Jak moc důvěryhodné jsou důvěryhodné Certifikační Autority?

Motto: „Uvnitř každého velkého problému je malý, který usiluje, aby se dostal ven.“

Jan Dušátko jan.dusatko@cryptosession.cz

O čem se tu budeme bavit?

- Certifikát (Root, Leaf, Self-signed, Trusted …)
- Závislost na dalších službách
- Certifikační autorita jako důvěryhodná třetí strana?
- Důkazy platnosti certifikátu
- DNS(SEC) jako důvěryhodná čtvrtá strana?
- Důkazy pravosti certifikátu
- Důkazy odpovídajícího vztahu certifikátu k danému zdroji
- Extra porce zábavy – důvěryhodnost v rámci SSL/TLS
- Dezert na závěr: vztah klíč-uživatel, důkaz (vůle, místa a času původu)

Certifikát

Jedná se o reprezentaci veřejného klíče s rozšiřujícími informacemi. Je generován na základě privátního klíče (formáty DER/CER/BER, uložen jako DER/PEM/CRT/P7/P12 ...)
Obsahuje důležité informace

- Platnost od-do
- Sériové číslo
- Specifikace algoritmu a veřejný klíč (slabiny hash funkci, výplní, nonce)
- Způsob použití klíče (podpis, šifrování, podepisování certifikátů, ...)
- Common name
- SKI - Subjec Key Identifier / AKI - Authority Key Identifier
  (SKI je hash veřejného klíče certifikátu, AKI autority, důležité pro certificate chain)
- ... a další
- Podpis autoritou

DER je důležitý formát s jednoznačnou syntaxí dat a v nejkratší možné délce !

Požadované služby

Pro ověření certifikátu je nutné mít k dispozici

- Přesný časový zdroj (NTP, NTS …)
- Funkční DNS pro rozlišení jmen
- Vhodná podpora dalších protokolů na straně CA
  - SVP, SVP
  - HTTP a díky HTTP i OSCP, CRL
  - HTTP/FTP/LDAP pro SCVP, DPD, DPV
  - LDAP pro poskytnutí informací o certifikátech

Přehled protokolů pro distribuci času https://cryptosession.cz/blog/bezpecnost-distribuce-casu

Rozdíly mezi certifikáty

Certifikát	Podepsán	Použití	Vlastnost
Self-sign	Sebou samým	Ochrana komunikace	Digitální podpis / šifrování
Root	Sebou samým	Poskytnutí důvěry	Podpisy certifikátů nebo seznamů
Intermediate	Nadřízeným	Poskytnutí důvěry	Podpisy certifikátů nebo seznamů
Leaf	Nadřízeným	Ochrana komunikace	Digitální podpis / šifrování

Certifikát je důvěryhodný, pokud je umístěn v důvěryhodném úložišti.
Důvěryhodnost je založena na kryptografickém důkazu.

Na správě důvěryhodného úložiště pracují:

- CA Browser forum
- Firmy zajišťující vývoj operačních systémů a aplikací
- Správci – opravdu?
- Evidence – opravdu?

Certifikační autorita jako důvěryhodná třetí strana

Poskytuje:

- Kořenový certifikát
- Informace o věrohodnosti certifikátu (verifikace)
- Metody ověření žadatele (Registrační Autorita pro OV/DV/IV, původně i EV)
- Důvěryhodnost je založena na kryptografickém důkazu.

Certifikační autority se shlukují do skupin: CA Browser forum
Certifikační autority jsou shlukovány do skupin: Trusted browser list

Důkaz platnosti certifikátu

	Certificate chain	CRL	CRL Lite	OCSP (+stapling)	Certificate Transparency
Příslušný k CA	Kryptograficky: **Q** Technicky: Ano	**Kryptograficky: Ne** Technicky: Ano	**Kryptograficky: Ne** Technicky: Ano	Kryptograficky: Ano Technicky: Ano	Kryptograficky: Ano Technicky: Ano
Vydaný	Kryptograficky: Ano Technicky: Ano	**Kryptograficky: Ne** Technicky: Ano	**Kryptograficky: Ne** Technicky: Ano	Kryptograficky: Ano Technicky: Ano	Kryptograficky: Ano Technicky: Ano
Platný	Kryptograficky: Ano Technicky: Ano	**Kryptograficky: Ne** Technicky: Ano	**Kryptograficky: Ne** Technicky: Ano	Kryptograficky: Ano Technicky: Ano	**Kryptograficky: Ne** Technicky: Ano
Expirovaný	Kryptograficky: Ano Technicky: Ano	Kryptograficky: Ano Technicky: Ano	Kryptograficky: Ano Technicky: Ano	Kryptograficky: Ano Technicky: Ano	**Kryptograficky: Ne** Technicky: Ano
Revokovaný	**Kryptograficky: Ne** Technicky: Ano	Kryptograficky: Ano Technicky: Ano	Kryptograficky: Ano Technicky: Ano	Kryptograficky: Ano Technicky: Ano	**Kryptograficky: Ne** Technicky: Ano
Pozastavený	**Kryptograficky: Ne** Technicky: Ano	Kryptograficky: Ano Technicky: Ano	Kryptograficky: Ano Technicky: Ano	Kryptograficky: Ano Technicky: Ano	**Kryptograficky: Ne** Technicky: Ano
Podvržení certifikátu	Kryptograficky: **Q** Technicky: Ano	**Kryptograficky: Ne** **Technicky: Ne**	**Kryptograficky: Ne** **Technicky: Ne**	Kryptograficky: Ano Technicky: Ano	**Kryptograficky: Q** **Technicky: Q**

Poznámka: Neurčitost v případě podvržení certifikátu je určena politikou. Odpovědnosti za publikování v CTL logů je podmíněno požadavkem na ověření (například pro prohlížeče), ale není striktní podmínkou.

DNSSEC jako důvěryhodná čtvrtá strana

Poskytuje:

- Metodu ověření certifikátu pro daný server (SRV+DANE TLSA)
- Informace o věrohodnosti certifikátu (verifikace)
- Nabízí volitelnou možnost autorizovat CA pro vydávání certifikátů (CAA)

DANE TLSA vyžaduje DNSSEC
DANE TLSA je vhodné automatizovat (často chybí)
CAA je určeno pro Certification Authority Authorization
CAA není striktně vyžadováno

... a není to málo Antone Pavloviči?

Důkaz pravosti certifikátu

	Certificate chain	CRL MiniCRL	OSCP	CTL	DANE TLSA	DANE CAA
Příslušnost k:						
• **CA**	Ne	Ne	Ano	Detekce?	Ne	Přihlíží se
• **Organizaci**	***CN***	Ne	Ne	Ne	Ne	Ne
• **Serveru**	***SAN***	Ne	***SAN***	Ne	Ano	Ne
Padělání:						
• **Certifikátu**	Ne	Ne	Ano	Detekce?	Ano	Ne
• **Žádosti pro CA**	Ne	Ne	Ne	Detekce?	Ne	Ne
• **Využití jiné CA**	Ne	Ne	Ne	Ne	Ne	Přihlíží se
• **Certifikátu pro server**	Ne	Ne	Ne	Ne	Ano	Ne

Poznámka: Mezi technickým a kryptografickým pohledem na důkaz je výrazný rozdíl.

Problémové menu

- Je certifikát vydaný správnou autoritou?
- Je certifikát platný (kryptograficky) a přísluší k dané autoritě?
- Je certifikát vydaný pro správnou organizaci?
  - domain squatting, domain typo-squatting, combo-squatting
  - homoglyph attacks, IDN spoofing, lookalike domain spoofing
  - subdomain takeover, subdomain delegation abuse, dangling DNS
- Odpovídá certifikát daného serveru požadovanému certifikátu?
- Je autorita v seznamu důvěryhodných certifikačních autorit?
- Je autorita v seznamu dle vaší politiky? Jiným způsobem, věříte jí?
- Došlo k MITM (podvržení na cestě)? Jak to ověříte?
- Jste varování, pokud je certifikát podvržen? (jiná CA/organizace/server)

A co zkracování životnosti certifikátů

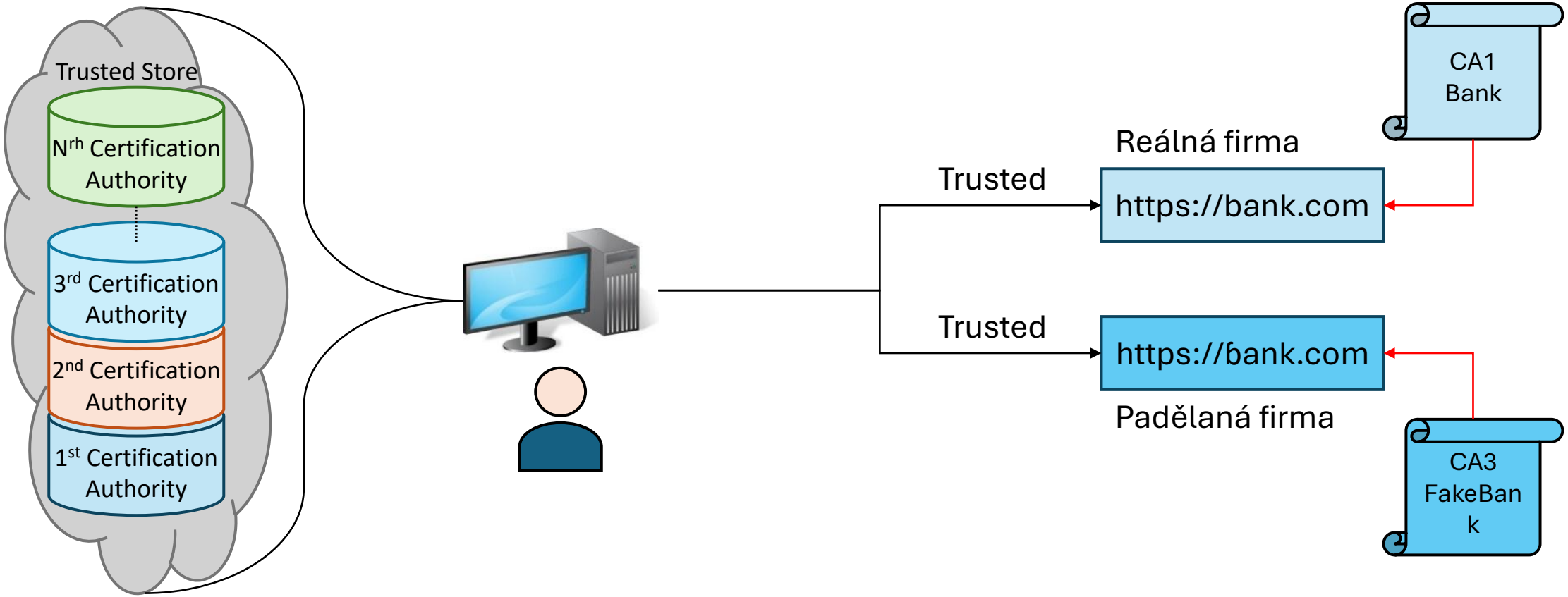
- Vyžaduje automatizaci
- Za určitých podmínek vyžaduje vyšší náklady
- Vytváří riziko Denial of Service
- Pro Let’s Encrypt je doba obnovy provozu (RTO) 72h, pro ostatní autority nenalezeno
- Žádost o registraci u Registrační Autority do 7 dnů
- Žádost o DV certifikáty v rozmezí 10sec – 1 den
- Žádost o EV certifikáty do 5 dní
- Odvolání certifikátů do 1 dne
- Zveřejnění nového CRL co nejdříve (nespecifikováno)

Nejhorší scénář pro novou žádost by měl být do 15 dní, pro obnovu do 8 dní
Nejhorší scénář pro revokaci by měl být kratší než 4 dny

Příklad homoglyfů, aneb certifikát na 100+1 způsob

Příklad:

- Přístup na **bank.com** je bezpečný, protože je chráněn certifikátem vydaným certifikační autoritou na bank.com, daná CA je v Trusted Certificate Store?
- Homoglyph attack: přístup na **bank.com** je bezpečný, protože je chráněn certifikátem vydaným certifikační autoritou na bank.com. Daná CA je v Trusted Certificate Store?



Důvěryhodnost v SSL/TLS

Anonymous TLS	TLS_Anon_Ciphersuite	Bez ověření
Jednostranné TLS	TLS_Ciphersuite	Server
Mutual TLS (mTLS)	TLS_Ciphersuite	Server+Klient

SSL 3.0 – TLS 1.2

TLS_	DH_	RSA_	EXPORT_	WITH_DES40_CBC_	SHA
	Ustanovení tajemství	Autentizace	Exportní verze	Symetrická šifra (+ mód)	MAC/PRNG

Důkazy

- Vztah subjekt a certifikát (uživatel a klíč), schopnost jeho kontroly
- Důkaz vůle, tedy prokazatelné a vědomé využití klíčového materiálu uživatelem k podpisu dat
- Důkaz místa původu, tedy podepsání dat/hashe dat klíčovým materiálem daného systému
- Důkaz času vytvoření, tedy podepsání dat/hashe dat a časového razítka klíčovým materiálem systému

Ale co dělat v případě, pokud je řetězec důvěry narušen?

Otázky: kdo má právo vytvářet klíčový materiál?
(téma na diskusi z hlediska zákonů a BCP)

https://cryptosession.cz/blog