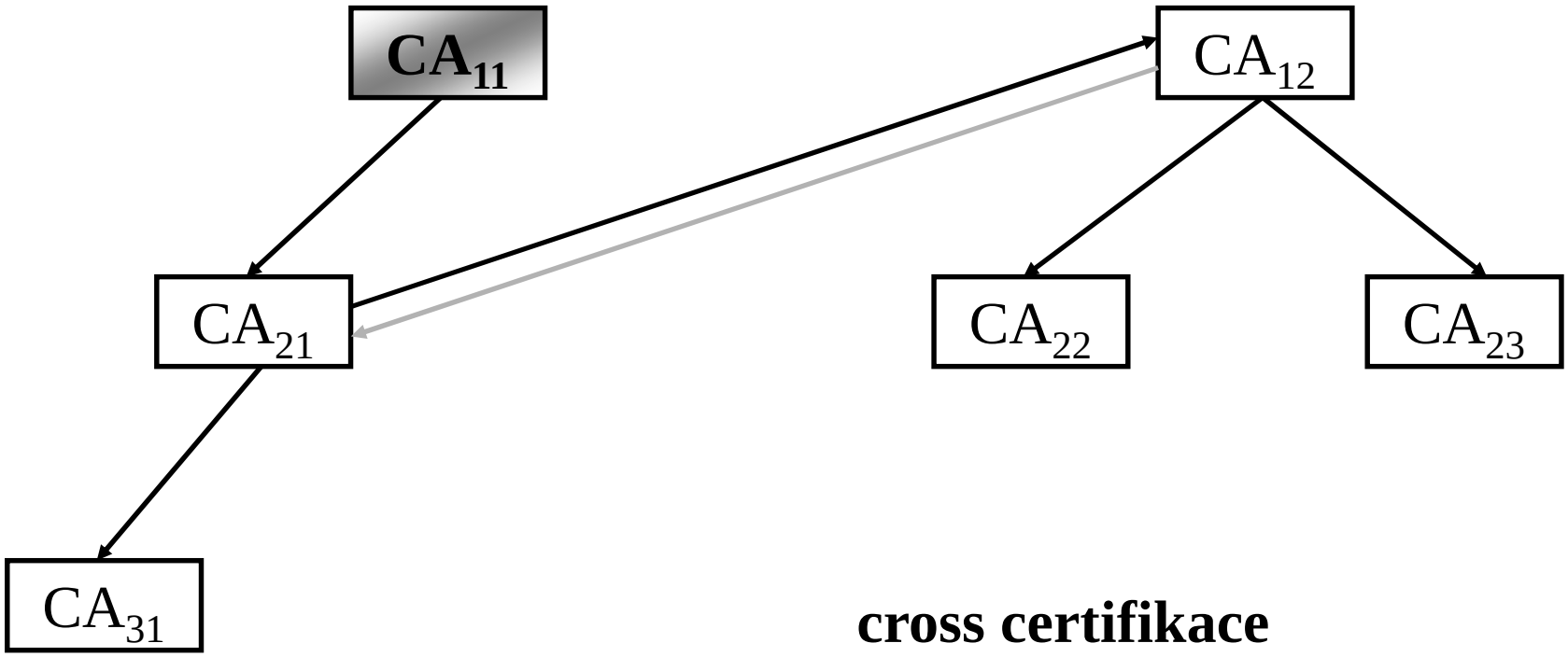


Stromový diagram certifikátů

CA hierarchie – příklad

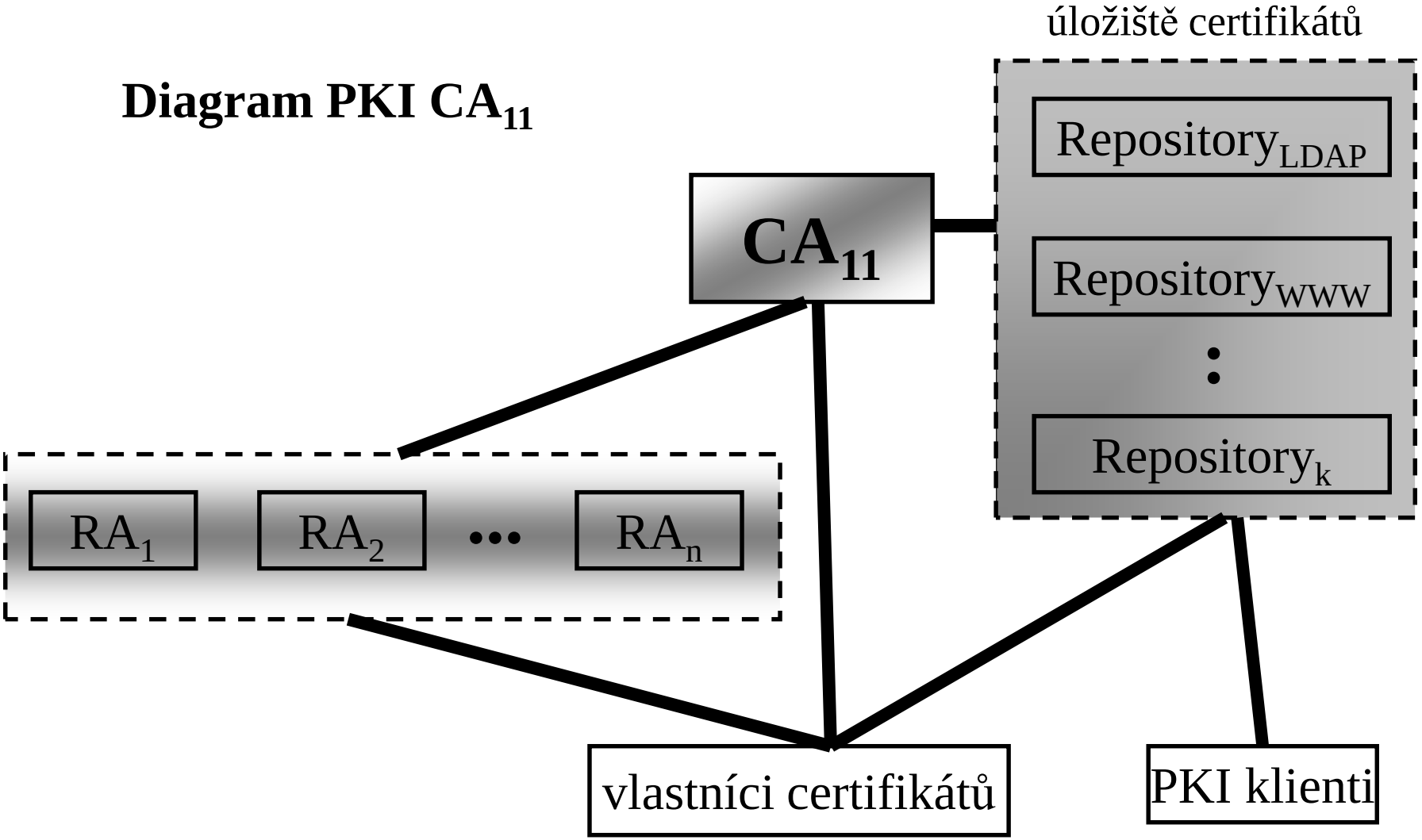


Cross certifikace



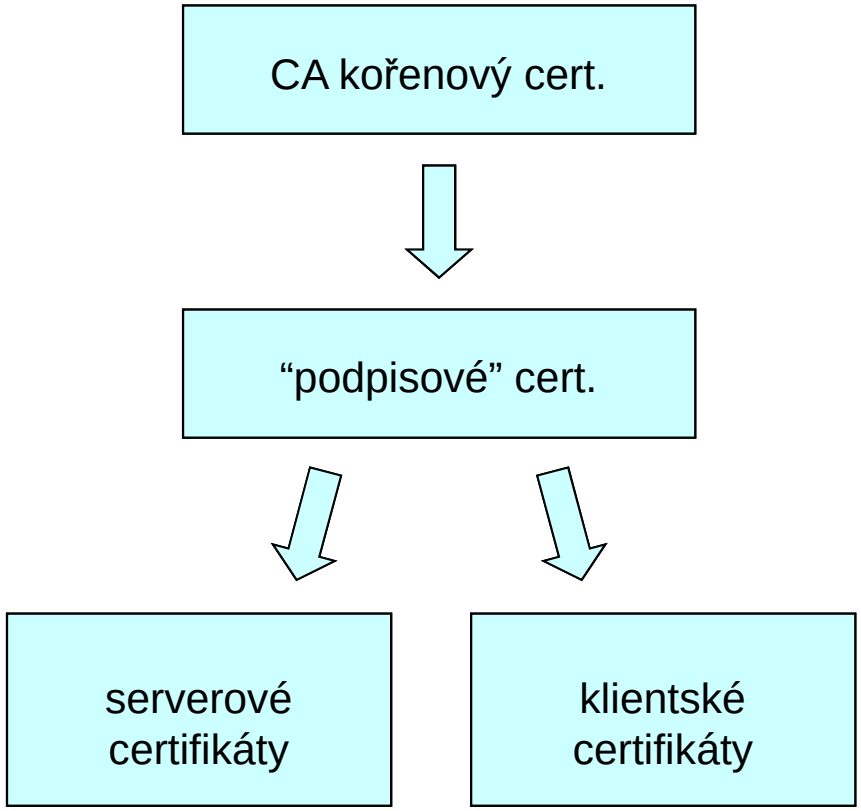
Certifikační autorita

Diagram PKI CA_{11}

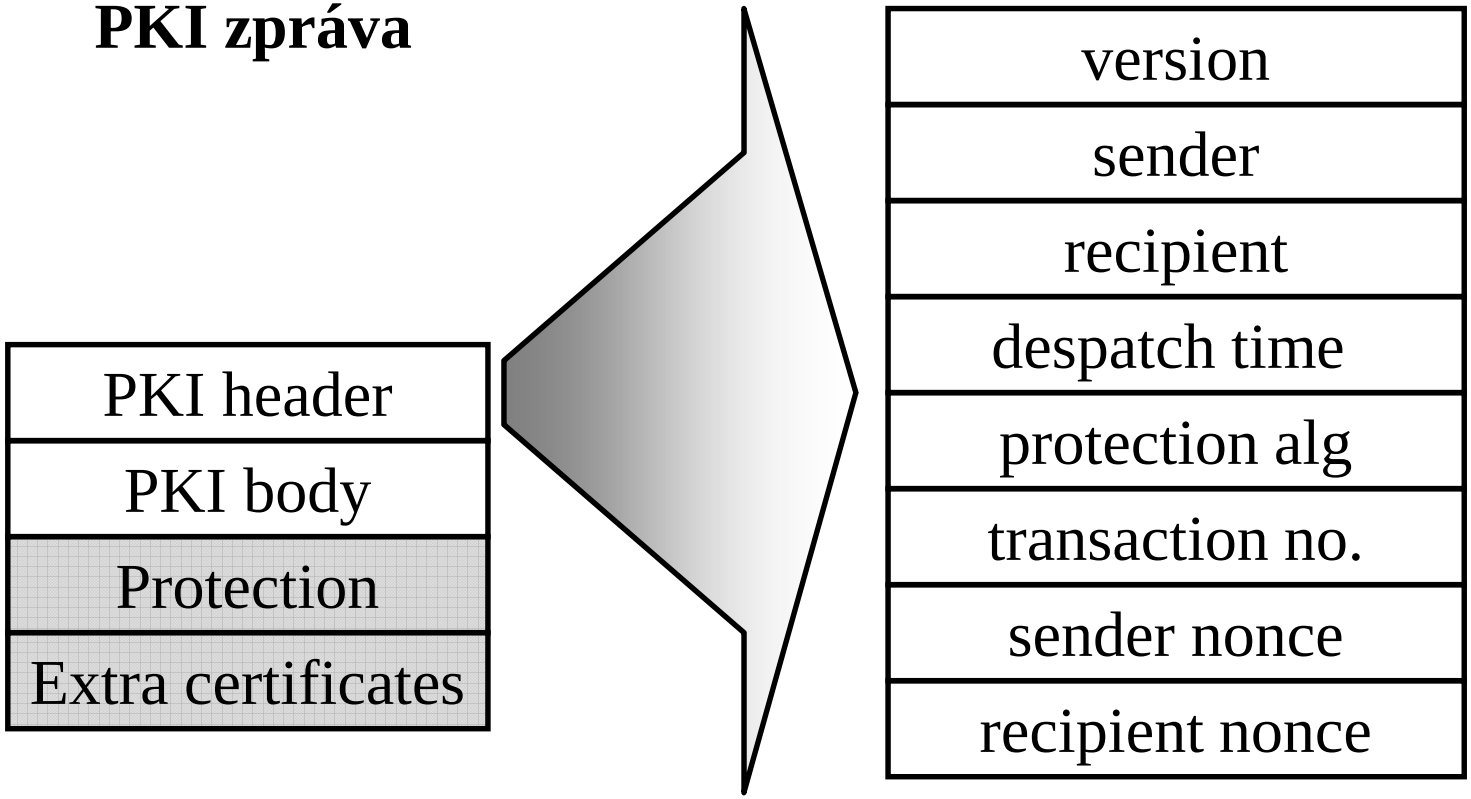


Typy certifikátů

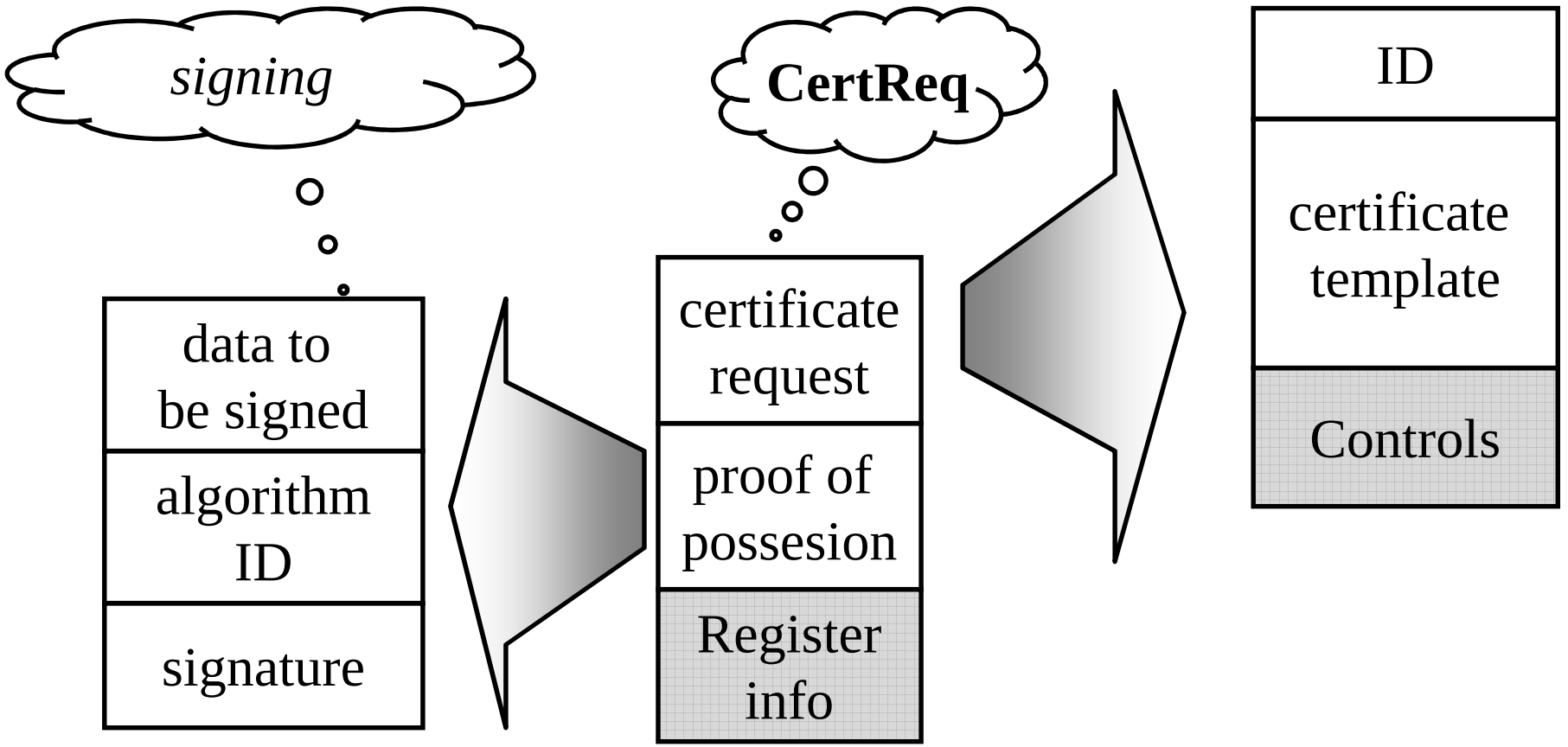
- hierarchické
  - kořenový certifikát CA
  - certifikáty pro podpisy
  - certifikáty web serverů
  - uživatelské certifikáty
- řetězce certifikátů



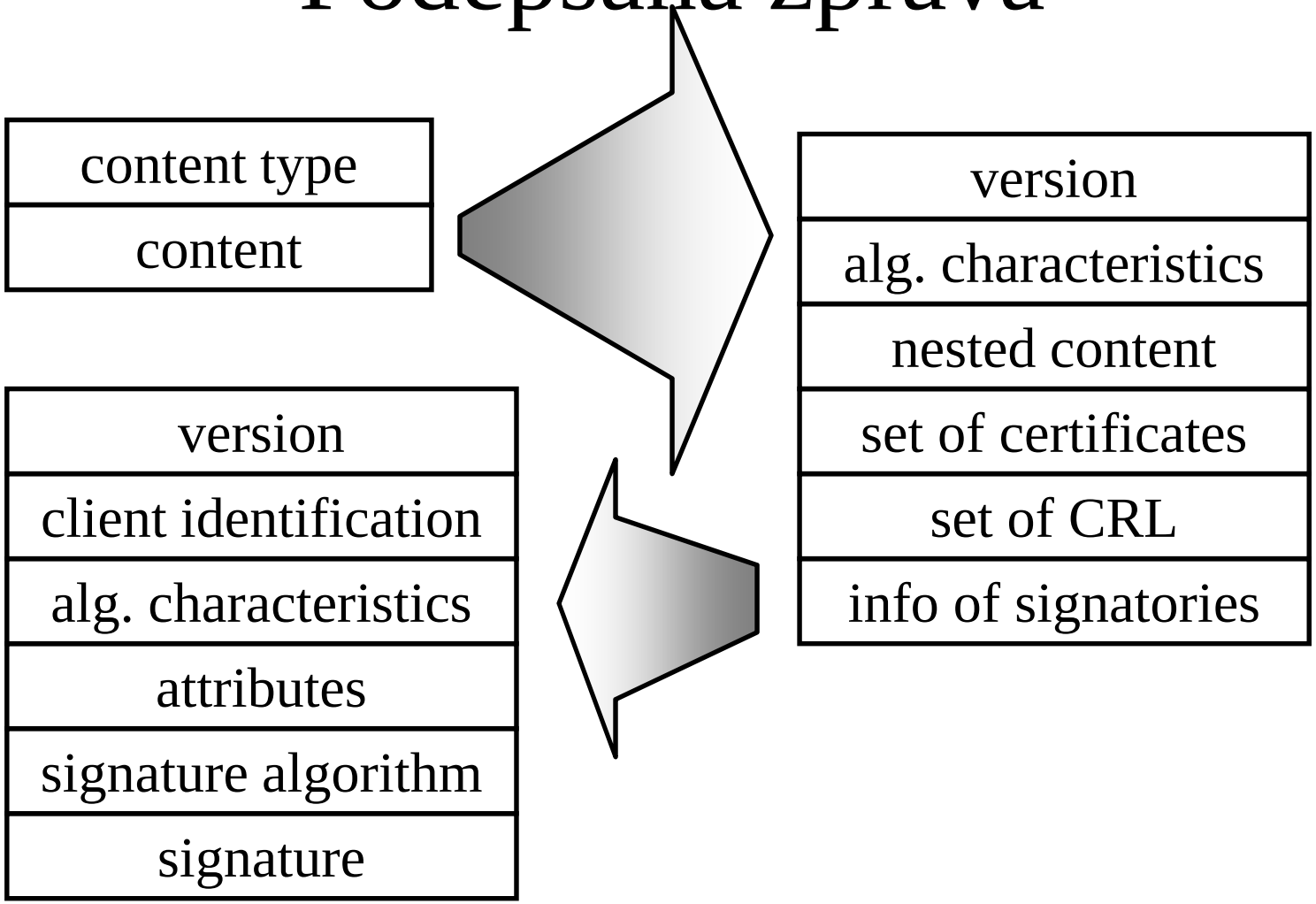
Požadavek na certifikát 1/2



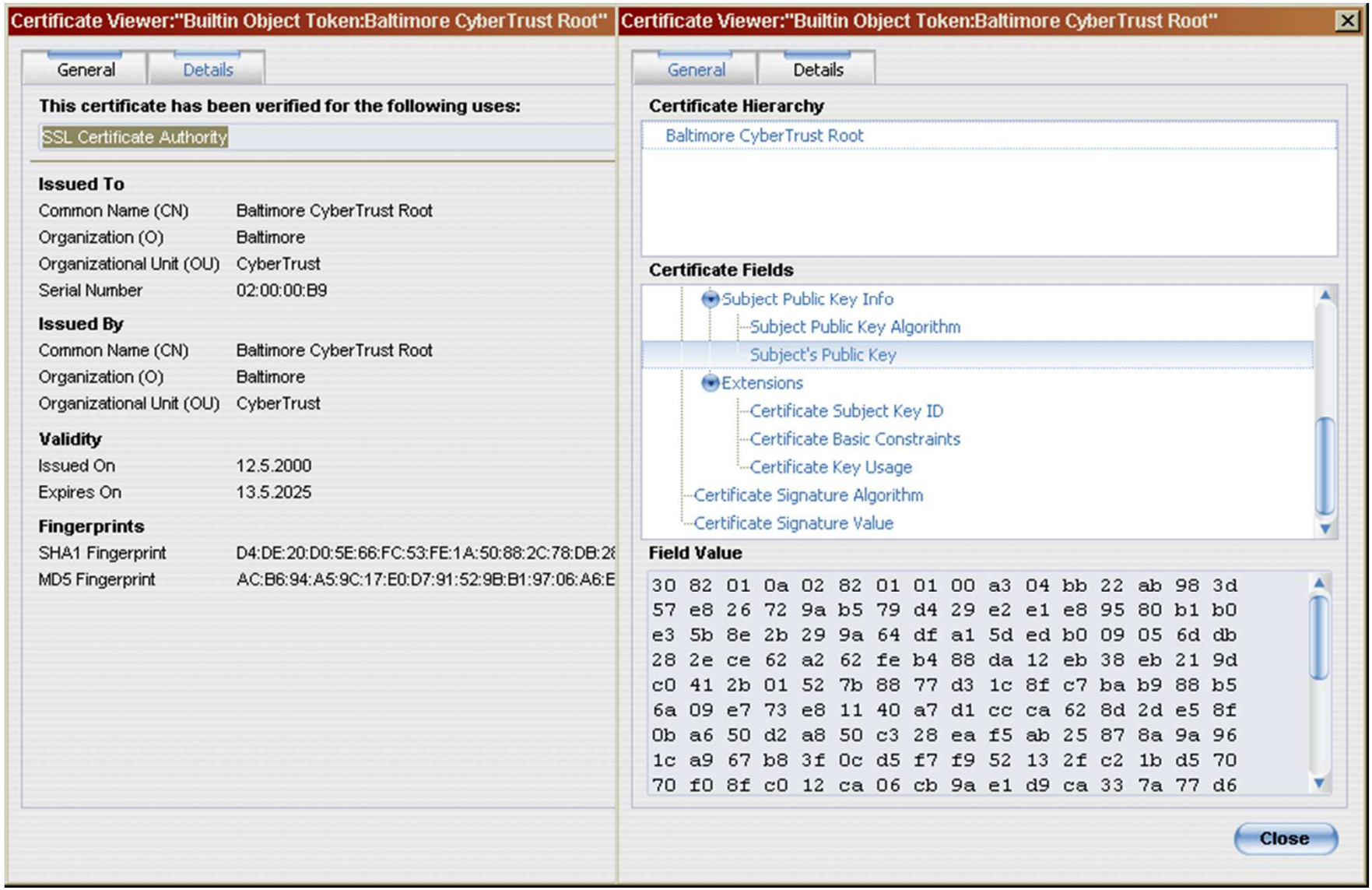
Požadavek na certifikát 2/2



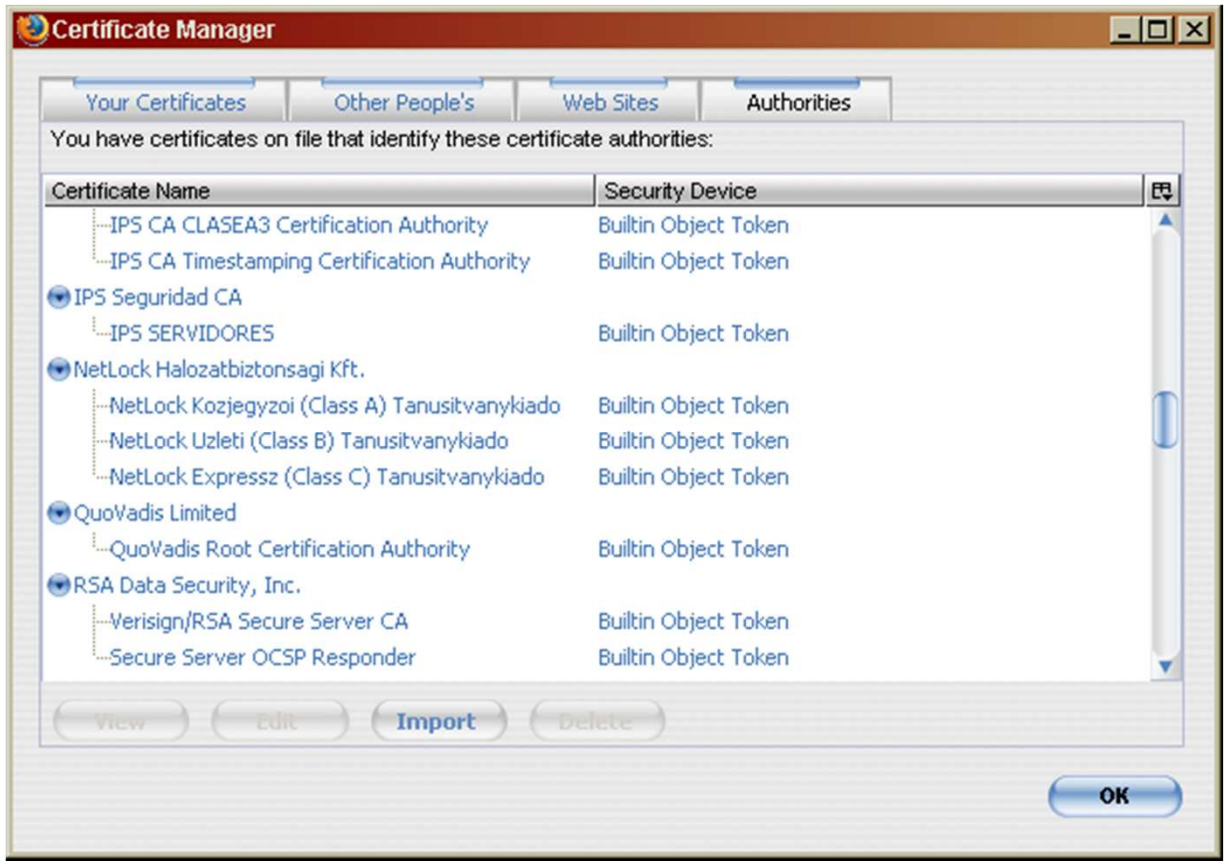
Podepsaná zpráva



… certifikát získaný ze serveru



… je v naší lokální databázi???



Platnost certifikátu

- explicitně uvedeno
  - platnost od
  - platnost do (např. 050814132432)
- certifikát lze v případě potřeby revokovat
  - sdělíme CA “certifikát je od této chvíle neplatný”
- X.509 – seznam revokovaných certifikátů - CRL

Verifikaci klíče/certifikátu

- konzervativní: klíč/certifikát je platný, pokud o tom máme dostatečný důkaz
  - potvrzení od CA v reálném čase
  - užitečné při řešení sporů, “rychlé” transakce
  - Online Certificate Status Protocol – OCSP
  - náročný na komunikaci

- liberální: klíč/certifikát je platný do doby, dokud není na seznamu revokovaných certifikátů
  - CRL – seznam revokovaných certifikátů

Problém revokace je velice důležitý!!!

X.509 problémy

- **složitost! – verifikace kódu, množství algoritmů, složitost zpráv**
- technologie
  - revokace certifikátů
    - implicitní předpoklad – certifikát je platný
    - jak detekovat prozrazení privátního klíče
    - časová prodleva po revokování certifikátu
    - časová prodleva pro publikaci nového CRLs
    - množství dat, které musí CA periodicky aktualizovat
  - bezpečná zařízení (HSM)
    - zařízení podporující krypto. funkce a verifikaci platnosti certifikátu
    - problémy vztahující se k principům, na nichž stojí PKI a X.509
- administrativa
  - využití PKI řešení je často velmi složité a s mnoha požadavky
  - procedury pro práci s klíči a dalšími citlivými údaji

X.509 problémy - registrace

- existující konflikty
  - jeden klíč CA vs. několik klíčů registračních autorit (RA)
    - bezpečnost RA není stejná jako bezpečnost CA (cena a management)
- úředník je zodpovědný za registrační proces
  - požadavky na identifikaci při registraci jsou vyšší než např. u policie
- bezpečnost RA je méně důležitá než bezpečnost CA
  - útočit na celý systém PKI je zřejmě nereálný, ale snaha o vlastnictví „cizích“ certifikátů je reálná hrozba

Věci které jsme nepokryli

- časová razítka
- archivace podepsaných dokumentů
  - z krátkodobého hlediska
  - z dlouhodobého hlediska
- právní aspekty

Případová studie

- autentizace bankovních klientů – typická autentizace 1:n (n klientů se autentizuje vůči jedné bance)
- Řešení 1
  - autentizační kalkulátor pro každého klienta umožní bezpečnou autorizaci bankovních transakcí
  - použití pouze symetrické kryptografie – jednoduché schéma snadné na implementaci
- Řešení 2
  - použití certifikátů – několik návštěv banky (běžně 2-3)
  - použití symetrické i asymetrické kryptografie
  - pouze SW implementace implikuje nižší bezpečnost autentizačního procesu

Jiný případ

- n:n nebo n:m autentizace
- neexistuje jedno centrum
  - komplikované v případě, že chceme použít symetrickou kryptografii
- PKI může pomoci
  - centrum s omezenou dostupností
  - dokončení transakce může trvat

a co soukromý klíč?

- … když ho ztratíme?
- … když je prozrazen?
- … když změníme zaměstnavatele?
- … když je uložen u nějaké třetí strany?
- … když je vyžadován soudně?
- … když …