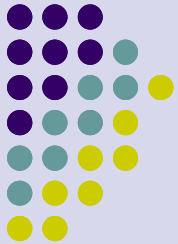
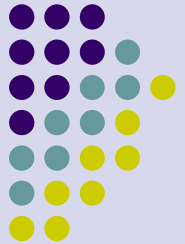
Public Key Infrastructure



Přednášky z Distribuovaných systémů

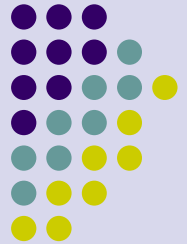
Ing. Jiří Ledvina, CSc.

Úvod



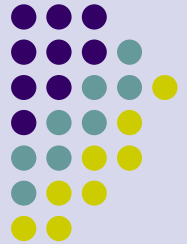
- Infrastruktura pro podporu použití šifrování veřejným klíčem
- PKI zahrnuje
  - Certifikační autority
  - Certifikáty
  - Úložiště pro obnovu certifikátů
  - Metody pro zneplatnění certifikátů
  - Metody pro vyhodnocení řetězu certifikátů od známého veřejného klíče po cílové jméno

Certifikační autorita



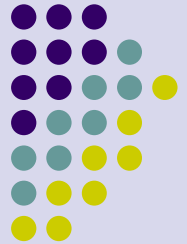
- Důvěryhodná entita, která udržuje seznam veřejných klíčů pro ostatní entity
- CA generuje certifikáty
- CA dovede potvrdit pravost veřejného klíče
- Není třeba komunikovat s vlastníkem veřejného klíče

Certifikát



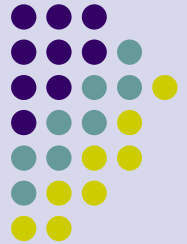
- Certifikát je podepsaná zpráva zaručující, že dané jméno je spojeno s veřejným klíčem
  - Běžně omezeno časově
- Ověření certifikátu se děje na základě znalosti veřejného klíče certifikační autority
- Certifikát může také obsahovat informaci o službách, které držiteli zaručuje

Modely důvěrnosti



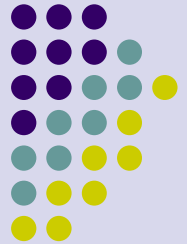
- Monopoly model
- Monopoly plus RA
- Delegování CA
- Oligarchy model
- Anarchy model

Monopoly model



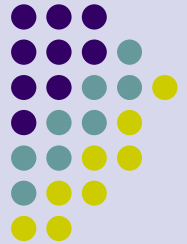
- Jedna CA je důvěryhodná pro všechny
- Všichni musí mít certifikát od této CA
- Veřejný klíč CA je základem důvěry a musí být zahrnut do všeho software i hardware používajícího PKI
- Nevýhoda
  - Neexistuje taková důvěryhodná organizace
  - Pokud takovou vybereme, těžko zvolíme jinou
  - Celý svět by ji využíval (výkonnost, bezpečnost)
  - Neexistovala by soutěž (cena)

Monopoly plus RA



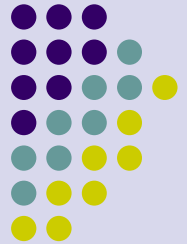
- RA – registrační autorita
- Registrační autority jsou přidružené k jedné CA a je jim důvěřováno
- RA kontrolují identitu uživatelů a poskytují CA odpovídající informaci (identitu a veřejný klíč) při vydávání certifikátů
- výhoda
  - Více míst pro vydávání certifikátů
  - Monopol pro registraci

Delegované CA



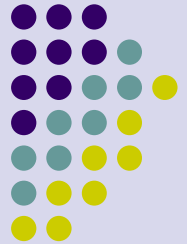
- Kořenová CA vydává certifikáty ostatním CA (delegovaným CA), zaručujíc jejich důvěryhodnost jako CA
- Uživatelé mohou obdržet certifikáty od delegovaných CA jako by to bylo od kořenové CA
- Výhoda – více CA, menší nebezpečí úzkého místa
- Vydávání závisí na jednom CA
- Obtížnější ověřování certifikátu
  - Uživatel musí prohledávat řetěz certifikátů
  - Uspořádání do hierarchie prohledávání ulehčuje

Oligarchy model



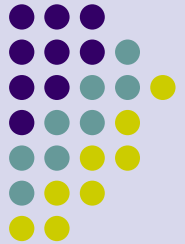
- Existuje několik důvěryhodných CA
- Je akceptován certifikát vydaný kteroukoliv z nich
- Obecně jsou takto konfigurovány web prohlížeče
- Výhoda – konkurence CA
- Snížení bezpečnosti
  - Možnost vložit do seznamu nedůvěryhodnou CA
  - Potřeba chránit více CA před kompromitováním

Anarchy model



- Kdokoliv může podepsat certifikát pro kohokoliv
  - Neexistuje CA nebo seznam CA určený uživatelům
  - Uživatelé si sami určují kdo je důvěryhodný
  - Uživatelé si musí sami nalézt řetězec od důvěryhodné CA k cíli
- Certifikáty mohou být od
  - Zdrojů
  - Subjektů
  - Veřejných úložišť – web serverů
- Výhody
  - Mnoho potenciálních důvěrných kořenů
  - Není třeba zavádět drahou infrastrukturu

Anarchy model

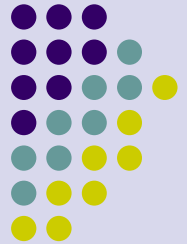


- Bezpečnost
  - Je důvěra tranzitivní
  - Co je to dost dobrá důvěra

Rušení certifikátů

- CA může zrušit certifikát s veřejným klíčem pokud jej uživatel nechce dále používat
- Kompromitování certifikátu
- Náhrada klíče (nový klíč)
- Ukončení členství ve skupině (organizaci)
- Způsoby informování ostatních
  - Broadcast
  - Uložení na veřejném místě
  - Všichni se ptají CA

Revocation list



- CA může periodicky vysílat CRL
  - Podepsaný CA
  - Před použitím certifikátu musí být prohlédnut CRL
  - Nevýhoda – četnost vysílání CRL
  - Nevýhoda počet certifikátů
- Delta CRL
  - Vysílají se pouze změny
  - Podstatně kratší
  - Celý seznam se vysílá méně často
  - Potřeba prohlédnou zěny i celý CRL

On-line Revocation Servers

- ORLS je systém serverů, který může být dotazován na stav jednotlivých certifikátů
- Musí obsahovat celý CRL
- Místo toho by bylo možné udržovat seznam nezrušených certifikátů
- Nevýhoda je v délce seznamu