Digitální podpis

- zásada neodmítnutelnosti odpovědnosti
- zásada integrity
- kryptografické algoritmy pro digitální podepisování
- princip digitálního podepisování
- PKI, CA, RA
- certifikát veřejného klíče
- způsoby uložení podpisových klíčů

Úloha digitálního podpisu

- Pro plnohodnotnou práci s elektronickými dokumenty je potřeba právně správný a ověřitelný digitální nebo chcete-li elektronický podpis.
- Zajistí ověření vaší totožnosti, nebo totožnosti toho, kdo vám dokument poslal (úřad, firma ...)
- Digitální podpis je velmi složitý, zašifrovaný číselný kód, který je pro každého uživatele ojedinělý obdobně jako otisk prstu, a který je právně ověřitelný.
- Podstata digitálního podpisu spočívá v "označkování" elektronického dokumentu, ze kterého je zřejmá nezpochybnitelná identita autora.
- K podepisování dokumentu slouží privátní, tajné klíče. Ke čtení dokumentu a ověření podpisů slouží veřejné klíče.

Zásady bezpečné elektronické komunikace

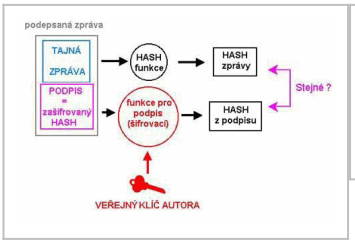
- **Zásada důvěrnosti**
  - Vyjadřuje potřebu uložit data tak, aby jejich obsah mohl přečíst jen ten, komu jsou určena, přičemž kdokoliv další nemá šanci obsah rozluštit ani za pomoci nejmodernějších technologií.
  - Zajišťuje se pomocí šifrování
- **Zásada neodmítnutelnosti odpovědnosti**
  - Vyjadřuje neméně důležitou potřebu možnosti dokázat, kdo je autorem zprávy. Zde nejde o utajení, ale naopak o průkaznost původu dat.
  - Požadavek neodmítnutelnosti odpovědnosti bývá často v praxi splněn digitálním, elektronickým podpisem.
- **Zásada integrity**
  - Má na starosti, aby data došla nejen úplná, ale též prokazatelně nezměněná.
  - Tuto funkci plní HASH

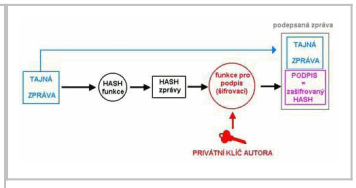
Kryptografie

- Kryptografie je věda, zabývající se šifrováním
  - slouží k ochraně dat před neautorizovaným odhalením
  - může zabránit neautorizovaným modifikacím (změnění) dokumentu

- **Šifrování** je proces, při němž se zpráva (nešifrovaný text) transformuje na jinou zprávu (zašifrovaný text) pomocí matematické funkce a speciálního šifrovacího hesla, tzv. klíče.
- **Dešifrování** je opačný proces: zašifrovaný text se pomocí matematické funkce a klíče převede zpět na text nešifrovaný.

Výtahy zpráv (HASH) a digitální podpisy





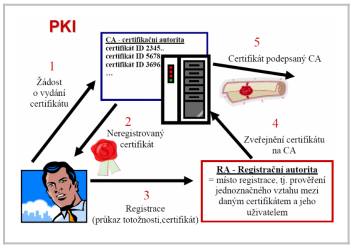
- **Výtahy zpráv** (kryptografický kontrolní součet ☐ HASH) není nic jiného, než číslo – speciální číslo, vytvořené nějakou funkcí, která se jen velmi obtížně invertuje (těžko se provádí pozpátku)
  - **Hashovací algoritmy:**
    - MD5 (128 bitový výtah)
    - SHA (160 bitový výtah)
- **Digitální podpis** (digital signature) je nejčastěji výtah zprávy zašifrovaný něčím privátní klíčem. Tomuto procesu se říká podepsání. Digitální podpis plní funkce, které jsou pro bezpečnost systému důležité:
  - **Integrita** – digitální podpis indikuje, zda nedošlo k modifikaci souboru nebo zprávy
  - **Autentizace** – digitální podpis umožňuje matematicky ověřit, kdo zprávu podepsal
  - **Nepopiratelnost** - jakmile zprávu podepíšete a odešlete, nemůžete nikdy v budoucnu tvrdit, že nejste autorem této zprávy. Nemůžete svou zprávu zapřít, protože byla podepsána vaším privátním klíčem, o němž se předpokládá, že jej vlastníte pouze vy.
  - **Spočívá v šifrování s veřejným klíčem – provozovaném ovšem opačným směrem**
    - Výtah zprávy zašifrujeme svým privátním (**podpisovým**) klíčem a kdokoli ji pak může rozšifrovat klíčem veřejným ☐ tím je zajištěna autentizace, protože se šifruje naším jedinečným podpisovým klíčem
    - **Použitím privátního klíče a funkce pro výtah zprávy vypočítáme digitální podpis odesílané zprávy**
    - Šifruje se pouze otisk zprávy a přikládá se k zašifrované zprávě, protože použitím privátního klíče k zašifrování trvá poměrně dlouho
    - Když příjemce zašifrovanou hodnotu obdrží, může ji dešifrovat veřejným klíčem. Ze vstupního souboru se rovněž snadno vytvoří hashovaná hodnota.
    - Pokud se obě hodnoty shodují, máte jistotu, že jste obdrželi stejnou zprávu, která byla odesílána.

Kryptografické algoritmy pro digitální podpis

V současné době se pro vytváření digitálních podpisů nejčastěji používají:

- Kombinace algoritmu pro výtah zprávy MD5 a kryptografického mechanismu s veřejným klíčem RSA
- Kombinace algoritmu SHA (Secure Hash Function) a ElGamalova mechanismu veřejného klíče – tyto algoritmy dohromady vytvářejí algoritmus DSA (Digital Signature Algorithm).

Certifikáty



Problémem asymetrické kryptografie je způsob, jak ověřit pravost zveřejněných veřejných klíčů. K tomu slouží digitální či elektronický certifikát.

Digitální certifikát obsahuje:

- Uživatelův veřejný klíč
- Uživatelovi popisné údaje (jméno, adresa ...)
- To vše je zašifrováno privátním (podpisovým klíčem)

Veřejný klíč je veřejně známý a je dostupný z nezaměnitelných zdrojů.

Držitelem privátního klíče je tzv. certifikační autorita (v ČR např. PostSignum), tedy instituce nebo útvar, který tyto certifikáty neboli elektronické občanské průkazy vydává. Každý může požádat certifikační autoritu o digitální certifikát.

Certifikáty mají příponu:

- Pro uložení celého certifikátu: **.P12**
- Uložení jednoho certifikátu bez privátního klíče: **.DER**
- Soubor .DER, akorát v textové podobě v Base64 má příponu **.PEM**

Do zpráv se posílá pouze veřejná část certifikátu, podpisový klíč se neposílá a jeho majitel by ho měl chránit (viz. Uložení certifikátů)

- Řešením problému distribuce a uchování veřejných klíčů je tedy využití služeb certifikační autority (tzv. **PKI - Public Key Infrastructure** neboli Infrastruktura veřejného klíče).
- Instituce **CA** (certifikačních autorit) se podobají státním notářům, kteří při vzájemné komunikaci dvou subjektů vystupují jako třetí nezávislý důvěryhodný subjekt. Prostřednictvím jím vydaného certifikátu jednoznačně svazuje identifikaci subjektu s jeho veřejným klíčem a potažmo tedy i s jím vytvořeným digitálním podpisem.
- Certifikáty obsahují ve své nejjednodušší formě veřejný klíč, jméno a další údaje zajišťující nezaměnitelnost subjektů.
- Běžně používané certifikáty též obsahují datum počátku platnosti, datum ukončení platnosti, jméno certifikační autority, která certifikát vydala, sériové číslo a některé další informace.
- Certifikační autorita garantuje jedinečnost subjektů podle užité identifikace subjektu. To je zajištěno legislativními a technickými pravidly provozu instituce certifikační autority. Splnění těchto požadavků potvrdí certifikační autorita podepsáním dokumentu svým privátním klíčem a následným vydáním tohoto certifikátu.

Uložení certifikátů - podpisových klíčů

- v počítači (nedoporučuje se)
- zakryptován pomocí operačního systému (chráněn heslem)
- Hardwarové řešení
  - Čipové karty (i bezkontaktní, chráněna pinem)

- USB Tokeny (iKey)