# KRYPTOGRAFICKÉ KĽÚČE DISTRIBÚCIA A DÔVERYHODNOSŤ

**Martin Rublík, PhD., CISSP**
martin.rublik@gmail.com

OWASP - Slovakia

# Program

- Prezentácia bude orientovaná na X.509 certifikáty
- Úvod do infraštruktúry verejných kľúčov
  - Ako nás (ne)chráni kryptografia a pred čím
  - Čo by mala PKI riešiť, aké typy PKI poznáme
  - Základné pojmy PKI postavenej na X.509 certifikátoch (model komunikácie, certifikát, CRL, CA, RA, OCSP, CP, CPS)
  - Ako rieši(?) PKI problém distribúcie a dôveryhodnosti kryptografických kľúčov
- Problémy súčasného modelu vzťahu dôvery založeného na X.509 certifikátoch
  - SSL Observatory
  - Dôveryhodnosť a bezpečnosť certifikačných a registračných autorít
  - Softvér (prehliadače): validačné problémy, UI problémy
- Long-term riešenia
  - DANE + DNSSEC
- Short-term alternatívy
  - Certificate Patrol
  - Network notary / Perspectives
- Záver

# Úvod do PKI

# Pred čím nás (ne)chráni kryptografia?

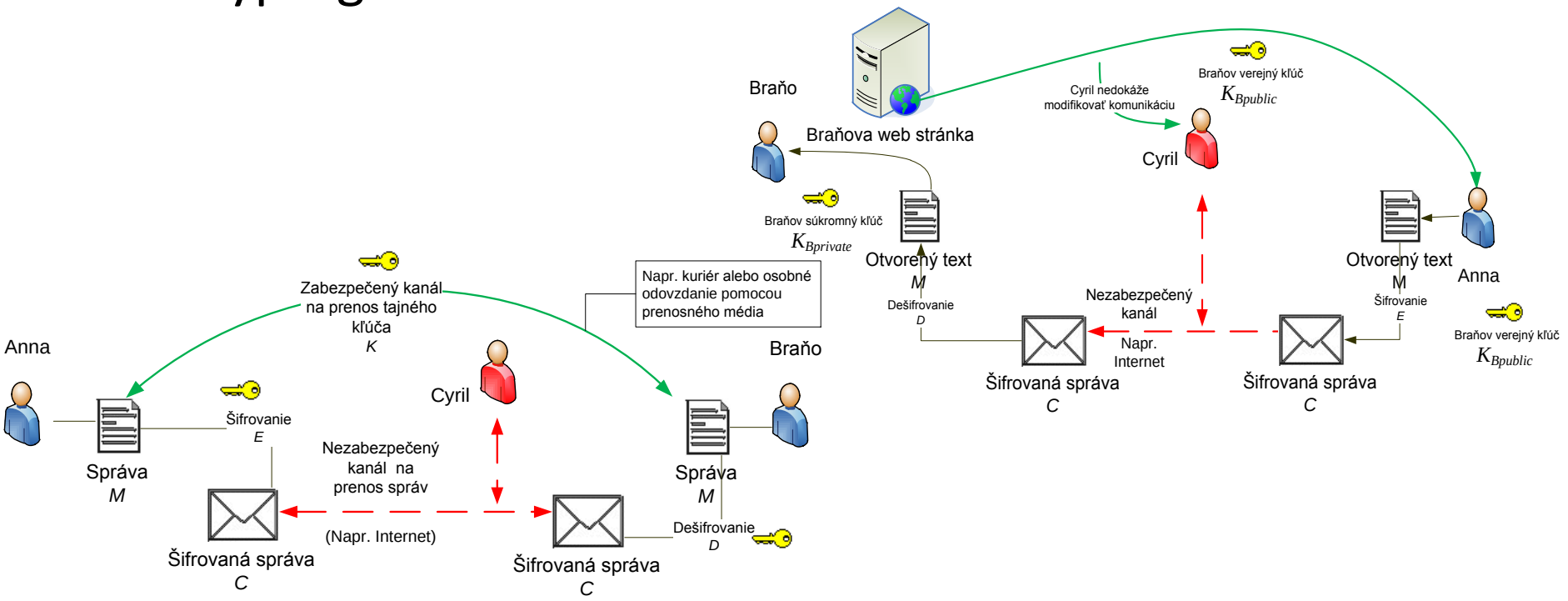
- Najčastejšie využitie v praxi
  - **Šifrovanie komunikácie a overenie identity servera (SSL/TLS)**
  - Ochrana používateľských hesiel a citlivých informácií
  - Ochrana záloh
- Menej časté využitie v praxi
  - Prihlasovanie do aplikácií, dvojfaktorová autentifikácia založená na certifikátoch verejného kľúča
  - Šifrovanie databáz
    - Transparentné šifrovanie celej databázy
    - Šifrovanie časti údajov v databáze
- Kryptografia nezníži riziko zneužitia
  - Chýb v aplikáciách a aplikačnom vybavení (aplikácia, framework, web server, operačný systém)
  - Útokov na strane klienta / malware (man-in-the-browser)
- Scenáre použitia
  - Ochrana pred odpočúvaním a modifikáciou komunikácie na sieťovej úrovni napr. pomocou SSL/TLS alebo IPSec (otvorené Wi-Fi siete, rogue DHCP, DNS cache poisoning, ARP cache poisoning, ...)
  - Ochrana pri kompromitácii aplikácie (najmä šifrované heslá)
  - Ochrana záloh

# Slabé miesta kryptografickej ochrany

- Vlastné kryptografické algoritmy a protokoly
  - Schneier's Law: Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can't break.
  - Príklady:
    - DVD CSS, A5/1
- Chybné použitie/implementácia kryptografických algoritmov
  - Kryptológia je zložitá na pochopenie (vyžaduje matematický aparát, ktorý väčšina programátorov nemá) a aj malá chyba obyčajne znamená katastrofické následky
  - Príklady:
    - RC4/WEP, Office RC4, ASP.NET Padding Oracle, OpenSSL Debian fiasco
- **Zlá/zložitá distribúcia a správa kryptografických kľúčov**
  - Najjednoduchšia cesta ako prelomiť kryptografickú ochranu je získať kľúče alebo presvedčiť obeť o tom, že kľúče, ktoré útočník podvrhol, sú autentické

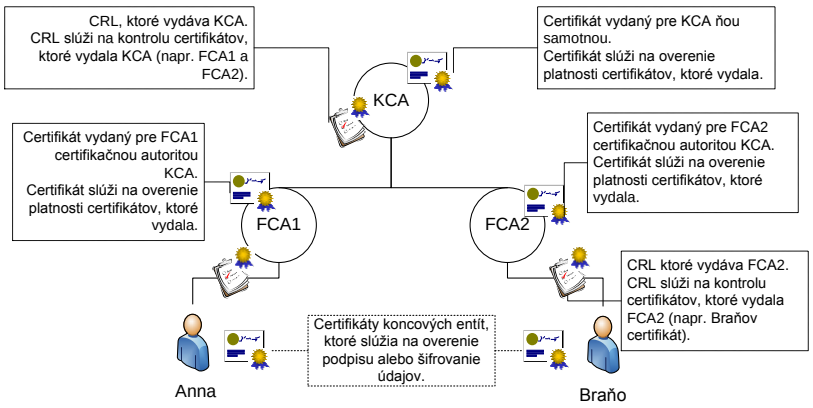
# Kryptografia a kryptografické kľúče

- Problém distribúcie kľúčov
- Problém autenticity / platnosti kryptografických kľúčov
- Problém zviazanosti identity subjektu a kryptografického kľúča

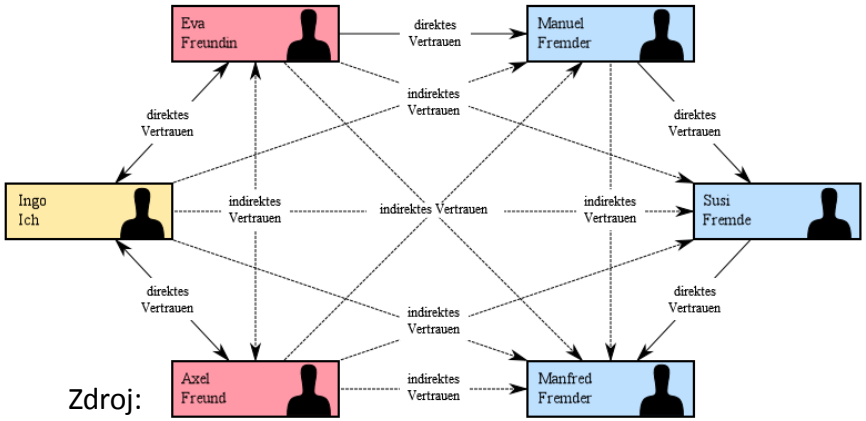


# Infraštruktúra verejných kľúčov

- **Centralizovaná infraštruktúra**
  - Centrálna autorita zabezpečuje správu verejných kľúčov (pomocou certifikátov, ktoré podpisuje)
  - Distribúcia kľúčov veľkého množstva koncových entít sa redukuje na distribúciu kľúčov malého množstva certifikačných autorít
  - Dôveryhodnosť prepojenia kľúčov a identity ich držiteľa určuje autorita
  - Platnosť certifikátov býva časovo obmedzená
  - Platnosť kľúčov sa overuje na základe periodicky publikovaných blacklistov
- Príklady
  - X.509, XrML
- Využitie
  - Bezpečný mail, TLS/SSL, 802.1X, IPSec, podpisovanie spustiteľného kódu,




- **Decentralizovaná infraštruktúra**
  - Správa kľúčov nie je riadená centrálne, každá entita vydáva svoj vlastný certifikát, ktorý neskôr môže byť podpísaný ďalším účastníkom infraštruktúry
  - Distribúcia kľúčov je riadená na základe vzťahov medzi účastníkmi infraštruktúry
  - Dôveryhodnosť prepojenia kľúčov a identity ich držiteľa určuje tranzitívny vzťah dôvery
  - Platnosť certifikátov nemusí byť časovo obmedzená
  - Ďalšia platnosť kľúčov sa prakticky neoveruje
- Príklady
  - PGP Web of Trust
- Využitie
  - Bezpečný mail, distribúcia softvéru

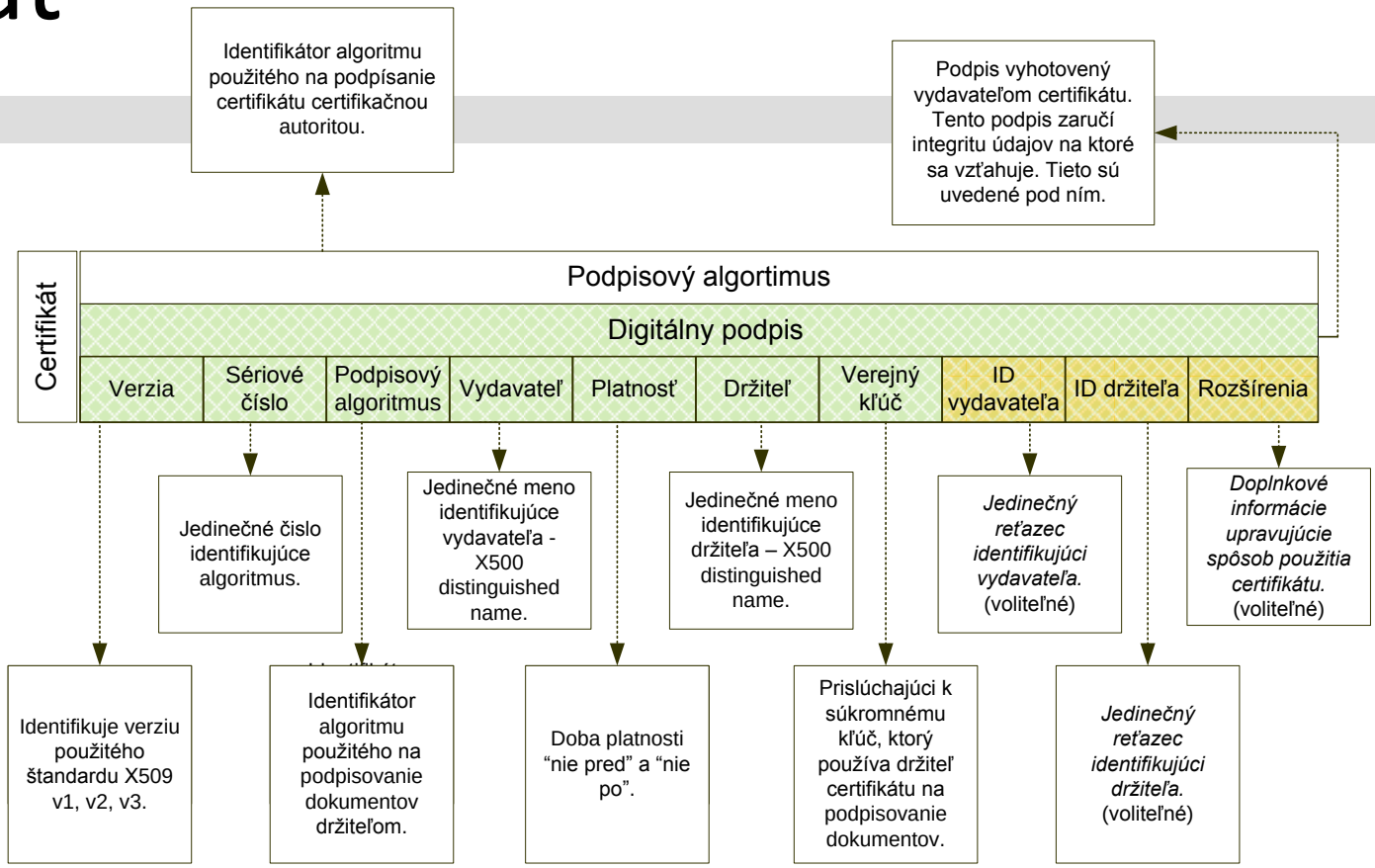



Zdroj: http://commons.wikimedia.org/wiki/File:Web_of_Trust.svg

# Certifikát

Obsahuje najmä informácie o:

- vlastníkovi certifikátu
- verejnom kľúči vlastníka certifikátu
- vydavateľovi certifikátu (certifikačnej autorite)
- dobe platnosti certifikátu
- povolenom spôsobe využitia kryptografických kľúčov



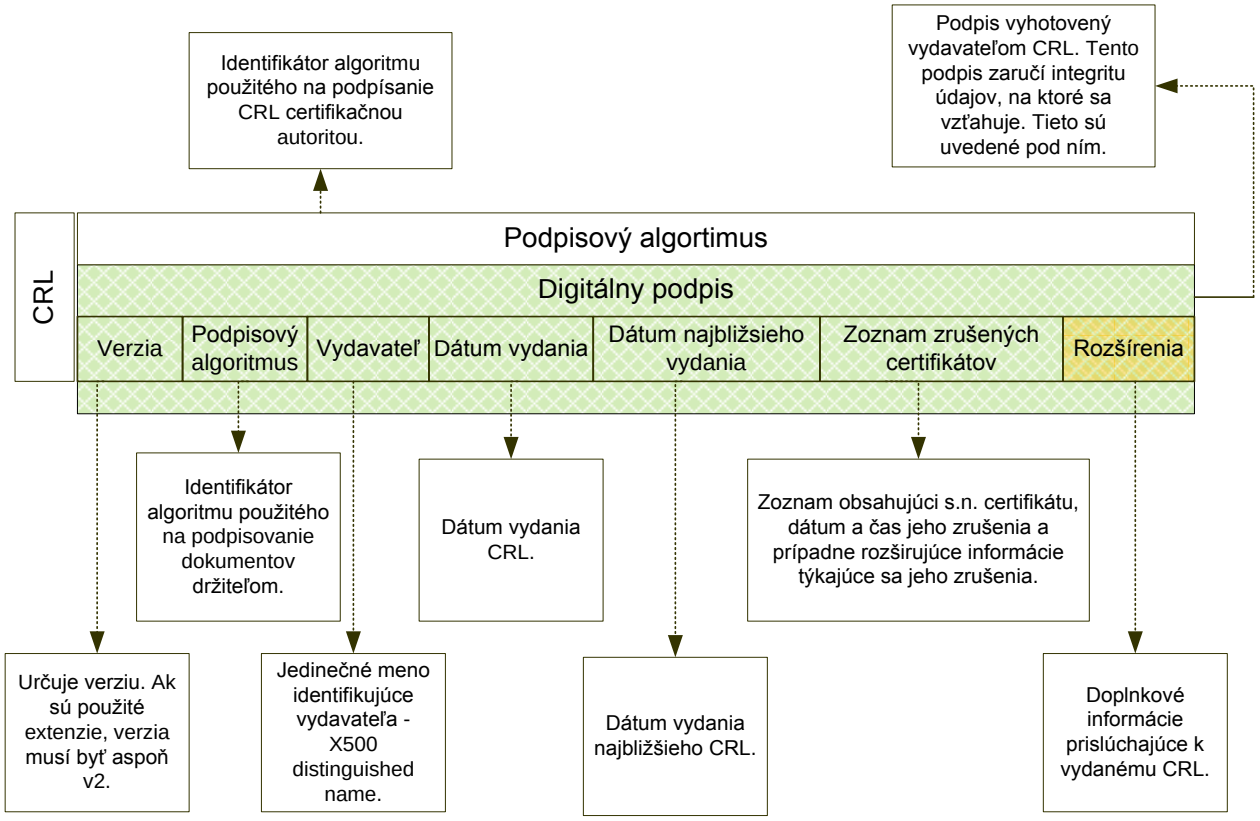
# Zoznam zrušených certifikátov (certificate revocation list CRL)

Vo vybraných prípadoch je nevyhnutné predčasne ukončiť platnosť certifikátu, medzi tieto môžeme zaradiť najmä prípady keď:

- certifikát nebol vydaný v súlade s pravidlami, ktoré stanovuje certifikačná autorita,
- údaje, ktoré boli uvedené pri vydávaní certifikátu, sa ukázali ako nepravdivé, alebo sa časom zmenili,
- vlastník certifikátu explicitne požiada o jeho zrušenie, napr. z dôvodu zmeny údajov uvedených na certifikáte, alebo z dôvodu kompromitácie jeho súkromného kľúča

Obsahuje najmä informácie o:

- mene vydavateľa (CA)
- dátume a čase vydania CRL
- dátume a čase vydania najbližšieho plánovaného CRL
- samotný zoznam zrušených certifikátov (sériové číslo certifikátu + dôvod jeho zrušenia)



# Certifikačná autorita (CA)

- Synonymá z praxe notár, vydavateľ preukazov, ...
- **Dôveryhodná** tretia strana, ktorá zabezpečuje
  - Certifikačné služby, najmä vydávanie, zverejňovanie a rušenie platnosti certifikátov, vydávanie CRL či podmienená obnova šifrovacích kľúčov
  - **Overenie identity koncových entít a vlastníctva asymetrických kľúčov**
- Aby vedela CA preukázať svoju dôveryhodnosť publikuje prevádzkovú (predovšetkým procesnú) dokumentáciu, najmä:
  - Certifikačný poriadok
  - Pravidlá na výkon certifikačných činností
  - Bezpečnostnú politiku
- Okrem publikovanej dokumentácie môže CA viesť aj dokumentáciu ktorá nie je verejná

# Certifikačný poriadok (Cerificate Policy – CP)

- CP je množina pravidiel, ktorá naznačuje či je certifikát použiteľný v rámci určitej komunity na vybrané účely (*ISO/IEC 9594-8:2005 Recommendation X.509*)
- CP slúži najmä koncovým entitám pri rozhodovaní do akej miery dôverujú certifikátom vydávaným príslušnou CA
- V rámci CP sú definované najmä:
  - **pre koho a za akých podmienok sú určené certifikačné služby**
  - práva a povinnosti používateľov certifikačných služieb
  - aké sú obmedzenia pri poskytovaní certifikačných služieb
  - **typy certifikátov vydávaných certifikačnou autoritou**
  - pravidlá používania a rušenia platnosti certifikátov a s nimi spojené procedúry
  - **procedúry pri overovaní identity žiadateľa o certifikát a pri overovaní vlastníctva kryptografických kľúčov**
  - spôsob a rozsah zverejnenia informácií súvisiacich s certifikačnými službami (adresa certifikačnej autority, certifikáty certifikačnej autority, zoznamy zrušených certifikátov a iné)
  - **fyzické, personálne a procedurálne opatrenia, ktoré zabezpečujú korektné poskytovanie certifikačných služieb**
  - spôsob spracovania (osobných) údajov a spôsob ich ochrany
  - ostatné organizačné a právne ustanovenia (napr. poplatky, finančná zodpovednosť a **poskytované záruky certifikačnej / registračnej autority**)

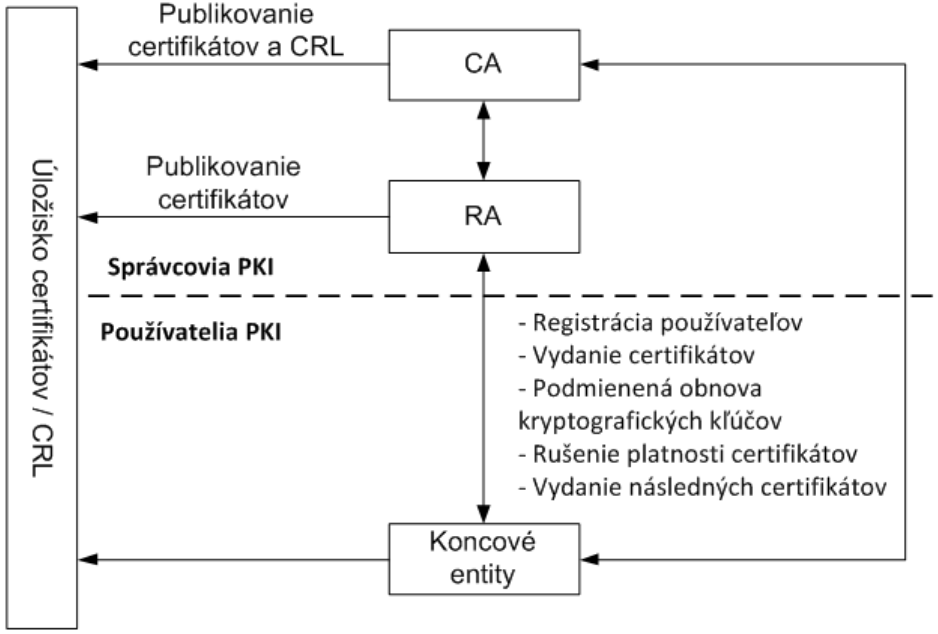
# Pravidlá na výkon certifikačných činností (Certificate Practice Statement – CPS)

- CPS predstavujú dokument podľa ktorého sa CA riadi pri vydávaní certifikátov (*ISO/IEC 9594-8:2005 Recommendation X.509*)
- CPS sú detailnejší dokument ako CP pričom opisujú akým spôsobom sú realizované opatrenia týkajúce záruk, ktoré sa zaviazala CA zabezpečiť v rámci CP a bezpečnosti certifikačných služieb vo všeobecnosti
- Vzhľadom na skutočnosť, že CPS môže obsahovať citlivé informácie, CA sa môže rozhodnúť že tento dokument nezverejní. Musí však byť prístupný v rámci auditu.

# Registračná autorita (RA)

- RA slúži na sprostredkovanie kontaktu medzi certifikačnou autoritou a (potenciálnymi) držiteľmi certifikátov
- RA je „pobočka“ certifikačnej autority, kde sa vybavujú formality spojené s registráciou, obnovovaním a revokovaním certifikátov
- RA môže sprostredkúvať napr. nasledovné činnosti:
  - prijímanie žiadosti o vydanie certifikátu
  - overenie totožnosti používateľa
  - overenie vlastníctva kryptografických kľúčov
  - odovzdanie vygenerovaných certifikátov, prípade zariadení ktoré ich uschovávajú (napr. čipové karty alebo USB tokeny)
  - prijímanie žiadostí o zrušenie certifikátu
  - komunikácia s príslušnou certifikačnou autoritou
  - podpora koncových používateľov (hotline / helpdesk)

# Komunikačný model CA, RA, koncové entity




Zdroj: http://tools.ietf.org/html/draft-ietf-pkix-roadmap-09#page-9

# Ako sa teda riešia základné problémy distribúcie/správy verejných kľúčov

- Distribúcia
  - Redukcia problému na distribúciu malého množstva CA
  - Certifikáty dôveryhodných (aj nedôveryhodných) CA sú pripojené k softvéru
  - Distribuujú sa len koreňové CA, podriadené CA možno získať:
    - v rámci SSL/TLS protokolu (posiela sa chain, pričom certifikát koreňovej CA je voliteľný)
    - v rámci procesu budovania reťaze dôvery (reťaz certifikátov CA)
- Dôveryhodnosť a autenticita
  - Požiadavky tvorcov softvéru, ktorý distribuuje certifikáty CA
  - Spôsob verifikácie identity držiteľa certifikátu
  - Platnosť certifikátu
    - CRL
    - OCSP
- Prepojenie identity
  - Validácia pomocou „oficiálnych“ dokumentov a zdrojov informácií tretích strán (obchodné registre, registrátori domén, telekomunikační operátori, ...)
  - Face-2-face overenie identity (v prípade kvalifikovaných certifikátov na overenie zaručeného elektronického podpisu)

# Distribúcia kľúčov/certifikátov CA (MS Windows)

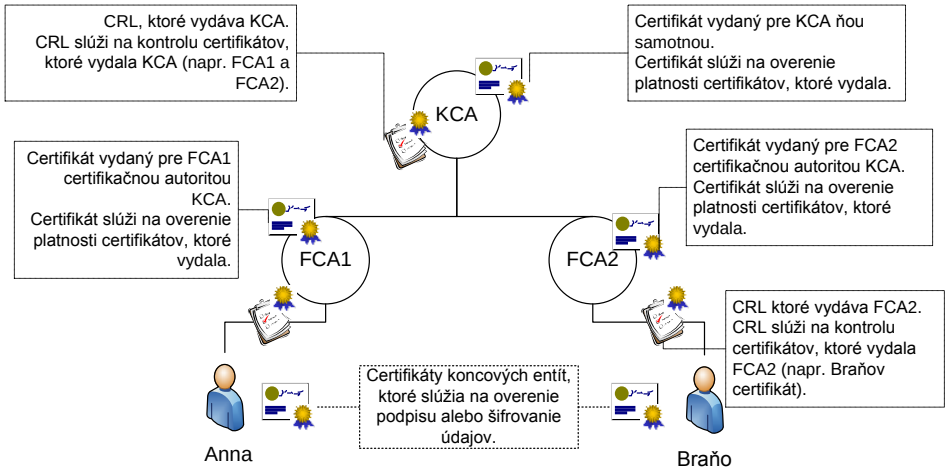
- Certifikáty dôveryhodných CA sa distribuujú spolu s operačným systémom
- Microsoft Windows Root Certificate Program
  - Spoločné úložisko certifikátov (store) pre všetky aplikácie čo využívajú MS CryptoAPI/CNG na kryptorgrafické operácie (napr. IE, Outlook, VPN klient, Smart-Card logon, ...)
- Vybrané podmienky začlenenia
  - Technické podmienky (verzia v3 X.509, zmysluplné meno, veľkosť a použiteľnosť kľúčov, hash algoritmus, a pod.)
  - Bezpečnostné podmienky
    - viac faktorová autentizácia pre operátorov CA/RA,
    - Zverejnené CP/CPS
    - ročný audit podľa (WebTrust, ETSI TS 101 456, ETSI TS 102 042, ISO 21188:2006) vrátane podriadených CA
  - Všeobecné (obchodné) požiadavky
    - Podpísanie zmluvy s MS
    - Obmedzenie využitia kľúča na ochranu elektronickej pošty, server autentifikáciu, klient autentifikáciu a pod.
    - Súčasťou programu nesmú byť koreňové CA, ktoré vydávajú certifikáty v uzavretom (enterprise) prostredí. CA v programe však môžu vydávať certifikáty iným CA ktoré pôsobia v uzavretom (enterprise) prostredí
    - Účasť v programe nepodlieha správnym poplatkom
- CA možno odstrániť s výnimkou 3 CA ktoré sú nevyhnutné pre správnu funkcionalitu OS

# Distribúcia kľúčov/certifikátov CA (ďalšie aplikácie)

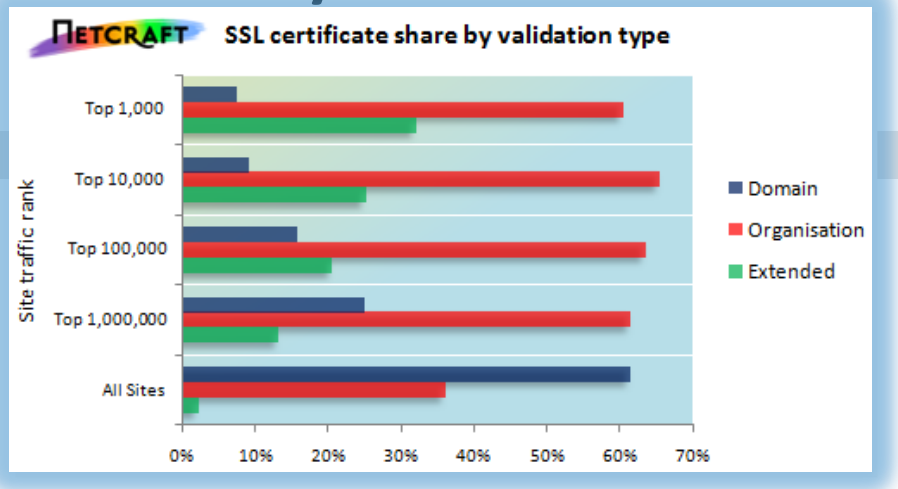
- Mozilla {Firefox, Thunderbird, ...}
  - Certifikáty dôveryhodných CA sa distribuujú spolu s aplikáciou (v rámci NSS)
  - Vybrané podmienky začlenenia
    - Obdobné podmienky ako v prípade MS
    - Podmienky sú momentálne v procese aktualizácie a konsolidácie
- Chrome
  - MS/Apple využíva systémový store
  - Linux Mozilla NSS store
- Opera
  - Vlastný store
  - Podmienky začlenenia
- Certifikáty CA možno odstrániť, odporúča sa však ich presunúť medzi nedôveryhodné

# Platnosť certifikátov

- Reťaz certifikátov sa buduje na základe
  - Certifikátov dôveryhodných CA
  - AKI / SKI extenzií v certifikátoch (meno CA, hash kľúča CA)
  - Extenzie AIA
- Podmienky
  - certifikačná autorita ktorá certifikát vydala je dôveryhodná
  - podpis CA na certifikáte je platný
  - doba platnosti certifikátu nevypršala
  - žiaden z certifikátov potrebných v rámci procesu overenia platnosti nie je na zozname zrušených certifikátov (resp. odpoveď OCSP servera je *„good“*)
    - adresa zoznamu zrušených certifikátov je určená extenziou certifikátu (CDP)
    - adresa OCSP je rovnako určená extenziou certifikátu (AIA)
  - aplikácia dokáže rozpoznať kritické extenzie certifikátu a tieto sú v súlade s predpokladaným využitím certifikátu resp. príslušného súkromného kľúča



# Spôsoby prepojenia identity a verejného kľúča




- SSL/TLS certifikáty
  - Domain validated (DV)
    - Kontrola na základe
      - WHOIS
      - E-Mail
    - Certifikát obsahuje „len“ validované DNS meno
  - Organization validated (OV)
    - Kontrola na základe skenovaných dokumentov + WHOIS + faktúra alebo niečo podobné ☺
    - Certifikát obsahuje validované DNS meno a meno organizácie, možnosť wildcard certifikátov
  - Extended validation (EV)
    - Musí spĺňať podmienky
      - Organizácia musí byť registrovaná a mať fyzické sídlo (IČO, kontrola cez register)
      - Kontrola vlastníctva domény cez registrátora
      - Osoba ktorá žiada o certifikát musí byť autorizovaná (kontrola cez HR)
    - Certifikát obsahuje validované DNS meno a meno organizácie, wildcard certifikáty **nie sú** povolené
    - Certifikát
      - Na štruktúru mena sú kladené striktné požiadavky (Meno, Organizácia, Sídlo, IČO, ...)
      - Maximálna doba platnosti EV certifikátu je 27 mesiacov
      - Kryptografické algoritmy a veľkosti kľúčov SHA1+, RSA2048+, ECC NIST P-256
- Certifikáty pre osoby
  - S/MIME (spätná kontrola e-mailu) ~ domain validated úroveň
  - ZEP (osobná kontrola identity na základe primárneho dokladu OP, pas, ...) > EV úroveň*

* - za predpokladu že držiteľ nikomu nedá k dispozícii token a PIN ☺

# Problémy a kritika súčasného stavu

# SSL Observatory I.

- Projekt EFF SSL Observatory (talk Defcon, [27C3])
- Cieľom projektu je priniesť prehľad certifikátov určených pre HTTP/SSL na Internete (IPv4☺)
- Niekoľko zaujímavých zistení:
  - ~1400 CA (koreňové + podriadené) ktoré sú dôveryhodné pre MS / Mozilla
  - ~ 650 organizácií, ~50 krajín
  - Platné certifikáty obsahujú neúplné DNS mená (localhost, privátne IP adresy, webmail, ...)
  - Porušenie EV pravidiel (512 bit RSA EV certifikát, nekvalifikované meno, privátne IP adresy, dlhá doba platnosti, wildcard certifikáty)

# SSL Observatory II.

- Kontrola dostupnosti CDP pre certifikáty, ktoré
  - Boli dôveryhodné v rámci MS/Mozilla
  - Nemali špecifikované AIA/OCSP URI
  - Neboli certifikáty koreňových CA
- Jednoduchý python skript, ktorý
  - Kontroloval dostupnosť CDP pomocou
    - HTTP HEAD metódy
    - LDAP bind
  - Nekontroloval som iné protokoly

```
SELECT
    DISTINCT

        Issuer,
        `X509v3 extensions:X509v3 Authority Key Identifier:DirName`,
        `X509v3 extensions:X509v3 Authority Key Identifier:keyid`,
        `X509v3 extensions:X509v3 Authority Key Identifier:serial`,
        `X509v3 extensions:X509v3 CRL Distribution Points`
    FROM
        valid_certs
    WHERE
        `X509v3 extensions:Authority Information Access:OCSP - URI`
        IS NULL
        AND
        Issuer != Subject
```

- Výsledky (**nie príliš presné** ☹, HEAD, problémy so sieťou, problémy s kódovaním URI, ...*):
  - CCA 750 CA (*Distinct Issuer*)
  - CCA 1700 rozličných CDP extenzií
  - Schémy: celkový# dostupné
    - http 1617 1368**
    - neznáme 884*** N/A
    - ldap 391 14
    - https 10 N/A
    - file 2 N/A
  - Z 1700 CDP cca. 700 nebolo dostupných

* - problémy som neriešil nakoniec vôbec, dôvod bude zrejmý neskôr ...

** - zrejme niektoré CA majú viac HTTP CRL URI (max. boli 3)

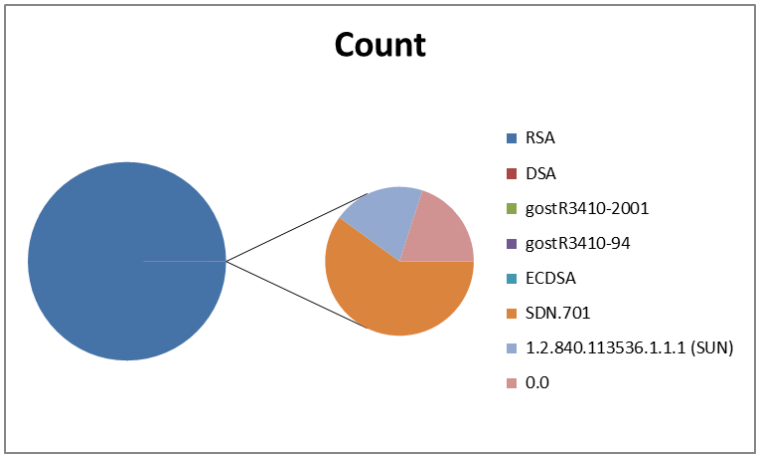
*** - napr. X.500 mená, prázdna extenzia

# SSL Observatory III.

- Rozdelenie algoritmov

| all | |
|---|---|
| RSA | 5603192 |
| DSA | 2890 |
| gostR3410-2001 | 359 |
| gostR3410-94 | 18 |
| ECDSA | 6 |
| SDN.701 | 3 |
| 1.2.840.113536.1.1.1 (SUN) | 1 |
| 0.0 | 1 |

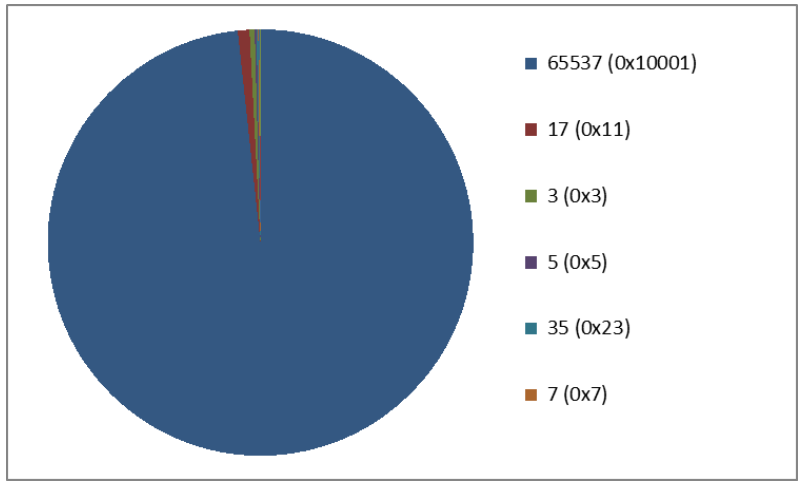
| valid | |
|---|---|
| rsaEncryption | 1455366 |
| dsaEncryption | 25 |




- Rozdelenie RSA exponentov

| all | |
|---|---|
| 65537 (0x10001) | 3 952 885 |
| 17 (0x11) | 35 313 |
| 3 (0x3) | 15 892 |
| 5 (0x5) | 5 521 |
| 35 (0x23) | 4 896 |
| 7 (0x7) | 2 977 |
| ... | ... |

| valid | |
|---|---|
| 65537 (0x10001) | 1 353 597 |
| 17 (0x11) | 23 692 |
| 3 (0x3) | 493 |
| 5 (0x5) | 212 |
| 7 (0x7) | 95 |
| 35 (0x23) | 46 |
| 11 (0xb) | 31 |
| ... | ... |



# SSL Observatory IV

```
SELECT
    `RSA Public Key:Modulus` AS RSA_MOD,
     count(*) AS CNT FROM valid_certs
  WHERE
    `RSA Public Key:Modulus` IS NOT NULL AND
    `Subject Public Key Info:RSA Public Key:Exponent`=65537
  GROUP BY RSA_MOD
  HAVING  CNT>1
```

- Duplicitné RSA kľúče
  - Exponent 65537
    - Spolu 1 353 597 Duplicitné 13 097 (cca 1%) Skupín 3191
  - Exponent 17
    - Spolu 23 692 Duplicitné 8 (cca 0%) Skupín 4
  - Exponent 3
    - Spolu 493 Duplicitné 24 (cca 5%) Skupín 8
  - Exponent 5
    - Spolu 212 Duplicitné 2 (cca 1%) Skupín 1
  - Exponent 7
    - Spolu 97 Duplicitné 0 (0%) Skupín 0
- Príčiny
  - Certifikáty od rozličných CA (málo)
  - Zlý spôsob generovania kľúčov
    - Debian bug, väčšinou odstránený
    - Iný podobný bug

# (Známe) pochybenia/otázne praktiky CA

- Verisign
  - Vydal code-signing certifikát osobe ktorá predstierala, že je zamestnancom MS
  - Následky
    - Zrušenie platnosti prostredníctvom CRL/OCSP
    - **Patch v OS, hardcoded hash certifikátu**
- DigiCert
  - Vydal certifikát s > 100 SAN (Subject Alternative Name), medzi inými www.isaca.org
  - V zásade nič tragické až na to, že niektoré aplikácie nepočítajú s takým vysokým množstvom mien
- Comodo hack
  - Iránsky hacker si vydal certifikáty pre mail.google.com, login.live.com, ...
  - Následky
    - Zrušenie platnosti prostredníctvom CRL/OCSP
    - **Patch v prehliadačoch/OS, hardcoded hash certifikátu**
- Certied Lies: Detecting and Defeating Government Interception Attacks Against SSL
  - Diskusia na tému čo sa stane keď CA je kontrolovaná štátom
  - Jeden z *„dôkazov“* mala byť skutočnosť že spoločnosť Packet Forensics vyrába zariadenie umožňujúce forenznú analýzu SSL/TLS spojení za predpokladu platného certifikátu

# Problémy v softvéri

- Validačné problémy
  - Ako sa správajú prehliadače ak nie je dostupné CRL/OCSP
  - FF 4
    - DV, OV – kontroluje OCSP (ak je v AIA), CRL nekontroluje
    - EV – kontroluje OCSP, ak nie je dostupný odstráni green bar
  - IE
    - DV, OV, EV – CRL+OCSP (na Vista+), ak nie je dostupné nenastane žiadna zmena v UI
  - Chrome 11
    - DV, OV – CRL + OCSP, zelený/žltý (dostupný/nedostupný)
    - EV – CRL + OCSP zelený bar/žltý (dostupný/nedostupný)
  - Opera
    - DV, OV, EV – CRL+OCSP, ak nie je dostupné UI odstráni indikáciu zabezpečenia
- Čiastočne fixnuté UI problémy
  - sslstrip (odstráni z liniek https schému, pridá favicon žltého zámku☺)
  - [Yes] button a chybové okná
- Už fixnuté problémy s null terminated menami v certifikátoch
  - www.paypal.com\0.toughcrime.org alebo *\0.toughcrime.org
  - CA overí toughcrime.org, prehliadač zobrazí paypal.com

# Long-term riešenia

# Prečo je ťažké odstrániť CA zo zoznamu dôveryhodných CA a prečo teda CA vôbec používame

- Comodo diskusia na mozilla-dev-security-policy@lists.mozilla.org
  - Držitelia certifikátov musia vymeniť všetky certifikáty (nemalé finančné náklady)
  - Používatelia môžu
    - (ešte viac) ignorovať chybové hlásenia ohľadom SSL
    - Prejsť na iný prehliadač
  - CA too big to fail
    - if the CA has 1000 certs on issue, and gets breached, the CA has a problem. If the CA has a million certs on issue, then we've got a problem.
  - https://bugzilla.mozilla.org/show_bug.cgi?id=647959 (Honest Achmed CA)
    - Achmed's business plan is to sell a sufficiently large number of certificates as quickly as possible in order to become too big to fail (see "regulatory capture"), at which point most of the rest of this application will become irrelevant.
- CA filtrujú mená náchylné na zneužitie, napr.:
  - your-account-bankofamerica.com
  - my-email-live.com
  - google-accounts.com
  - my-paypal-account.com
- Infraštruktúra je dosť rozšírená, začať na zelenej lúke sa prakticky nedá
- Riešenie: kontrola CA (nie audit ☺)

# DANE I.

## (DNS based authentication of named entities)

- Protokol (v štádiu návrhu), ktorý umožní asociovať certifikát s DNS menom pomocou nového DNS RR záznamu TLSA
- Poskytuje dve služby
  - Asociácia certifikátu s DNS menom
  - Kontrola asociácie certifikátu s DNS menom
- Stručný opis protokolu
  - Meno záznamu _<port>._<protokol>.<meno> napr.
    - _443._tcp.www.example.com
    - _25._tcp.mail.example.com
  - Hodnota záznamu <typ asociácie>.<typ certifikátu>.<hodnota>
    - Typ asociácie
      - 1 – certifikát koncovej entity
      - 2 – certifikát CA
    - Typ certifikátu
      - 0 – celý certifikát DER kódovaný, (bajty v hexadecimálnom zápise)
      - 1 – SHA-256 hash certifikátu (ako v prípade 0)
      - 2 – SHA-512 hash certifikátu (ako v prípade 0)

# DANE II. (príklady)

SHA-256 hash certifikátu pre www.progressbar.sk

_443._tcp.www.progressbar.sk. IN TLSA (

1 1

840df9719e3b01c448cec697df09f7c9a9169e690b780a12bbc4dfe3da68237d)

DER kódovaný certifikát www.progressbar.sk

_443._tcp.www.progressbar.sk. IN TLSA (

1 0 308207CD308206B5A003020102020301...)

# DANE III.

- Výhody
  - Umožní distribúciu self-signed certifikátov
- Nevýhody
  - Vyžaduje implementáciu na strane klienta
  - DNS nie je bezpečný protokol
  - Na zabezpečenie maximálnej bezpečnosti vyžaduje DNSSEC
  - DNSSEC – ďalšia PKI, ktorá sa presadzuje len veľmi pomaly. Výhodou je že na rozdiel od X.509 PKI, DNSSEC má lepšiu možnosti validácie koncových entít
  - Self-signed certifikáty pre progressbar.sk a progresbar.sk budú z pohľadu prehliadača nerozlíšiteľné
- Otázne
  - Podľa jedného z predbežných draft-ov nie je DNSSEC nevyhnutný pre kontrolu asociácií. V takom prípade by boli klienti chránení, ak majú DNS TLSA RR uložený v cache, alebo ak útočník nedokáže modifikovať DNS komunikáciu.

# DNS Certification Authority Authorization (CAA) Resource Record

- Protokol v štádiu návrhu, určený pre komunikáciu medzi koncovou entitou a CA, resp. na overenie platnosti certifikátu spoliehajúcou stranou.
- Pridáva ďalšie kritérium pre validáciu, tento krát na vydávajúcu CA
- Stručný opis protokolu DNS RR CAA
  - <dns meno> <flags> <tag> <data>
  - flags – opisujú komu je RR určený (CA / spoliehajúca strana) ako aj kritickosť údajov
  - tag – určuje typ údajov napr. OID identifikátor policy alebo cestu dôvery
    - OID policy špecifikuje že ľubovoľná CA, ktorá deklaruje danú policy môže vydať pre túto doménu certifikát
    - Cesta dôvery môže byť určená ako hash certifikátu alebo verejného kľúča, v tvare

```
ObjectDigestReference ::= SEQUENCE {
    type            OBJECT IDENTIFIER,
    digestAlgorithm  OBJECT IDENTIFIER,
    digest          OCTET STRING    }
```

# CAA II.
# (príklady)

**Certifikát môže byť vydaný len ak CA delaruje dodržanie jednej z policy ...**

$ORIGIN example.com

. CAA 1 policy 1.3.6.1.4.1.35405.666.1

. CAA 1 policy 1.3.6.1.4.1.35405.666.2

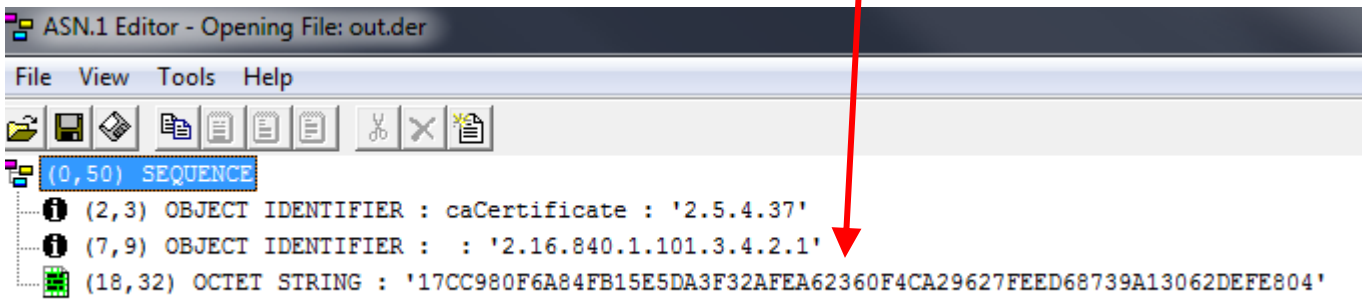
**Certifikát môže vydať len CA ktorej certifiát/verejný kľúč zodpovedá ceste**

$ORIGIN example.com

. CAA 1 path MDIGA1UEJQYJYIZIAWUDBAIBBCAXzJgPaoT7Fe
XaPzKv6mI2D0yilif+7WhzmhMGLe/oBA==

```
$echo MDIGA1UEJQYJYIZIAWUDBAIBBCAXzJgPaoT7FeXaPzKv6mI2D0yilif+7WhzmhMGLe/oBA== ! base64 -d > c:\temp\out.der

$openssl sha256 c:\temp\ca-der.crt.cer
SHA256(c:\temp\ca-der.crt.cer)= 17cc980f6a84fb15e5da3f32afea62360f4ca29627feed68739a13062defe804
```



# CAA III.

- Všeobecnejší prístup ako DANE
- Umožňuje obmedziť tak klientov ako aj (najmä) CA
- Teoreticky nevyžaduje DNSSEC (pre CA)
- Nevyžaduje zmeny na klientovi (ak sa používa len CA časť)
- Vynútiteľné zo strany prehliadačov
- Prirodzene nechráni pred CA ktoré sú zlomyseľné

# Short-term riešenia

# Extenzie v prehliadačoch

- DNSSEC (zatiaľ FF/v budúcnosti aj Chrome)
  - Umožňuje podporu DNSSEC v rámci prehliadača
- Certificate Patrol (FF)
  - SSH like Trust-on-first-use
  - lokálna databáza certifikátov, pri prvom použití uloží, ak sa zmení tak FF upozorní
  - problematické pri rotovaní kľúčov (napr. google tak robí)
- Perspectives (FF/Chrome)
  - Distribuovaná databáza certifikátov pre servery, udržiavaná „notármi“
  - Komunikácia medzi klientom a servermi „notára“ je digitálne podpísaná (samostatná PKI ☺)
  - Umožňuje override FF chybových hlásení

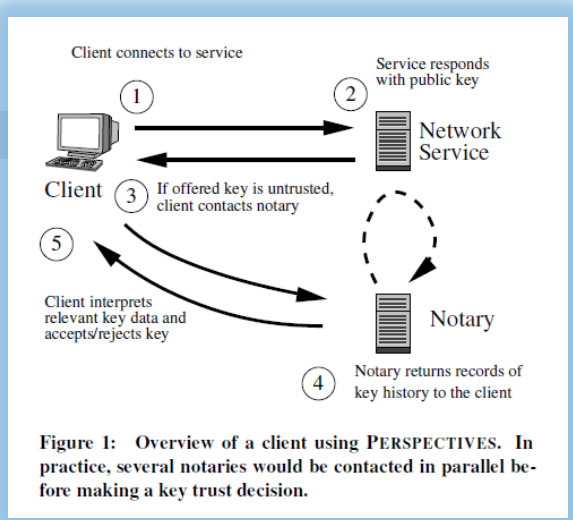
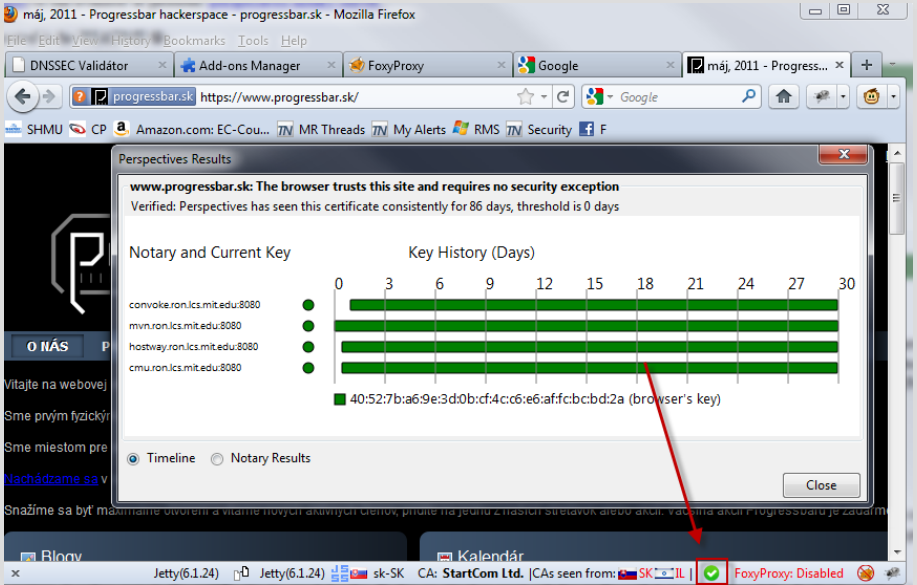
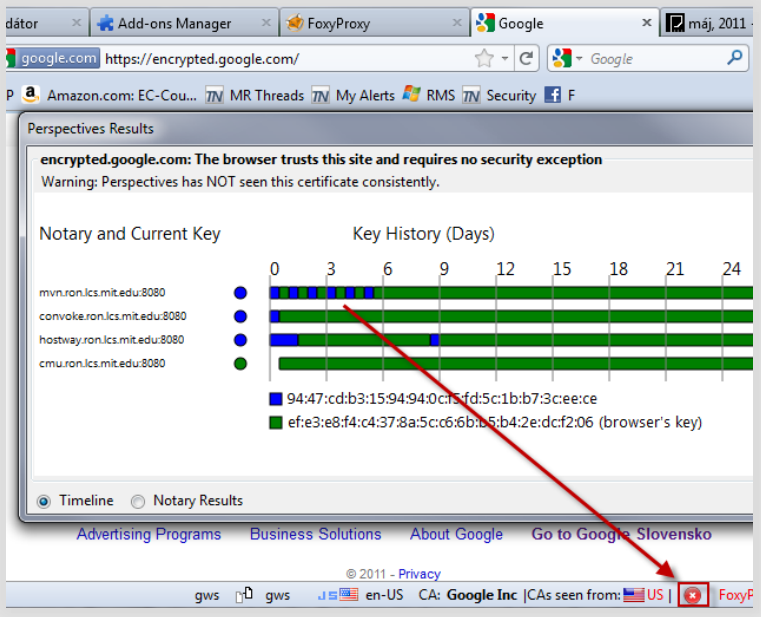


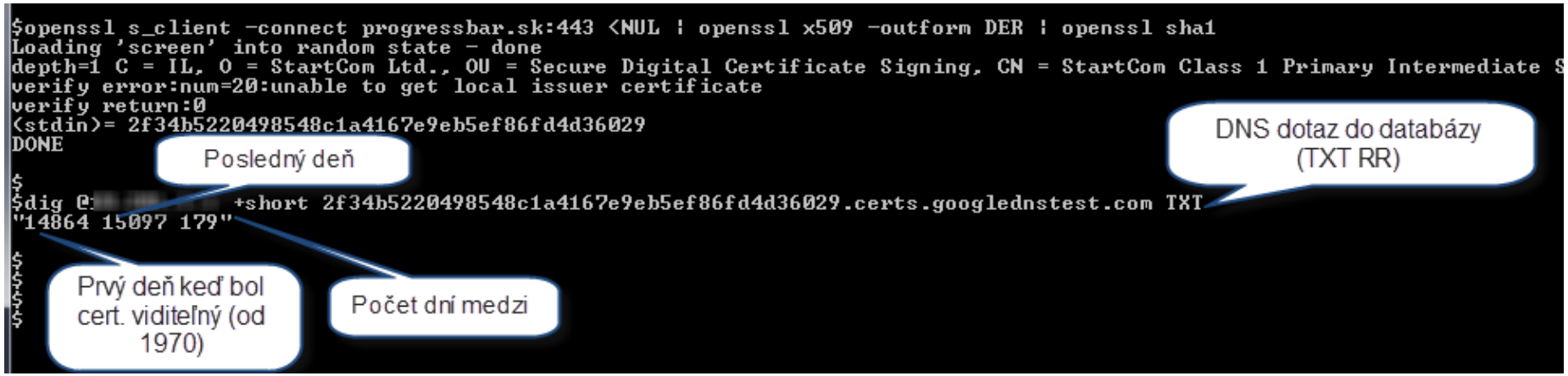

**Figure 1: Overview of a client using PERSPECTIVES. In practice, several notaries would be contacted in parallel before making a key trust decision.**



# Chrome a Google certificate catalog

- Obdoba Perspectives / DANE
- Databáza vybudovaná google servermi pri prehliadaní internetu
- Súčasťou databázy sú len certifikáty ktorých mená sedia s doménou a sedí dig. podpis
- Publikovaná prostredníctvom DNS (SHA-1 hash)
- Uvažuje sa o implementácii do Chrome
- Prirodzene nerieši revokáciu ale len kontrolu CA
- Tiež vyžaduje DNSSEC na bezpečnú implementáciu ☹



# Vďaka že ste vydržali

Otázky?

martin.rublik@gmail.com