Elektronický podpis

Základní princip

- Odesílatel
  - podepíše otevřený text
  - vznikne digitálně podepsaný text
- Příjemce
  - ověří zda podpis patří odesílateli
  - uvěří v pravost podpisu
  - ověří zda podpis a text k sobě patří = nebyla zpráva v průběhu přenosu modifikována?

Digitální podpis

- asymetrická kryptografie
- pár klíčů – veřejně publikovaný a soukromý klíč
- po kompromitaci soukromého klíče ztrácí digitální podpisování smysl – nutno zamezit zneužívání klíče
- dig. podpis vytvářen pomocí soukromého klíče
- ověřován pomocí veřejného klíče

Podpis vs. šifrování

- pomocí veřejného klíče se šifruje
- kdokoliv může zprávu zašifrovat (proto se používá veřejný klíč)
- dešifruje se pomocí soukromého klíče
- dešifrovat může pouze oprávněná osoba = majitel soukromého klíče

Jednosměrné funkce

- Nevýhoda asymetrické kryptografie – náročnost na výpočetní kapacity
- jednosměrné funkce – speciální skupina matematických funkcí
  - jednoduché vypočítat hodnotu funkce při daných vstupech
  - v konečném čase prakticky nemožné stanovit původní vstupy z výsledku funkce

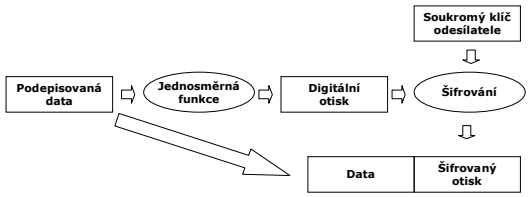
Hashování

- vstup funkce – otevřený text
- výstup funkce – digitální otisk (hash)
- dig. otisk mnohem menší než původní text (řádově stovky bitů)
- funkce zhušťující text = hashovací funkce

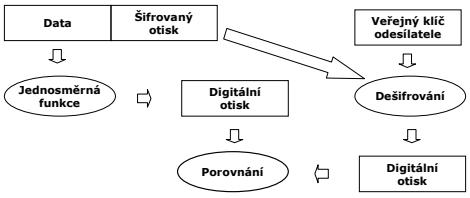
Hashovací funkce

- jednosměrnost
- bezkoliznost – stejný dig. otisk nelze získat z jiné zprávy
- nejpoužívanější algoritmy:
  - MD4 – 128 bitový otisk (má slabiny => 20 bit)
  - MD5 – 128 bit (nekompromitován)
  - SHA1 – 160 bit
- **Pomocí asymetrické kryptografie se šifruje pouze několik stovek bitů !!!**

Vytváření digitálního podpisu



Ověření digitálního podpisu



Cerifikovaný klíč

- při výměně veřejného klíče se může někdo vydávat za jinou osobu
- řešením je certifikace veřejných klíčů
- certifikační autorita – Trusted Third Party
  - příjemce ověří podpis v certifikátu
  - lze přiloženému veřejnému klíči důvěřovat
  - použije klíč k ověření digitálního podpisu vlastní zprávy

Obsah certifikátu

Položka	Popis
ID certifikátu	Jednoznačné sériové číslo
Datum vydání	Kdy byl certifikát vydán
Platnost do	Časové omezení platnosti
Omezení certifikátu	Účel, pro který lze certifikát použít (např. podepisování)
ID certifikační autority	Kdo certifikát vydal
Algoritmy CA	Jaké algoritmy používá pro podepisování certifikační autorita
Veřejný klíč CA	Nemusí být součástí certifikátu
ID vlastníka	Rodné číslo nebo IČO
Veřejný klíč vlastníka	Vlastní certifikovaný klíč
Podpis	Předchozí data jsou podepsána soukromým klíčem CA

Třídy certifikátů

- class 1
  - CA ověří pouze, zda je jméno volné
- class 2
  - identita vlastníka certifikátu ověřena třetí stranou (např. notářsky ověřený formulář žádosti)
- class 3 - standard
  - žadatel musí osobně navštívit CA, kde předepsaným způsobem ověří totožnost
- class 4
  - jako class 3 + prokázání oprávněnost k nějaké činnosti

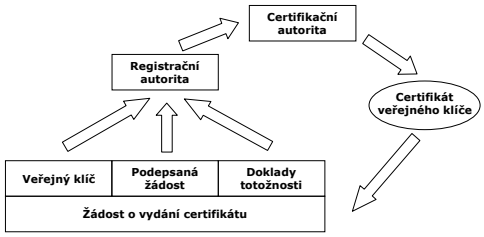
Certifikační autorita

- důvěryhodný subjekt s dostatečnou autoritou
- veřejný klíč (např. na internetu)
- soukromý klíč (střežen jako oko v hlavě) – podepisují se v ním všechny vydávané certifikáty
- ztráta soukromého klíče CA
  - nutnost zneplatnění všech certifikátů
  - vydání nových
  - ztráta dobrého jména

Vydání certifikátu

- příprava žádosti (všechny potřebné identifikační údaje)
- přiloží veřejný klíč
- podepíše příslušným soukromým klíčem (žadatel tím dokazuje, že je vlastníkem soukromého klíče k certifikovanému veřejnému klíči)
  - jinak by bylo možné, že někdo cizí si nechá vystavit certifikát k cizímu páru klíčů, samozřejmě na své jméno
- registrační autorita (pobočky) sbírá a předává žádosti dále do centra CA

Certifikační autorita



Odesílatel

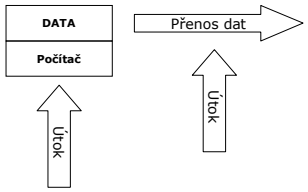
- vypočte digitální otisk z otevřeného textu
- otisk zašifruje svým soukromým klíčem
- zprávu a zašifrovaný otisk odešle příjemci, volitelně přiloží certifikát svého veřejného klíče, volitelně celou zprávu zašifruje

Příjemce

- pokud je třeba, zprávu rozšifruje
- pokud je třeba, získá z veřejného serveru či vlastní databáze certifikát veřejného klíče odesílatele
- ověří osobní údaje uvedené v certifikátu, ověří časovou platnost certifikátu
- ověří, zda certifikát nebyl odvolán
- postupuje po certifikační cestě směrem nahoru (až k důvěryhodné autoritě)
- vypočte digitální otisk z otevřeného textu
- rozšifruje veřejným klíčem odesílatele přiložený elektronický podpis
- obě hodnoty porovná a podle výsledků se dále zařídí

Bezpečná síť

Nebezpečí hrozí počítači připojenému na síť



- Odposlech a modifikace dat
  - Síť = nezabezpečený kanál
- Útoky na připojené počítače
  - Síť umožňuje vzdálený přístup na váš počítač
  - Při útoku zjišťují, které síťové služby na počítači pracují – otevřenost portů
  - Získají informace o protokolech, programech a jejich verzích
  - Pak např. využití známé bezpečnostní chyby

Firewally

- Zabezpečení připojených počítačů
- Vše zakázáno a povoleno jen to co je nezbytně nutné
- Centralizace propojení s vnějším světem = „brána hradu"
- Firewall = „ozbrojená stráž"
- Nainstalovaný a **správně** nakonfigurovaný firewall

Firewall

= sada opatření (HW, SW či personální), která propojují 2 nebo více sítí s různou úrovní důvěryhodnosti.

= SW program na vyhrazeném počítači nebo HW zařízení zapojené mezi chráněnou síť a internet.

- Jednoduchý IP filtr
- Stavový IP filtr
- proxy

Jednoduchý IP filtr

- Blokovač internetového provozu
- Sada pravidel, která zakazují provoz na jednotlivých portech
- Co není zakázáno, je povoleno.
- Nevýhody
  - Nelze analyzovat procházející data
  - Nelze zakazovat či povolovat jejich průchod dle jejich významu

Stavový IP filtr

- V jádře uchovávána tabulka stavů
- Filtr monitoruje síťový provoz a upravuje podle něj tabulku stavů
- Povoluje nebo zakazuje síťový provoz dle nastavených pravidel a stavové tabulky

Proxy

- Program určený pro jeden konkrétní protokol
- Filtruje pakety dle toho, která aplikace a na kterém portu s nimi pracuje
- Jeden program má přístup na daný port a ostatní ho mají zakázzaný.

Demilitarizovaná zóna

- S vnějším světem připojená oblast přes firewall
- Skrze demilitarizovanou nemohou prostupovat žádné síťové pakety
- Segment, který je "viditelný" z každé z obou stran, ale není "průhledný skrz„
- Spojení zajistí proxy

Personální firewally

- Přídavný firewall na každém počítači
- Chrání počítač i před hrozbami z vnitřní sítě
- Obdoba instalace antiviru
- Nemusí se jednat o plnohodnotný firewall
- Nastavení není složité
- Na počátku vše zakázáno a pomocí „žádostí o povolení" se povolí spojení