Infrastruktura veřejného klíče

Milan Radojčić

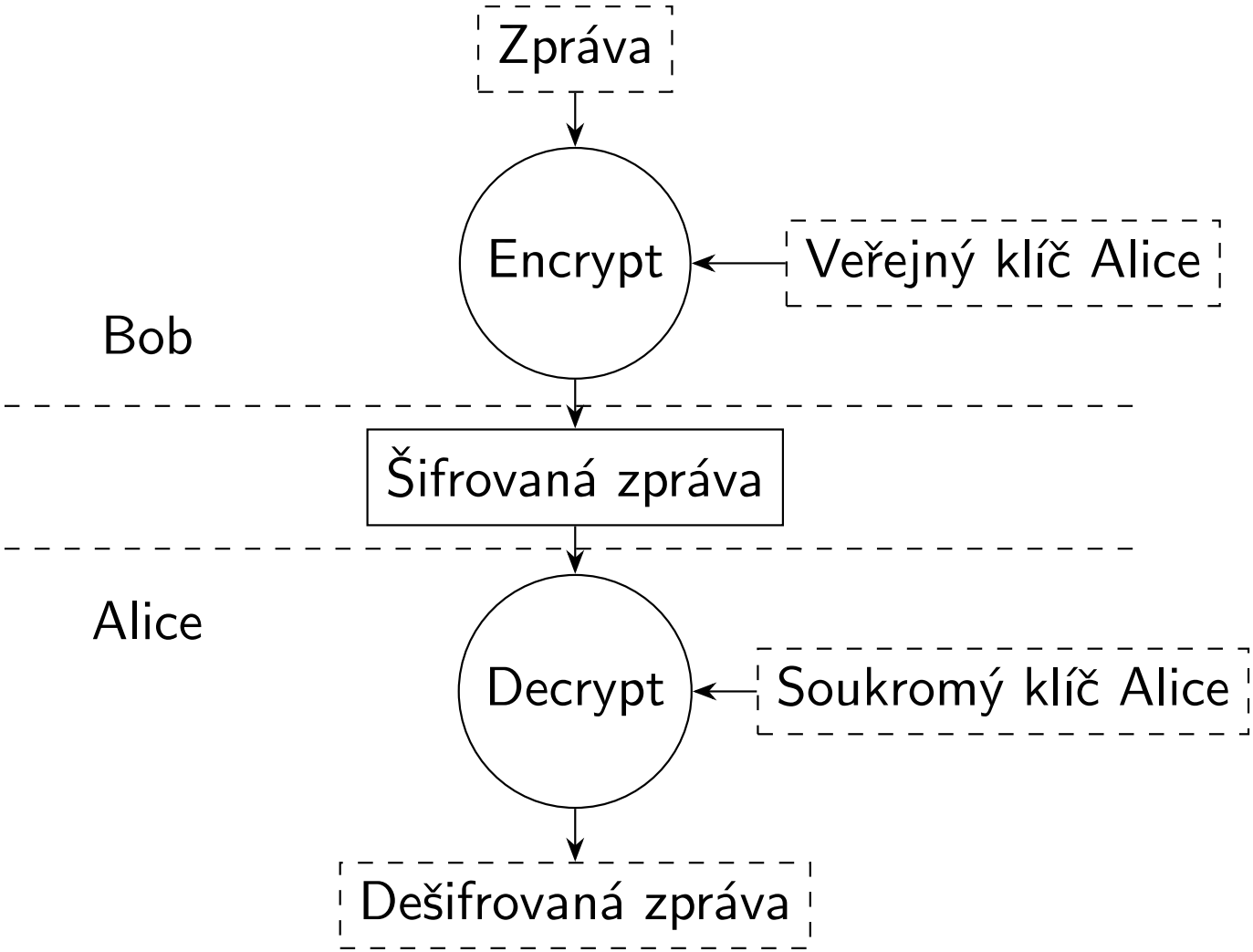
SSPŠaG – KBB

6. dubna 2026

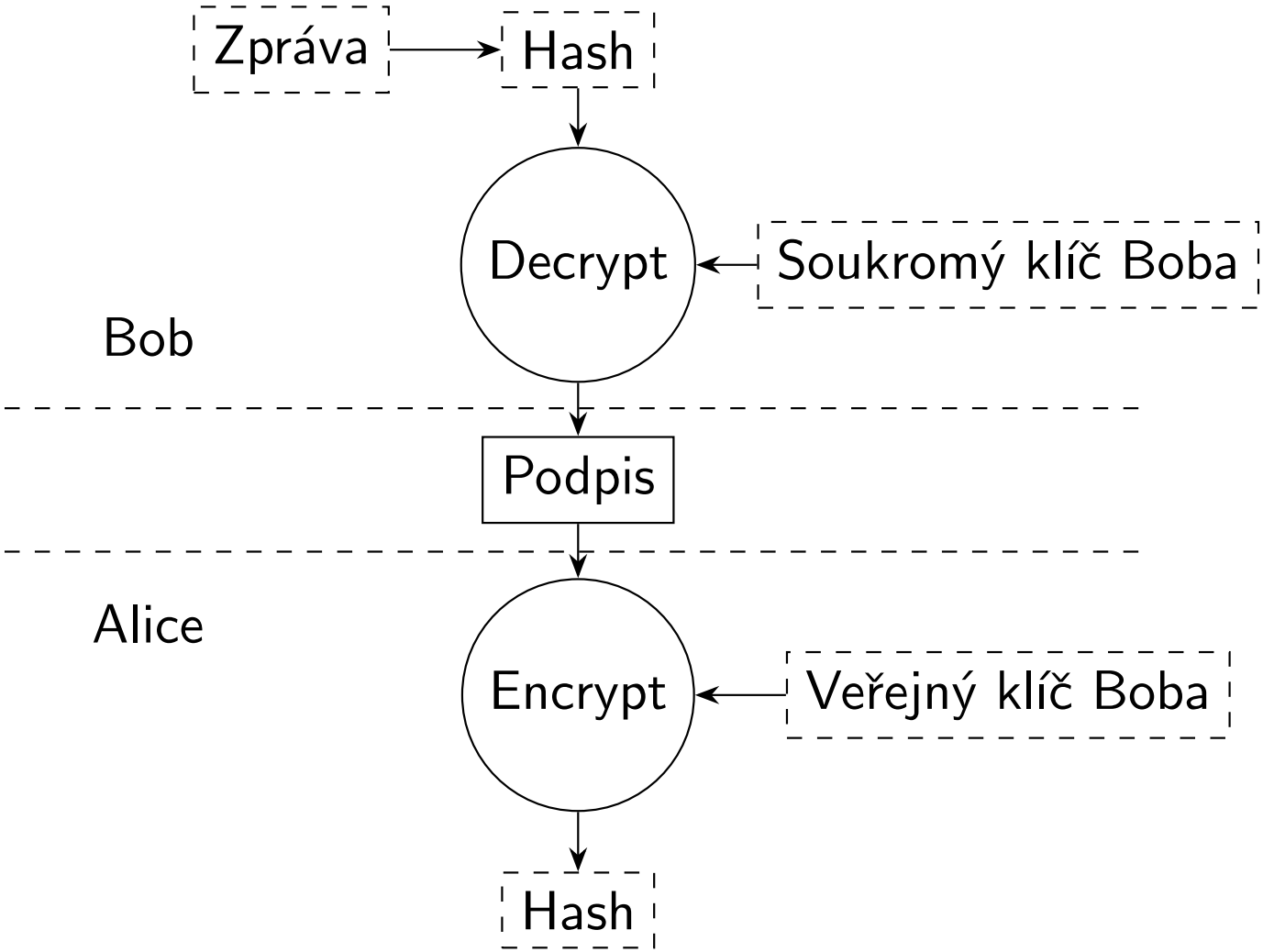
Hlavní body

Hlavní body

Šifrování asymetrickou šifrou



Asymetrický podpis

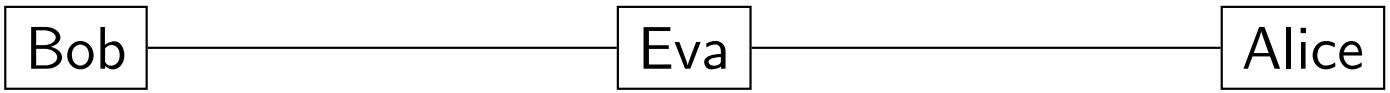


Proč potřebujeme řešit distribuci veřejného klíče?

Než začnou komunikovat, musí Bob poslat Alici svůj VK.

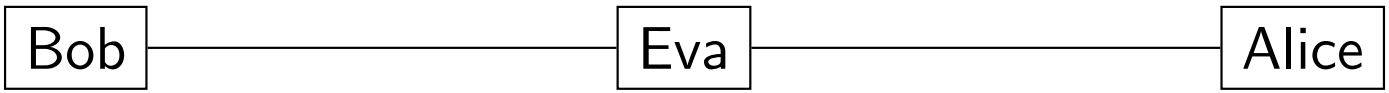
Proč potřebujeme řešit distribuci veřejného klíče?

VK Boba $\rightarrow$

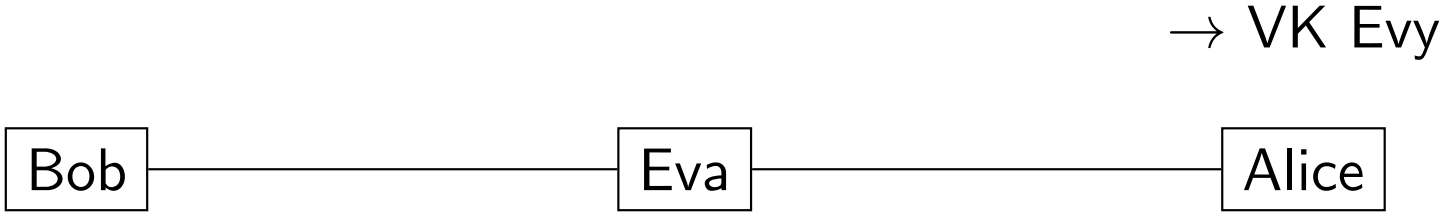


Proč potřebujeme řešit distribuci veřejného klíče?

VK Boba $\rightarrow$ VK Evy



Proč potřebujeme řešit distribuci veřejného klíče?



Alice získá VK Evy, o kterém si myslí, že to je VK Boba.

Proč potřebujeme řešit distribuci veřejného klíče?

Podpis SK Boba $\rightarrow$

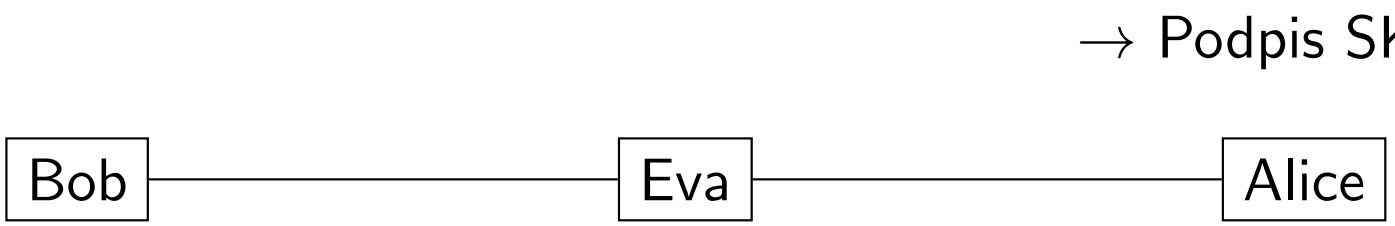
Teď chtějí Alice a Bob komunikovat s použitím autentifikace.

Proč potřebujeme řešit distribuci veřejného klíče?

Podpis SK Boba $\rightarrow$ Podpis SK Evy

Eva může upravit zprávu a změnit podpis na svůj.

Proč potřebujeme řešit distribuci veřejného klíče?



Alice přijímá zprávu, o které si myslí, že je od Boba, ale doopravdy je od Evy.

Proč potřebujeme řešit distribuci veřejného klíče?

- Problém – Chceme nějak spojit klíč a identifikační údaje tak, aby Alice mohla ověřit, že daný klíč opravdu patří Bobovi.
- Jedním z možných řešení je **certifikace veřejných klíčů**.

Hlavní body

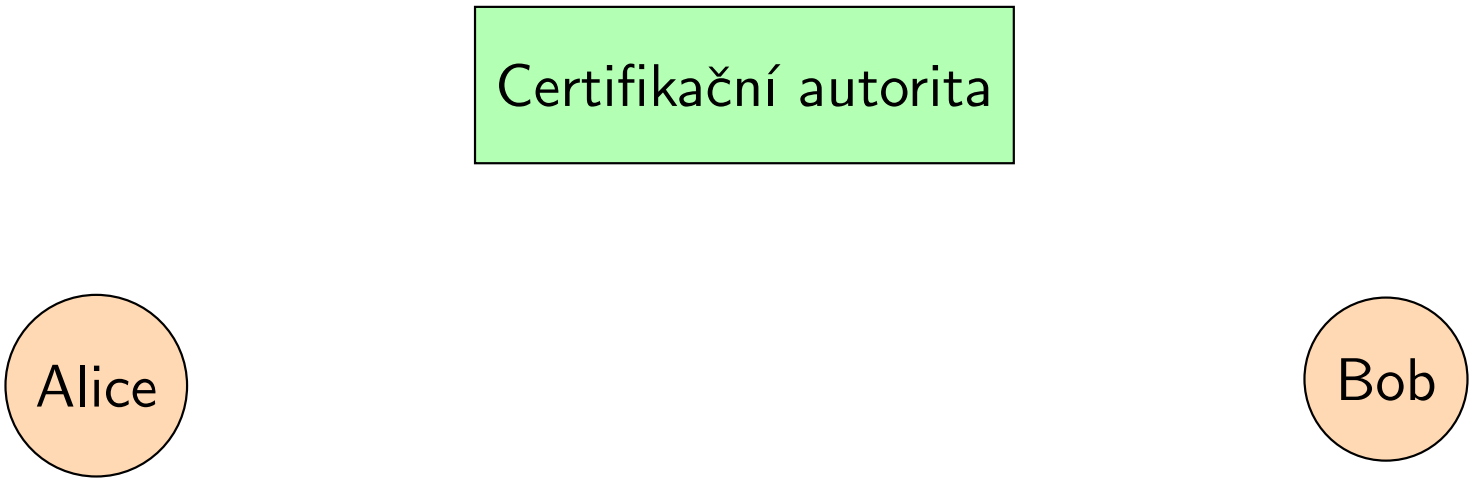
Certifikace veřejných klíčů

- Autorita vydá **certifikát**, který obsahuje veřejný klíč, identifikaci subjektu a dobu platnosti.
  - Certifikát je podepsaný autoritou.
- Při komunikaci si můžou strany vyměnit své certifikáty a ověřit, že jsou podepsány certifikační autoritou bez nutnosti kontaktovat autoritu.

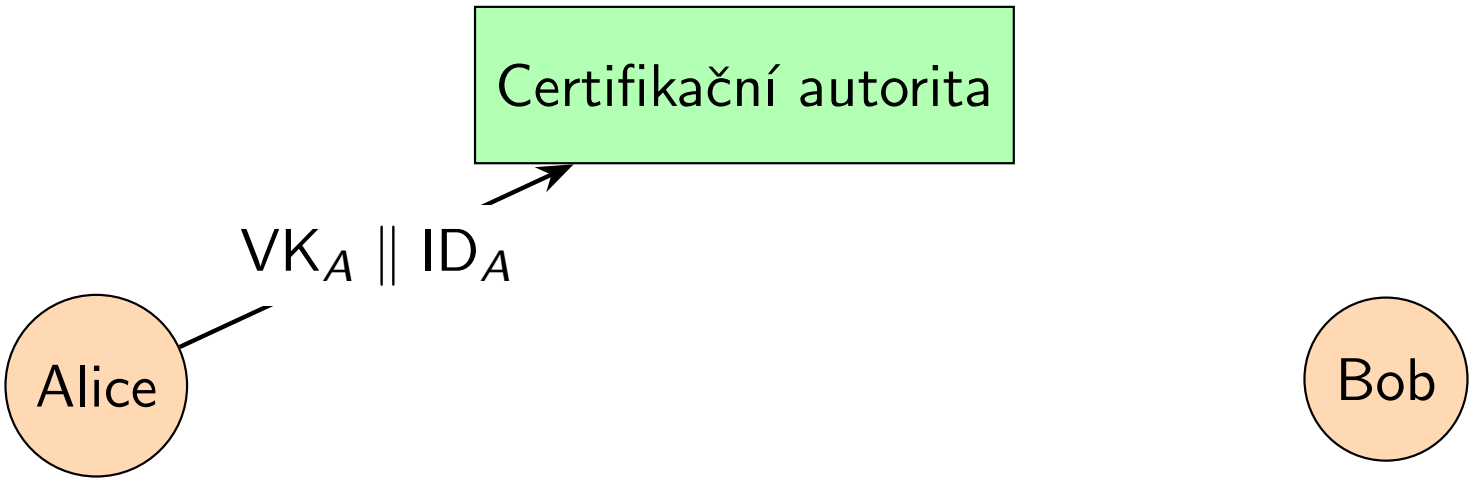
Certifikace veřejných klíčů

- Autorita vydá **certifikát**, který obsahuje veřejný klíč, identifikaci subjektu a dobu platnosti.
  - Certifikát je podepsaný autoritou.
- Při komunikaci si můžou strany vyměnit své certifikáty a ověřit, že jsou podepsány certifikační autoritou bez nutnosti kontaktovat autoritu.
- Nutnost předem sdíleného veřejného klíče autority.

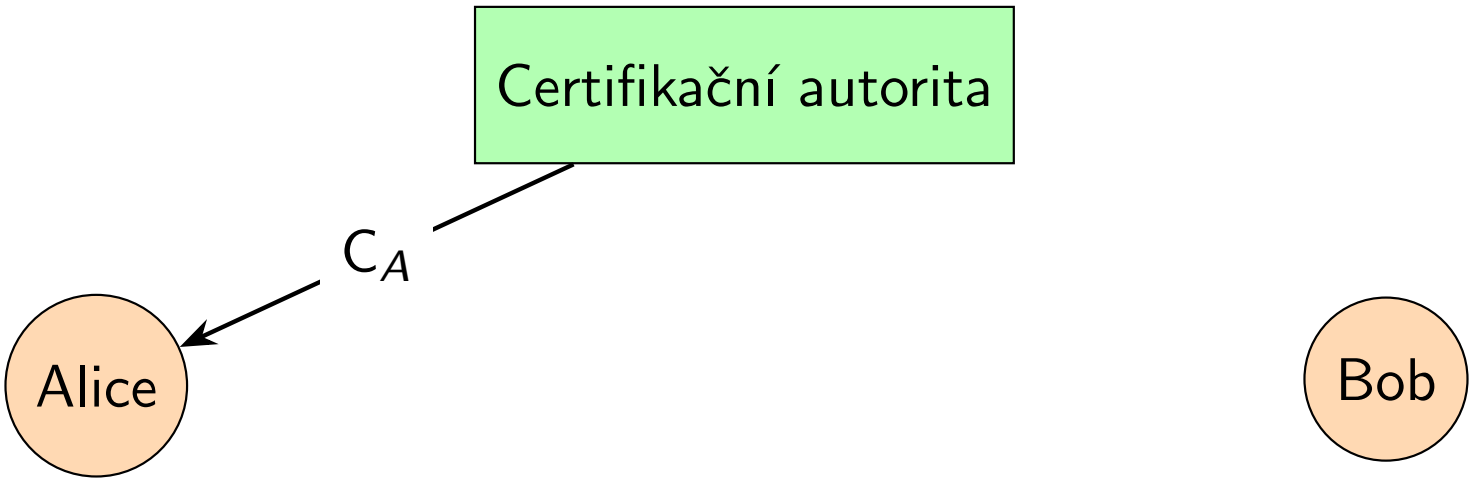
Certifikace veřejných klíčů



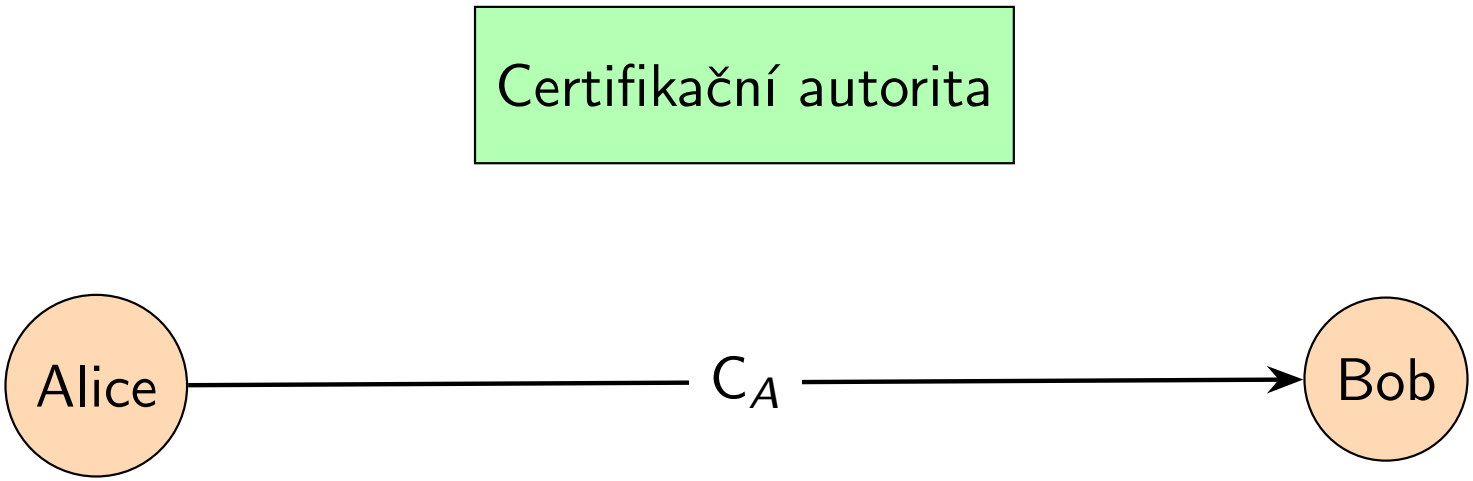
Certifikace veřejných klíčů



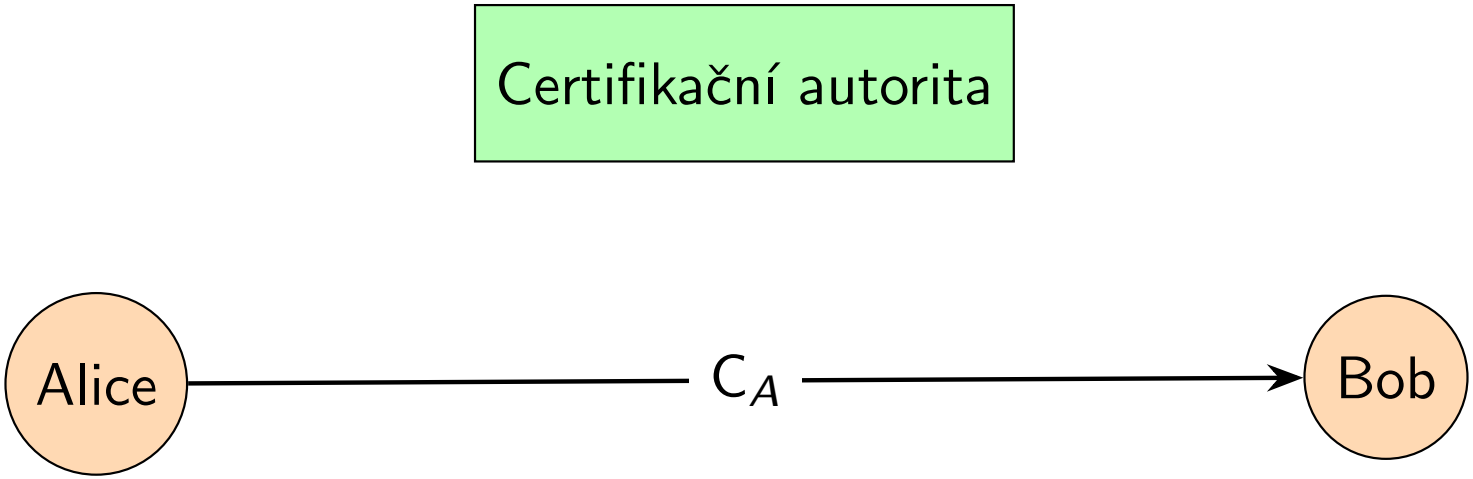
Certifikace veřejných klíčů



Certifikace veřejných klíčů



Certifikace veřejných klíčů



Bob může zkontrolovat, že klíč opravdu patří Alici bez nutnosti kontaktovat CA.

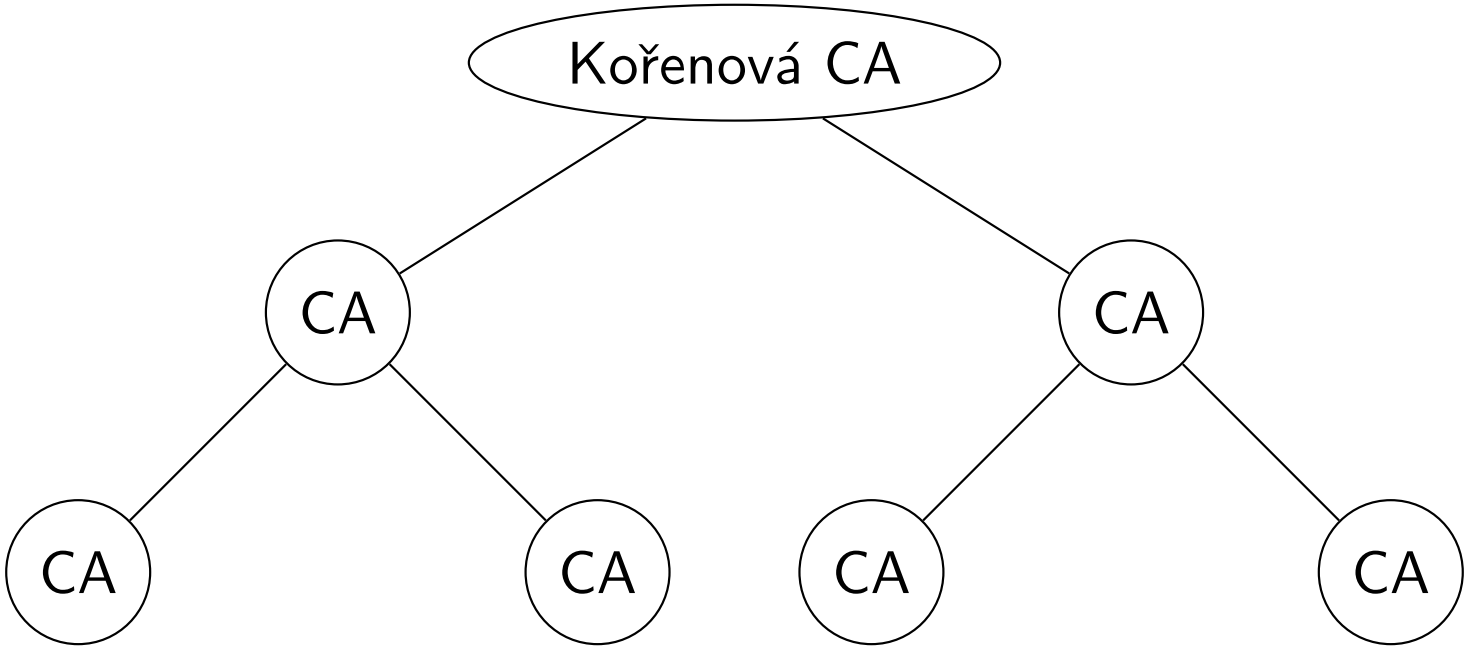
Certifikace veřejných klíčů

Pro toto schéma platí:

1. Kdokoliv může číst certifikát, aby zjistil, komu patří.
2. Kdokoliv může zkontrolovat, že je certifikát validní (validně podepsaný).
3. Jenom CA může vydávat nové certifikáty.
4. Kdokoliv může verifikovat, že je certifikát platný (timestamp).

Certifikace veřejných klíčů

- Nastává ale problém: jedna autorita nemusí zvládnout spravovat tolik subjektů.
- Řešení: stromová hierarchie


Kořenová CA
CA
CA
CA
CA
CA
CA

- Při ověřování musíme pak projít celý řetěz certifikátů a ověřit, že všechny platí.
- Pokud všechny platí a věříme kořenové CA $\Rightarrow$ certifikát je platný.

Platnost klíčů

- Certifikáty obsahují timestamp.
- Na žádost lze certifikát zrušit (např. vyzrazen SK).
- CA pak publikuje seznam zrušených certifikátů.

Zobrazení certifikátů

- `openssl s_client -showcerts -servername ssps.cz -connect ssps.cz:443`
- `openssl x509 -text`

Hlavní body

Struktura TLS certifikátu

Nejčastější pole certifikátu jsou:

- **Doména subjektu**
- Organizace subjektu
- Název autority, která vydala certifikát
- Čas vydání
- **Čas expirace**
- **Veřejný klíč subjektu**
- **Podpis CA**

ACME (Automatic Certificate Management Environment)

- ACME je systém pro automatické vydávání certifikátů.
- Existují různé klientovské implementace.
- Např. webový server Caddy používá ACME k automatické konfiguraci HTTPS.

ACME (Automatic Certificate Management Environment)

Idea toho, jak ACME funguje:

1. Klient požádá o vydání certifikátu tak, že pošle požadavek, ve kterém je doména (k certifikaci).
2. Server odpoví tím, že dá klientovi náhodnou URL kterou má zpřístupnit.
3. Klient provede změny, co server potřebuje na ověření a odešle potvrzení, že změny provedl.
4. Server ověří, zda-li je daná URL přístupná, pokud je vše v pořádku, vydává certifikát.