Sieťová a komunikačná bezpečnosť

08 Správa dôvery, certifikáty

Ústav informatiky, PF UPJŠ v Košiciach

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja

OPERAČNÝ PROGRAM
ĽUDSKÉ ZDROJE

MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje

www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

certifikácia

- zabezpečenie prenosu dôvery pomocou tretích strán (PKI)
- nepopierateľnosť, zabezpečená asymetrickou kryptografiou
- identita (priradenie verejného kľúča pre asymetrickú kryptografiu), podpísaná dôveryhodnou certifikačnou autoritou
- certifikát je možné zverejniť

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

varianty použitia

- dlhodobé certifikáty
- krátkodobé certifikáty – využitie limitovaných zdrojov (grid computing) – dočasné (vydáva správca zdrojov)
- proxy certifikáty (RFC 3820) – na špeciálne účely
- atribútové certifikáty (RFC 5755) – osvedčenie atribútov entity
- časové certifikáty (časové razítka) pre notariát

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

distribúcia dôvery certifikátmi

- vytváranie dôvery na základe overených informácií
- dôveryhodná autorita potvrdí verejný kľúč subjektu digitálnym podpisom správy, obsahujúcej verejný kľúč a identitu subjektu

  $Cert_A = [EK_A, ID_A, Sig_{CA}(EK_A, ID_A)]$

  digitálny podpis zabezpečí nepopierateľnosť a umožní zistiť porušenie integrity
- certifikát – spája identitu subjektu s jeho verejným kľúčom
- bezpečná distribúcia verejných kľúčov je základ súčasnej kryptografie

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

X.509

- implementácia PKI (Public Key Infrastructure)
- RFC 5280
- formáty certifikátov
- protokoly pre vytváranie, správu a overovanie certifikátov - využitie v množstve sieťových protokolov

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
UNIVERZITA MATEJA BELA

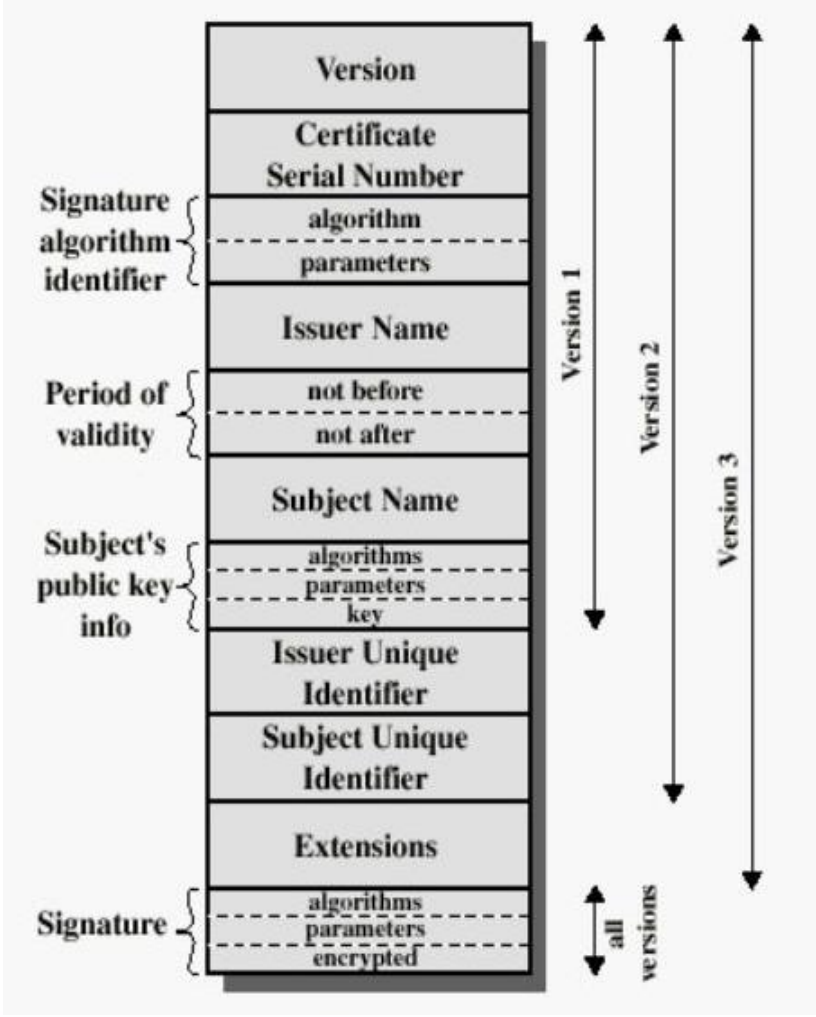
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje

www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

Certifikát X.509

poštová (ITU-T) norma pre formáty a správu verejných kľúčov PKI

- verzia – verzia formátu
- poradové (sériové) číslo (vždy iné)
- algoritmus pre hash a podpis
- vydavateľ (issuer) – meno X.501
- platnosť od – do
- predmet (držiteľ, subjekt)
- EK – algoritmus, kľúč
- podpis hašovaného obsahu



EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja

OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje

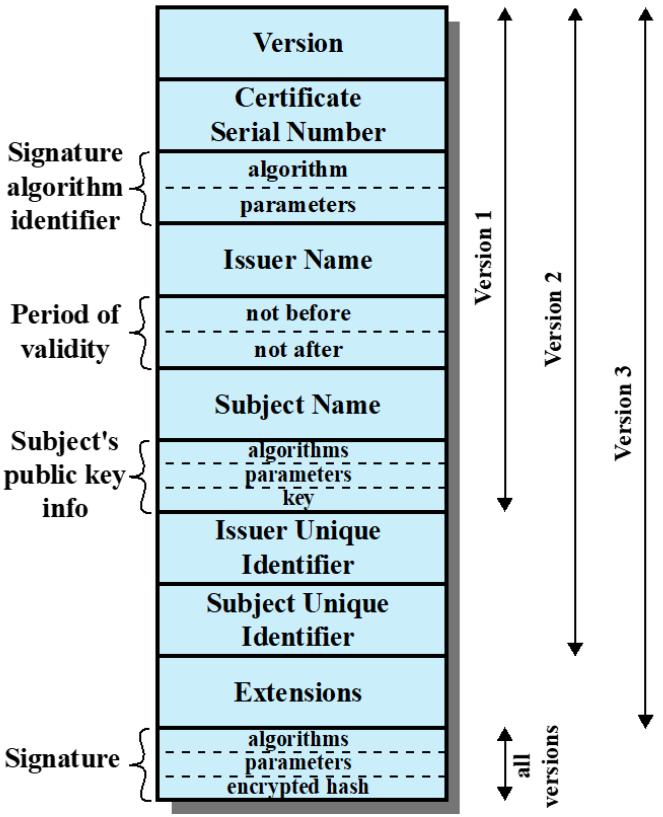
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

Certifikát X.509 - rozšírenia

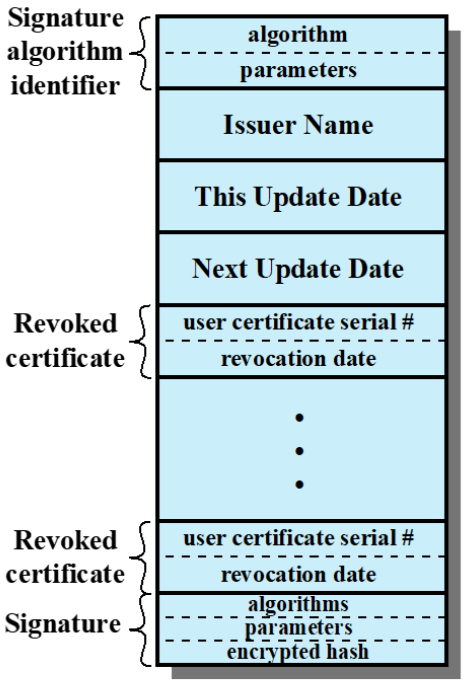
- použitie kľúča
  podpisovanie, overovanie nepopierateľnosti, šifrovanie kľúčov, šifrovanie údajov, výmena kľúčov (DH), podpisovanie certifikátov, verejný kľúč na verifikáciu zoznamu odvolaných kľúčov, DH na šifrovanie, DH na dešifrovanie ...
  na nič iné sa kľúč nesmie použiť !
- alternatívne meno – DNS, IP, URI, X.400 (el. pošta)
- certifikačné politiky a zásady
- miesto zoznamu odvolaných certifikátov
- biometrické informácie

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

X.509 formát



(a) X.509 Certificate



(b) Certificate Revocation List

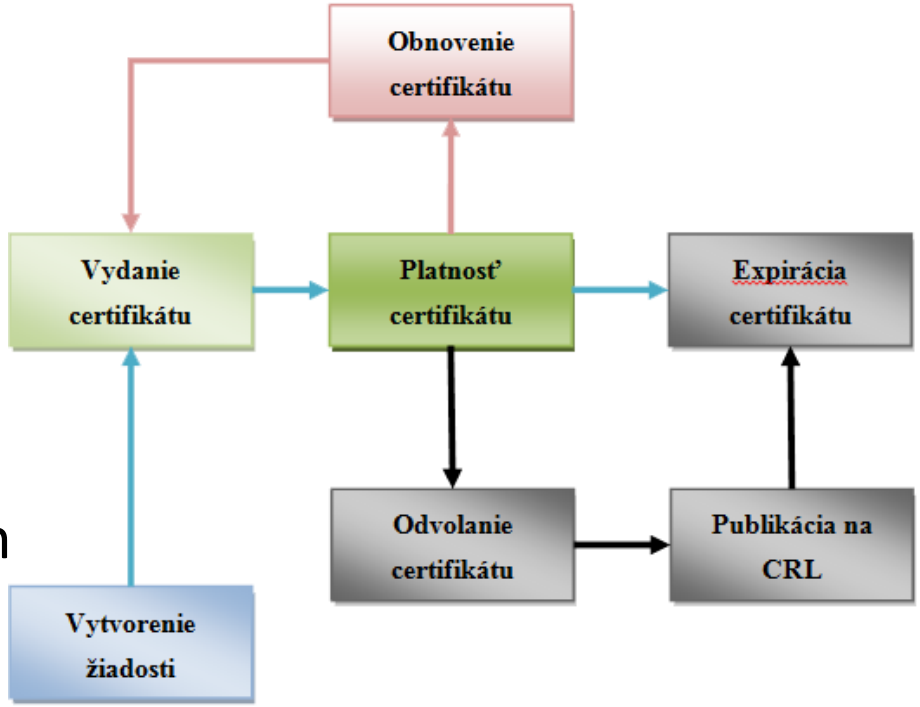
EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
UNIVERZITA MATEJA BELA

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje

www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

certifikát X.509 – životný cyklus

- žiadosť a registrácia (registračná autorita)
- vydanie certifikátu
- platnosť – obnovenie (renew, rekey), vypršanie platnosti, odvolanie (revokácia) CRL – zoznam odvolaných certifikátov
- archivácia



EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

OCSP
Online Certificate Status Protocol

žiadosť a odpoveď OCSP servera na platnosť certifikátu

môže prevádzkovať CA (odpoveď s jej podpisom)

žiadosť – sériové čísla, h(CAname), h(VK CA)

podpis žiadateľa(nie je nutný) + algoritmus, certifikát

odpoveď – ne/platnosť resp. id chyby (odmietnutie)

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

certifikačná autorita

certifikáty udeľuje dôveryhodná Certifikačná autorita

registrácia - identifikácia subjektu

- pre už vytvorené kľúče ID_A , EK_A -> $[EK_A, ID_A, Sig_{CA}(EK_A, ID_A)]$
  CA overí identitu, podpíše certifikát a poskytne svoj verejný kľúč E_{CA}
  (prípadne certifikáty, dokazujúce jeho vlastníctvo)
- ak je problém s doručením (ID_A, EK_A), vytvorí CA kľúče EK_A DK_A
  a spolu s certifikátom pošle subjektu zabezpečeným kanálom

certifikát verejného kľúča CA podpisuje iná CA - vzniká tak reťazec dôvery (chain of trust)

koreňový certifikát – certifikát CA, ktorý si CA podpisuje sama
(dôvera sa musí získať inou cestou – legálnou distribúciou sw, verejne dobre prístupným uložením, osobnou návštevou)

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

certifikačná cesta, overenie certifikátu

certifikát subjektu A a certifikát jeho CA

- $Cert_A$ [vydávateľ] = $Cert_{CA}$ [Predmet]
  $Cert_A$ [authority key ID] = $Cert_{CA}$ [subject key ID]
- platnosť $Cert_A$ a $Cert_{CA}$, overenie odvolania (CRL)
- použiteľnosť, certifikačná politika
- overenie podpisu $h(Cert_A) =? E_{CA}(Cert_A[signature])$

pokiaľ nedôverujem certifikátu CA, potrebujem certifikát (EK) CA2, ktorá vydala certifikát pre CA -> overím $Cert_{CA}$ a $Cert_{CA2}$

reťazovite až po koreňovú (root) CA (podpisuje certifikát sama), možno len skontrolovať správnosť výpočtu

ak subjekt nie je v mojej reťazi, nájdem posledný spoločný uzol a overujem ho až po CA subjektu

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
UNIVERZITA MATEJA BELA V BANSKEJ BYSTRICI
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

žiadosť RA o certifikát

- PKCS#10 (RFC-2314)
  verzia, subject
  subjectPublicKeyInfo – algoritmus a VK žiadateľa
  attributes – jednorazové heslo na odvolanie ...
  podpis súkromným kľúčom subjektu
- CRMF (Certificate Request Massage Format)
  parametre certifikátu (možnosť nechať CA generovať kľúče)
  dôkaz vlastníctva – pre podpisovací kľúč – podpis žiadosti,
  pre šifrovací kľúč – certifikát CA zašifruje VK subjektu, RA
  možnosť poslať SK subjektu zašifrovaný VK CA
  atribúty – jednorazové heslo na vydanie certifikátu, na jeho odvolanie
  spôsob vystavovania, kontakty na žiadateľa, účtovné informácie ...

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

CMP
Certificate Management Protocol

vydávanie a správa certifikátov v PKI

- záhlavie – verzia, sender, recipient, time, alg. ochrany, id key sender, id key recipietn, id transakcie, sender nonce, recipient nonce (proti replay attack)
- telo – žiadosť o certifikát (CRMF), odpoveď, žiadosť o obnovenie certifikátu, žiadosť o obnovenie kľúčov, žiadosť o odvolanie kľúčov, žiadosť o odvolanie certifikátu, vydanie nového certifikátu, ponuka CRL ...
- ochrana – MAC s dohodnutým kľúčom, MAC s DH zo súkromnej časti žiadosti o DH certifikát, podpis pri žiadosti o kľúč k el. podpisu
- ďalšie certifikáty (CA ...)

môže byť použitý samostatne 829/tcp (RFC-2510)
elektronickou poštou typu pkicxmp v DER formáte a base64
HTTP protokolom

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
UNIVERZITA MATEJA BELA V BANSKEJ BYSTRICI
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

CMS – Cryptographic Message Standard

- PKCS#7 (RFC-2315) + rozšírenie RFC-2630 CMS bezpečný prenos dát pomocou PKI

Data – nezabezpečené údaje

Signed Data – algoritmy pre MAC, vstupné údaje, certifikáty, CRL, podpisy
podpis – id certifikátu pre podpis, alg. MAC a podpis, atribúty (čas ..)
napr. pre POP3, export certifikátu ...

Enveloped Data – dáta v elektronickej obálke – zašifrované náhodným symetrickým kľúčom, pripojeným k správe šifrovaným VK adresáta

Digest Data – správa s kontrolným súčtom (MDC)

Encrypted Data – šifrované neznámym kľúčom

Authenticated Data – správa autentifikovaná MAC

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
UNIVERZITA MATEJA BELA V BANSKEJ BYSTRICI
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

ďalšie riadiace protokoly PKI

- CMC – Certificate Management Messages over CMS
  - ako CMP, zabezpečené protokolom CMS
  - štruktúra PKIData do obálky CMS

DVCSP – Data Validation and Certification Server Protocols RFC-3029

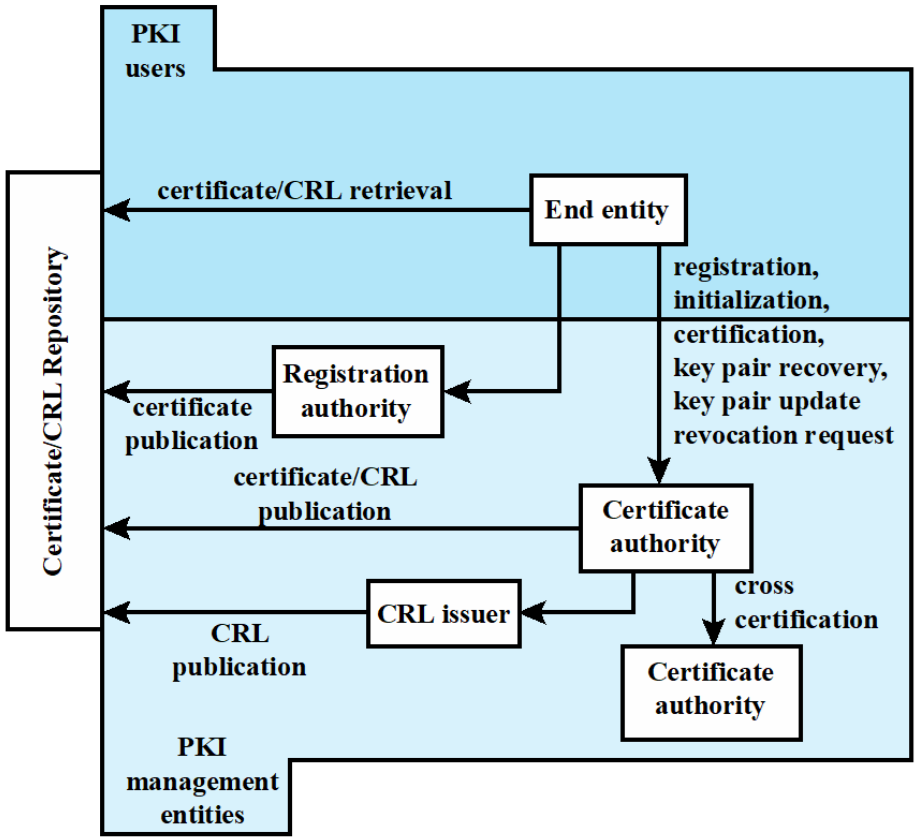
- využívajú DVCS servery na overenie certifikátu

TSP – Time Stamp Protocol - žiadosť o časovú pečiatku

- na TSA (Time Stamping Authority)
- hash, id hash alg., nonce – TSA vráti hash + čas. pečiatku

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

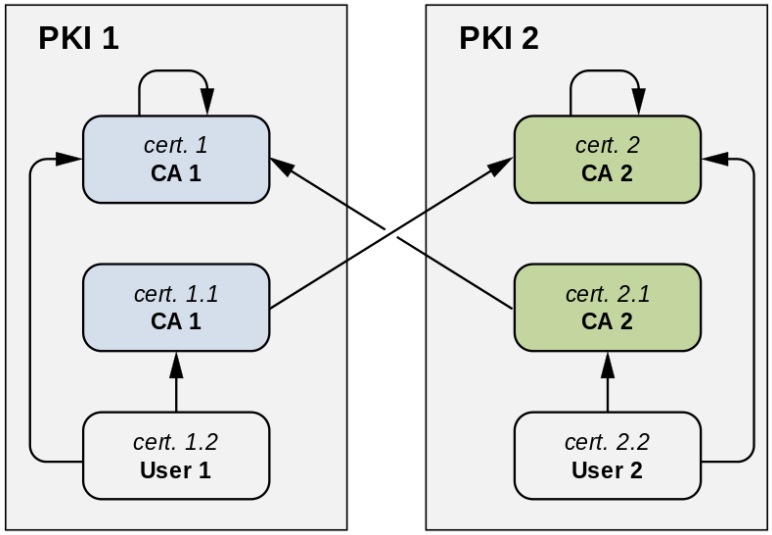
architektúra PKIX



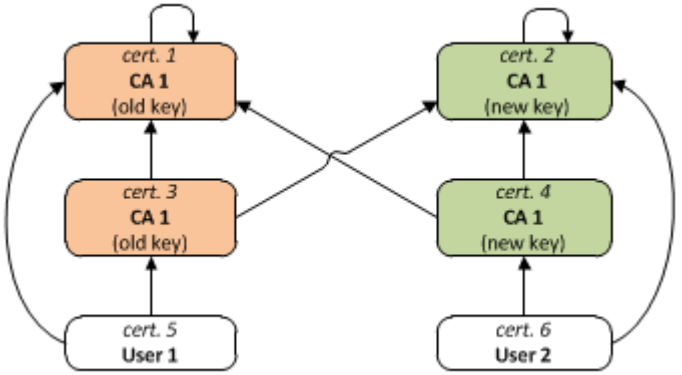
EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
UNIVERZITA MATEJA BELA
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje
www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

PKIX management

- protokoly CMP, CMC



krížová certifikácia



obnovenie kľúča

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
UNIVERZITA MATEJA BELA

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje

www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

Literatúra

L. Dostálek a kol.: Velký průvodce protokoly TCP/IP – Bezpečnost, kap. 8, 9

W. Stallings, L. Brown : Computer Security (Principle and Practice), 4. ed., Pearson 2018, ISBN 978-1-292-22061-1, chapter 23

D. Gollmann : Computer Security, 3. ed., Wiley 2011, ISBN 978-0-470-74115-3, chapter 15

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja

OPERAČNÝ PROGRAM
ĽUDSKÉ ZDROJE

MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje

www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk