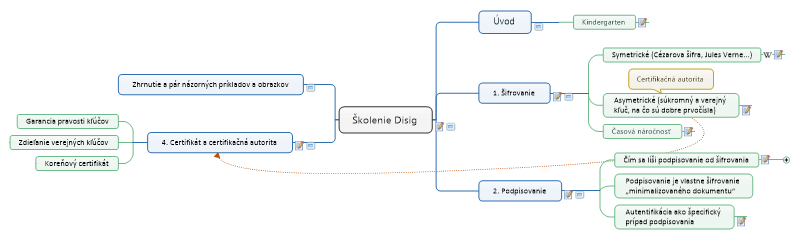
Školenie kluce



Stručný laický úvod do problematiky podpisov, kľúčov, šifrovania a certifikátov

Úvod 1

Kindergarten 1

1. Šifrovanie 1

Symetrické (Cézarova šifra, Jules Verne...) 2

Asymetrické šifrovanie (súkromný a verejný kľuč, na čo sú dobre prvočísla) 2

Časová náročnosť 2

2. Podpisovanie 3

Čím sa líši podpisovanie od šifrovania 3

Otlačok 3

Autentifikácia ako špecifický prípad podpisovania 4

4. Certifikát a certifikačná autorita 4

Garancia pravosti kľúčov 4

Zdieľanie verejných kľúčov 4

Koreňový certifikát 4

Zhrnutie a pár názorných príkladov a obrázkov 4

1. Úvod
   1. Kindergarten

Keď som ešte chodil na MFF tak na prvej prednáške z QM nám profesor Pišút povedal, že hlavne sa nemáme zamýšľať nad filozofickými dôsledkami QM *(hĺbanie nad kvantovou je obľúbené aj u nefyzikov).* Že on nám teraz dá taký ľahký úvodný kurz: Nazýval to **Kindergarten**. Potom o rok trošku viac matematiky i fyziky a za par rokov môžeme začať hĺbať.

Jeho predstava bola taká, že učiť sa treba v špirálach stúpajúcich dohora ako struna a *vedomosti si postupne upevňovať na stále vyššej úrovni*. Týmto sa chcem ospravedlniť všetky, čo vedia o kryptovaní a podpisoch viac ako ja. Účelom tejto prednášky je urobiť takú Kindergarten o kľúčoch, certifikátoch, šifrovaní a podpisoch. *Kindergarten s minimom technických, počítačových alebo právnych a zákonných informácií.*  
  
Skratka ide len o to vysvetliť na čo všetko sa dá použiť šifrovanie. **Lebo základom podpisovania je práve šifrovanie.**

1. 1. Šifrovanie

Digitálny alebo elektronický podpis je technológia založená na šifrovaní. Preto si najprv povieme pár slov o šifrovaní.  
  
Úlohou šifrovania je v prvom rade "znečitateľniť správu" pre neoprávnenú osobu, ale s tým, že oprávnená osoba ju prečítať dokáže. Klasickým príkladom je napríklad Cézarova šifra

* 1. Symetrické (Cézarova šifra, Jules Verne...)

<https://sk.wikipedia.org/wiki/C%C3%A9zarova_%C5%A1ifra>

Asi všetci poznáte ten príbeh, možno budete tvrdiť, že tu nejde o šifrovanie pomocou kľúču ale podstatné je jedno. Šifrujúci i oprávnená osoba musia vlastniť nejakú informáciu alebo predmet pomocou ktorej dokážu správu zašifrovať i odšifrovať. Ak majú šifrujúci i oprávnený rovnaký predmet, pomocné slovo alebo kľúč hovoríme o symetrickom šifrovaní.



V Cézarovej šifre išlo o to, že Cézar písmeno A sa nahradilo písmenom E, B sa nahradilo F-kom. A tak ďalej. Opravnený to urobil naopak. Každe E nahradil písmenom A, miesto F písal B...  
  
Podobne funguje aj tá matica ktorú 2000 rokov neskôr spopularizoval Jules Verne a je známa pod menom Fleissnerova otočná mriežka.



Alebo aj americky film Kod Navaho, kde Američania miesto zložiteho šifrovania povolali do armady ku každej vysielačke jedného Indiana z kmeňa Navaho. Návahovia najprv angličtinu zašifrovali do jazyka navaho, potom odvysielali a ich kamarát na opačnej strane vysielačky použil rovnaký kľúč a spravu dešifroval do angličtiny.

Toto všetko však bol šifrantský pravek, a dnes je šifrovanie úplne inde. Myšlienkovo, matematickým aparátom i technologicky. Ale kľúč ako návod alebo postup pomocou ktorého sa správa znečitateľní a potom opäť sčitateľní tu ostáva. Ibaže máme kľúče dva.

* 1. Asymetrické šifrovanie (súkromný a verejný kľuč, na čo sú dobre prvočísla)

See also: 4. Certifikát a certifikačná autorita

Pokročilejším spôsobom šifrovania je asymetrické šifrovanie kde sa jeden kľúč používa na šifrovanie a druhý na dešifrovanie. Matematicky je to realizované napríklad formou veľkých prvočísiel. To však nie je dôležité, dôležité je to, že kvôli rozlíšeniu sa jeden kľúč nazýva **súkromným (privátnym)** a druhý **verejným**.

***Správa zašifrovaná súkromným kľúčom sa da odomknúť jedine a výhradne spárovaným verejným kľúčom a naopak.***Privátny kľúč by mal ostať pevne v rukách vlastníka, verejne sú k dispozícii všetkým ostatným (*aj na toto šírenie kľúčov slúži certifikačná autorita)*

* 1. Časová náročnosť

Celkom logicky, čím dlhšiu správu alebo dokument chceme šifrovať, tým dlhšie šifrovanie trvá. Tak isto doba šifrovania a dešifrovania rastie so zložitosťou spôsobu šifrovania.

1. 2. Podpisovanie

Úlohou podpisovania dokumentu rukou v reálnom svete je potvrdenie, že osoba čo sa podpísala perom dáva na javo že daný dokument:

* napísala,
* a jeho obsah berie na vedomie
* že v ňom vymenované knihy si požičala...
* a že kym na tomto papierovom dokumente nie su viditeľné znamky dopńania, mazania alebo falšovania súhlasí s jeho obsahom

Ekvivalentom podpisu v digitálnom svete by mohlo byť práve šifrovanie dokumentu, ale pri zvlášť dlhých dokumentoch by to prinášala niekoľko problémov *(napríklad s dobou trvania podpisu).* Niekto šikovný preto vymyslel **digitálne podpisovanie dokumentu** ktoré vychádza s toho, že dokument netreba zašifrovať, stači zariať aby sa dalo zisťiť či dokument nenesie „vidteľné znamky dopńania, mazania falšovania“

* 1. Čím sa líši podpisovanie od šifrovania

Pri elektronickom podpisovaní sa šifruje nejaká skrátená verzia dokumentu nazývana otlačok

* + 1. Otlačok

Táto skrátená verzia dokumentu sa nazýva otlačok *(alebo hash).* Otlačok sa vyvára **nejakým jednoznačne definovaným postupom,** takže pri každom ďalšom robení otlačku je výsledok rovnaký a vznikne taký istý otlačok. Ale pozor, z otlačku nie je možne obnoviť pôvodný dokument.

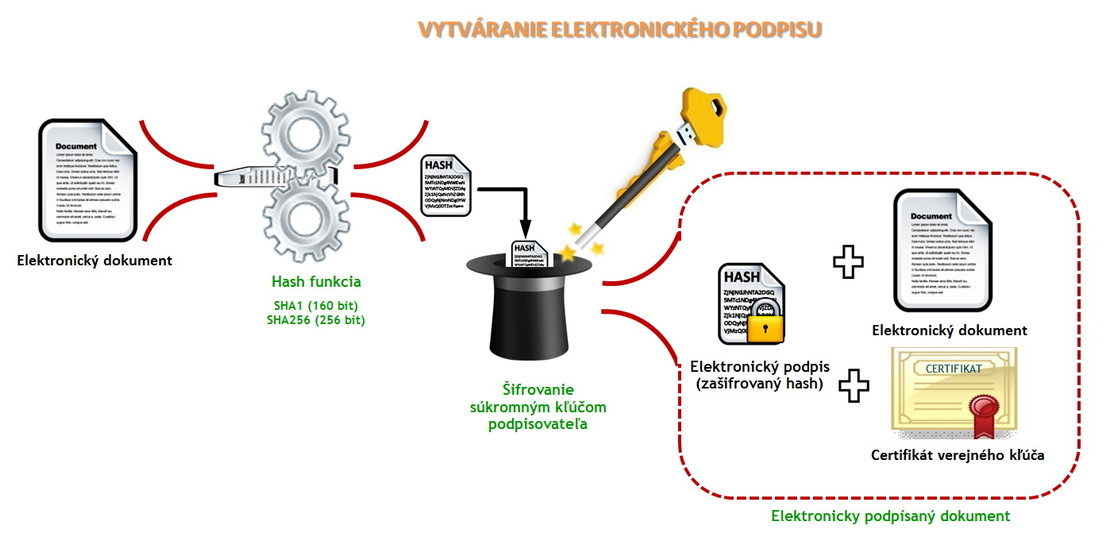
Takto vzniknutý otlačok sa zašifruje privátnym kľúčom podpisujúceho a zašifrovaný sa priloží k pôvodnému dokumentu. Dokument s priloženým otlačkom je považovaný za podpísaný.  


Figure : Ako vzniká elektronicky podpísaný dokument

Čítajúci si potom "podpis" overí tak, že z toho čo má k dispozícii *(dokument a šifrovaný otlačok)* môže vyrobiť **dve verzie otlačku**. Jednu tým, že dešifruje priložený otlačok a druhý že z dokumentu urobí otlačok rovnakým postupom. Ak sa tie dva otlačky zhodujú, dokument sa považuje za podpísaný.

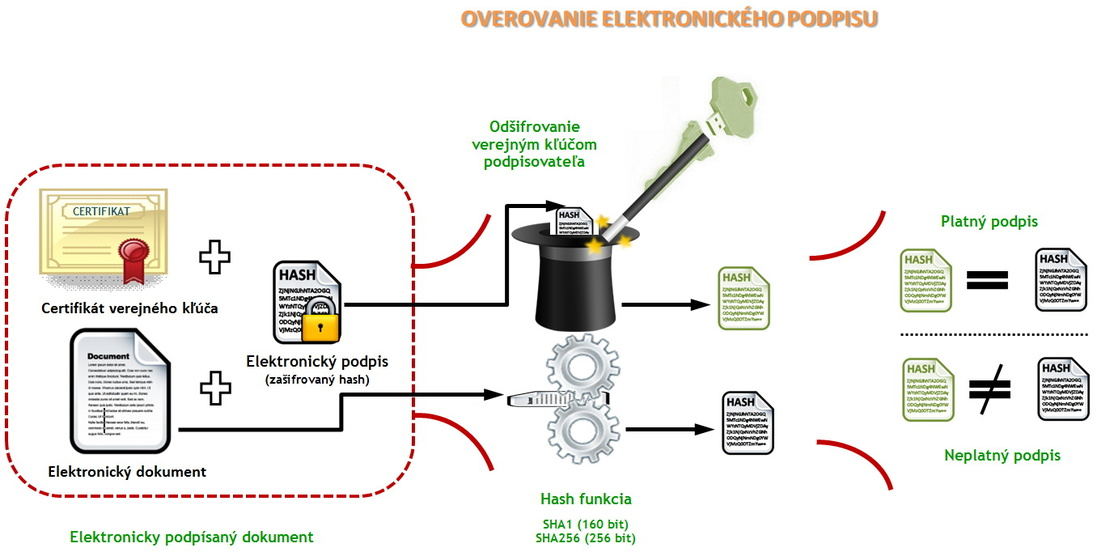


Figure : Overenie podpisu

**Podpisovanie je vlastne šifrovanie „minimalizovaného dokumentu“**

* 1. Autentifikácia ako špecifický prípad podpisovania

Jeden svojský príklad používania podpisu je autentifikácia neznámej osoby. Osobe pošlem malý dokument, táto osoba mi ho podpíše svojim privátnym kľúčom. Ak dokážem verejným kľúčom danej osoby podpis overiť, osobu považujem za autentifikovanú.

1. 4. Certifikát a certifikačná autorita

Kým si šifruje a podpisuje malá uzavretá skupina ľudí, tak si vystačia sami a jediné čo potrebujú je SW na generovanie kľúčových párov. Akonáhle to však treba robiť vo väčšej mierke, tak je potrebne zaistiť, aby si ľudia mali možnosť stiahnuť verejný kľuč, overiť kto kľúčový par vydal, či je kľúčový pár platný, či majiteľ nestratil privátny kľúč....   
  
Celá títo administratíva okolo kľúčových párov je oblasťou ktorú spravujú certifikačné autority.

* 1. Garancia pravosti kľúčov
  2. Zdieľanie verejných kľúčov
  3. Koreňový certifikát

1. Zhrnutie a pár názorných príkladov a obrázkov