Bezpečnosť elektronických dokumentov

Elektronický podpis a PKI

Daniel Olejár

Univerzita Komenského

Marec 2023

Autorské práva

- V prezentácii boli použité
  - príklad hašovacej funkcie `https://en.wikipedia.org/wiki/Cryptographic_hash_function`
  - ilustratívny obrázok podpisovacieho tabletu, uvedený na adrese `https://www.autorentalnews.com/fc_images/articles/l-e-signature-pad-2.jpg`
- Prezentácia je určená predovšetkým pre poslucháčov prednášky Úvod do informačnej bezpečnosti, konanej na FMFI UK v LS 2022/23 a pre ďalších záujemcov o túto problematiku.
- Prezentáciu je možné používať za podmienok CC-BY-NC-ND.

Agenda

- elektronický podpis je dôležitý nástroj na ochranu autentickosti dokumentov
- v porovnaní s minulosťou sa bežne používa v aplikáciách
- občianske preukazy s čipom - e-Government, e-commerce
- potrebujeme poznať princípy a podmienky používania, aby sme zachovali potrebnú úroveň bezpečnosti a od nej odvodenej dôvery

Agenda

V prednáške preberieme

- požiadavky na bezpečnosť dokumentov
- elektronický podpis ako bezpečnostnú funkciu rovnocennú vlastnoručnému podpisu
- kryptografické princípy elektronického podpisu
- Technologické podmienky pre aplikáciu elektronického podpisu
- Bezpečnosť a vierohodnosť elektronicky podpísaných správ
- aplikácie a alternatívy elektronického podpisu
- (legislatíva nariadenie e-IDAS)

Prednáška vznikla podstatným prepracovaním prednášky D.Olejár, J. Janáček Elektronický podpis a PKI

Kontext - písomné dokumenty

- História: informácie sú uchovávané a často aj prenášané v písomnej podobe (údaje v písomnej podobe – písomnosť, dokument)
- Prečo sa používa písomná podoba: relatívna nemennosť obsahu, trvácnosť záznamu, hodnovernosť, právna váha
- Podstatný na dokumente je obsah (=informácia)
- Poznáme základné bezpečnostné požiadavky na ochranu informácie (dôvernosť, integrita, autentickosť, dostupnosť)
- Informácia/obsah dokumentu je spojená s materiálnym nosičom – viaceré vlastnosti dokumentu sú odvodené od spôsobu jeho realizácie (napr. papierový dokument)
- Aj viaceré bezpečnostné funkcie (ktoré realizujú bezpečnostné požiadavky) sú závislé na spôsobe realizácie dokumentu

- V súčasnosti – elektronické dokumenty
- úloha
  Ako zaistiť bezpečnosť elektronických dokumentov na porovnateľnej úrovni ako je zabezpečenie papierových dokumentov?

Informačné procesy

- Dokumenty sú objektom informačných procesov a z toho, akým spôsobom sa spracovávajú, vyplývajú aj hrozby voči nim a bezpečnostné požiadavky na ich ochranu
- Základ informačných procesov: prenos informácie (v priestore – komunikácia alebo v čase - zápis a čítanie informácie)
- Budeme sa zaoberať prenosom informácie v priestore (názornejšie)
- vysielajúca strana (Alica) – prenosový kanál – prijímajúca strana (Bob)
- Kanál môže byť ovplyvnený šumom, alebo k nemu môže mať prístup nepovolaná tretia strana (Eva);
- kanál realizuje transformáciu informácie - kanál (vstupná informácia/údaje, šum, Eva) = výstupná informácia/údaje

Bezpečnostné požiadavky na písomné dokumenty

- Požiadavky na dokument:
  - Nemennosť (prijatý dokument by mal byť totožný s odvysielaným dokumentom - integrita)
  - Utajenie obsahu (nepovolaná osoba–Eva–by sa nemala dostať k obsahu dokumentu - dôvernosť)
  - Určenie autorstva (malo byť jasné, kto dokument vytvoril - autentickosť *)
- Prvé dve požiadavky by sa dali zabezpečiť, ak by bol prenosový kanál spoľahlivý; t.j.
  - Realizoval by identickú transformáciu (informácia pri prenose by sa nemenila)
  - Eva by nemala prístup k prenášanému dokumentu

Bezpečnostné požiadavky na písomné dokumenty

- Tretia požiadavka predpokladá pripojenie znaku jedinečného pre danú osobu (autora dokumentu) k dokumentu
- *) autentickosť zahŕňa aj integritu: dokument je autentický, keď je identický s tým, ktorý autor vytvoril (a autor je jednoznačne určený)
- Realita: absolútne spoľahlivý kanál zatiaľ nemáme k dispozícii (*), dostatočne spoľahlivé kanály sú drahé a majú malú kapacitu
- riešenie: šifrová ochrana proti Eve a samoopravné kódy proti prírode (šumu)
- Autentickosť dokumentu: ochranné znaky, pečate, podpisy v papierovom svete
- (*) kvantové prenosy

Elektronické (virtuálne) dokumenty

- čo to je?
  = Dokumenty (údaje) v elektronickej alebo optickej podobe, ktoré nie sú pevne viazané na nosič (zaznamenané na elektromagnetických médiách, prenášané sieťami, prostredníctvom satelitov, dokumenty v pamäti počítača)
- používajú sa lebo objem informácií, ktoré spoločnosť na svoje fungovanie potrebuje, nie je zvládnuteľný klasickými prostriedkami
- koexistencia papierového a elektronického sveta
- Životný cyklus dokumentov: informácia sa transformuje z papierovej do elektronickej podoby, spracovanie v elektronickej podobe a potom spätná transformácia (tlač)
- papierová fáza je drahá a pomalá - snaha vylúčiť ju
- Elektronická forma dokumentu rovnocenná s papierovou
- cieľový stav prevládajúca elektronická forma

Čo vlastne je dokument?

- snaha o zovšeobecnenie pojmu dokument, aby nezáležal od konkrétnej realizácie dokumentu
- ide o možnosť transformácie dokumentu z jednej formy do druhej (s rovnakými bezpečnostnými zárukami a právnymi účinkami)
- Zákon o elektronickom podpise: dokument = *ľubovoľná konečná neprázdna postupnosť znakov nad nejakou konečnou abecedou*
- poslanci odmietli definovať abecedu
- NBÚ v anglickej verzii preložilo "neprázdnu postupnosť" ako "nonzero sequence"
- o čo išlo v definícii: možnosť jednoznačne priradiť dokumentu číselnú hodnotu (číslo, alebo postupnosť čísel)
- neuvažovali sme obsah a formát
- to sme museli riešiť vo vyhláškach

Definícia dokumentu

Dokument je usporiadaná pätica

- informačný obsah (zaznamenaný v podobe údajov)
- formát (konvencia, ako interpretovať údaje)
- bezpečnostné mechanizmy (ochranné prvky na zaistenie dôvernosti, integrity, autentickosti, prípadne iných bezpečnostných požiadaviek kladených na dokument)
- úroveň bezpečnostných záruk (závisí od výberu bezpečnostných mechanizmov a ich sily, danej napríklad kryptografickými algoritmami a dĺžkou kľúčov, použitými protokolmi, životnosťou certifikátov a pod.)
- realizácia (fyzická realizácia dokumentu: papierový, súbor uložený v pamäti, prenášaný komunikačným kanálom prostredníctvom signálov a pod.)

Prečo takáto definícia dokumentu?

- problém bol s konverziou z jednej formy do druhej
- formulácia *celý dokument sa z formy A transformuje do formy B* bola problematická, lebo
  - ako sa transformuje papier do elektronickej formy?
  - ako sa overí korektnosť transformácie?
  - čo s bezpečnostnými prvkami špecifickými pre jednu formu (vlastnoručný podpis na papieri) ale nerealizovateľnými v inej forme?
- transformujeme obsah
- korektnosť transformácie overujeme spätnou transformáciou (zložením konverznej transformácie a spätnej transformácie by sme mali dostať identickú transformáciu)

Prečo takáto definícia dokumentu?

- pri konverzii zachovávame bezpečnostné požiadavky na dokument
  - konkrétne ktoré (CIA)
  - na akej úrovni
- bezpečnostné mechanizmy z formy A dokumentu nahrádzame ekvivalentnými bezpečnostnými mechanizmami, ktoré zaisťujú naplnenie bezpečnostnej požiadavky na dokument vo forme B úroveň bezpečnostných požiadaviek vo forme B nesmie byť nižšia ako vo forme A

Výhody a nevýhody elektronických dokumentov

- vráťme sa k elektronickým dokumentom (digitálne kódované, realizované pomocou elektromagnetických fyzikálnych veličín/signálov)
- výhody
  - Veľké množstvo informácií na malom priestore (vysoká koncentrácia informácií)
  - Jednoduchá možnosť modifikácie údajov
  - Rýchle a nepozorovane sa dajú kopírovať
  - Rýchly prenos na veľké vzdialenosti
- nevýhody
  - Veľké množstvo informácií na malom priestore (vysoká koncentrácia informácií)
  - Jednoduchá možnosť modifikácie údajov
  - Rýchle a nepozorovane sa dajú kopírovať
  - Rýchly prenos na veľké vzdialenosti

Bezpečnostné požiadavky na elektronické dokumenty

- Výhody prevažujú nad nevýhodami, elektronické dokumenty sa budú používať;
- bezpečnostné problémy treba riešiť
  - Dôvernosť (confidentiality)
  - Integrita (integrity)
  - Dostupnosť (availability)
  - Autentickosť (authenticity)
  - Zodpovednosť (accountability)
  - Súkromie (privacy)
  - Nepopretie pôvodu (nonrepudiation of origin)
  - Nepopretie prijatia (nonrepudiation of receipt)
  - a ďalšie

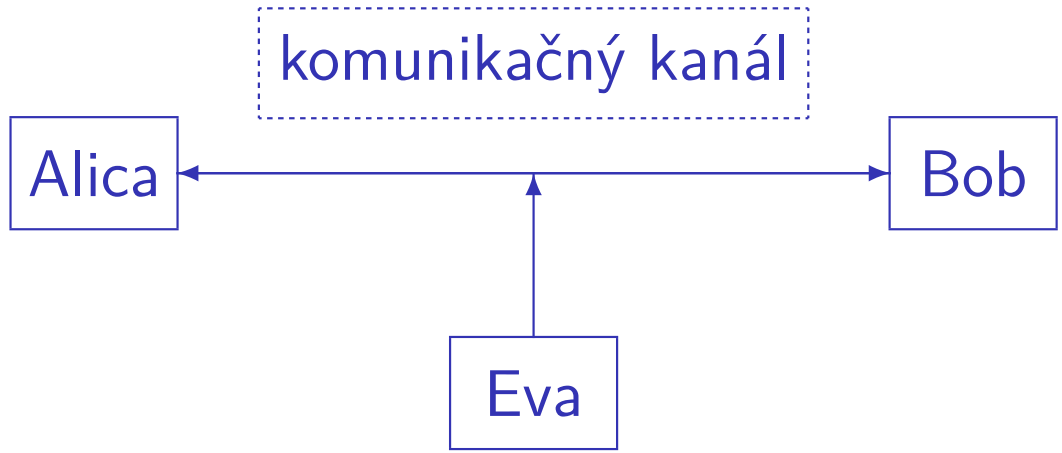
- Univerzálne, jednorazové riešenie informačnej bezpečnosti nexistuje
- Riešenia - kombinované:
  - Organizačné (jasné stanovenie práv a povinností, ochrana prístupu k informačnému systému,...)
  - Právne (legislatíva: elektronický podpis, elektronický obchod, ochrana osobných údajov, ochrana utajovaných skutočností,... , ale aj vnútorná legislatíva)
  - Technické (ochrana infraštruktúry, technické zabezpečovacie prostriedky, zálohovanie,...)
  - Normy a štandardy (kompatibilita a kvalita riešení)
  - Kryptológia

- Dôvernosť, integrita, autentickosť, nemožnosť popretia pôvodu sa dajú riešiť pomocou kryptologických prostriedkov
- Nepriamo sa kryptologické riešenia využívajú aj pri ochrane súkromia, zodpovednosti za činnosť v systéme, nemožnosti popretia prijatia a ďalších bezpečnostných problémov

Kryptologické minimum (1)

- *poslucháči, ktorí majú základné vedomosti z kryptológie, môžu túto časť prezentácie preskočiť*
- **začiatok skoku** $\Rightarrow$
- Vychádzajme z modelovej situácie: Alica chce poslať Bobovi nejakú správu prostredníctvom prenosového kanálu, na ktorého spoľahlivosť sa nemôže spoľahnúť
- Alica a Bob sú oprávnené osoby (oprávnení účastníci komunikácie)
- Eva (= protivník) môže odvysielanú správu zachytiť a pokúsiť sa prečítať, modifikovať, poslať príjemcovi zachytenú správu oneskorene, alebo ešte raz, poslať mu modifikovanú správu, predstierať Bobovi, že je Alica a voči Alici vystupovať ako Bob a pod.

- poznámka Eva je eavsdropper (pasívny odpočúvateľ), niekedy sa zavádza aj Mallory (malicious oponent, aktívny protivník) ktorý aktívne zasahuje do komunikácie. My vystačíme s Evou, ktorej povolíme aj aktívne zasahovanie do komunikácie Alice a Boba



Kryptologické minimum (2)

- Správa = dokument, ktorý posiela Alica Bobovi alebo Bob Alici,
- predpokladáme, že je v textovej podobe (nad dohodnutou abecedou A)
- Ak je správa v čitateľnej podobe, hovoríme, že ide o otvorený text, cleartext.
- Konkrétnu (otvorenú) správu označíme m (message), množinu všetkých možných otvorených správ symbolom M
- formálne $m \in A^+; M = A^+$.
- Kryptografická transformácia = zobrazenie (predpis), ktorý jednoznačne transformuje ľubovoľný text
- Kryptografická transformácie má dva parametre (vstupné hodnoty) = text a kryptografický kľúč $k \in K$ kryptografický kľúč môže byť opäť slovo nad nejakou abecedou, pre naše účely stačí, keď ako kľúče budeme uvažovať prirodzené čísla z množiny K

Kryptologické minimum (3)

- Množina kryptografických kľúčov K musí byť dostatočne veľká, aby sa nedali prebrať všetky možnosti
- Rozlišujeme dve kryptografické transformácie:
  - Šifrovaciu
    $$E : M \times K \rightarrow C$$
  - Dešifrovaciu
    $$D : C \times K \ toM$$
- Množina C je množina všetkých šifrových textov (ciphertexts), predpokladáme, že $C \subseteq A^+$.
- Šifrovacia transformácia na základe kryptografického kľúča (šifrovacieho kľúča k_1) transformuje správu m na šifrový text c

$$E(m, k_1) = c$$

Kryptologické minimum (4)

- Dešifrovacia transformácia D šifrový text (šifrovú správu) c pomocou kryptografického (dešifrovacieho) kľúča k_2 dešifruje na pôvodnú správu m:

$$D(c, k_2) = m$$

- Kľúče k_1, k_2 tvoria dvojicu a v mnohých šifrovacích systémoch $k_1 = k_2$ (na chvíľu budeme predpokladať, že skutočne $k_1 = k_2$)
- množinu dvojíc transformácií (šifrovacích a dešifrovacích)

$$E : M \times K \to C; \quad D : C \times K$$

takých, že

$$\forall m \forall k \left((m \in M \& k \in K) \Rightarrow D(E(m, k), k) = m \right)$$

budeme nazývať kryptosystémom.

- formálne z matematického hľadiska je teda kryptosystém (šifra) usporiadaná štvorica $(M, C, K, (E, D))$, ale postačí nám aj menej formálna definícia
- Kryptosystém, v ktorom sa zhoduje šifrovací a dešifrovací kľúč, sa nazýva *symetrický kryptosystém*
- Príklad: substitučná šifra. Abeceda A je anglická abeceda (otvorené texty zapisujeme pomocou malých písmen, šifrové pomocou veľkých písmen)
- kľúčom je permutácia ϕ písmen anglickej abecedy, množinou kľúčov je množina všetkých možných permutácií písmen (tých je 26!), C, M sú všetky konečné reťazce znakov anglickej abecedy (M môžeme obmedziť na množinu postupností slov)

Kryptologické minimum (7)

- šifrovanie otvoreného textu spočíva v nahradení každéhoho písmena otvoreného textu x znakom $phi(x)$
- pri dešifrovaní nahrádzame znak Y šifrového textu znakom $\phi^{-1}(Y)$ otvoreného textu

a	b	c	d	e	f	g	h	i	j	k	l	m
W	C	U	S	T	F	D	M	E	P	V	A	X
n	o	p	q	r	s	t	u	v	w	x	y	z
R	Y	I	G	H	L	N	Z	Q	J	B	O	K

Table: Šifrovacia tabuľka (kľúč) substitučnej šifry

Kryptologické minimum (8)

- Ako použijú Alica s Bobom klasický symetrický kryptosystém na utajenie obsahu svojej komunikácie pred Evou?
- Alica sa stretne s Bobom a dohodnú sa na kryptosystéme a na kľúči, ktorý budú na šifrovanie/dešifrovanie používať.
- Musia predpokladať, že Eva má prístup ku komunikačnému kanálu a že sa po čase dozvie, aký kryptosystém používajú
- Jedinou zárukou dôvernosti ich komunikácie je, že sa Eva nedozvie ich kľúč (tajný kľúč).
- Alica a Bob si posielajú správy šifrované dohodnutým tajným kľúčom, ktoré pomocou neho aj dešifrujú

A čo Eva?

- Ak nepozná tajný kľúč, môže skúsiť zistiť obsah komunikácie Alica-Bob analýzou zachytených šifrových textov, využijúc ďalšie informácie, ktoré sa jej podarilo získať (napr. použitý textový editor)
- Evina činnosť = kryptoanalýza, Eva = kryptoanalytička
- Pokus o odhalenie obsahu šifrovej správy = kryptoanalytický útok
- Existuje viacero typov kryptoanalytických útokov, nebudeme ich rozoberať

Kryptologické minimum (10)

- Úplné preberanie (kľúčov, otvorených textov)
- Existujú absolútne bezpečné kryptosystémy (Vernamova šifra)
- Ďalšie sú dostatočne bezpečné (nie je známa metóda kryptoanalýzy, ktorá by v rozumnom čase, s vynaložením rozumného množstva peňazí a technických prostriedkov umožnila šifrový text rozbiť)
- Kryptografia = veda o návrhu kryptosystémov
- Kryptoanalýza = veda o rozbíjaní kryptosystémov (lúštení šifrových textov)
- Kryptológia = kryptografia + kryptoanalýza
- $\Leftarrow$ koniec skoku
- ak vás kryptológia zaujíma, choďte si pozrieť prednášku Martina Staneka

Asymetrické kryptosystémy (1)

- Klasické kryptosystémy: šifrovací kľúč = dešifrovací kľúč
- 1976 Diffie a Helmann: idea kryptosystému, v ktorom šifrovací kľúč $\neq$ dešifrovací kľúč, naviac jeden sa z druhého nedá ľahko odvodiť
- Odvtedy okolo 10 kryptosystémov, ktoré tento princíp používajú
- Ako sa to dá použiť?
  - Alica chce dôverne komunikovať s Bobom, ale nemôžu sa stretnúť, aby sa dohodli na tajnom kľúči
  - Alica si vygeneruje dvojicu (šifrovací a dešifrovací) kľúč pre asymetrický kryptosystém a šifrovací kľúč $k_{Alice,public}$ zverejní (!), dešifrovací kľúč $k_{Alice,private}$ utají
  - Preto sa zverejnený šifrovací kľúč nazýva verejným (public) kľúčom a utajený dešifrovací kľúč súkromným (privátnym) kľúčom

Asymetrické kryptosystémy (2)

- Bob si taktiež vygeneruje dvojicu kryptografických kľúčov $k_{Bob,private}$, $k_{Bob,public}$, a zverejní svoj verejný kľúč $k_{Bob,public}$,
- Alica bude teraz posielať Bobovi správy šifrované Bobovým verejným kľúčom $k_{Bob,public}$, Bob si ich bude dešifrovať pomocou svojho súkromného kľúča $k_{Bob,private}$
- Bob bude posielať Alici správy šifrované Aliciným verejným kľúčom $k_{Alice,public}$ a ona si ich bude dešifrovať pomocou svojho súkromného kľúča $k_{Alice,private}$
- Ak by aj Eva zachytila šifrovú správu, keďže nemá k dispozícii dešifrovací (súkromný) kľúč adresáta, správu nemôže dešifrovať a musí sa pokúsiť o kryptoanalýzu
- Kryptografické transformácie tvoriace asymetrický kryptosystém (kryptosystém s verejnými kľúčmi) sú veľmi zložité a v porovnaní so symetrickými kryptosystémami výpočtovo náročné

Asymetrické kryptosystémy (3)

- Bežne sa nepoužívajú na šifrovanie celých správ Šifrujú sa nimi kryptografické kľúče pre symetrické kryptosystémy (kľúče na správu)
- na ilustráciu uvedieme najznámejší asymetrický šifrovací systém RSA (Rivest, Shamir Adleman) v minimalistickom prevedení
- podrobný popis nájdete v ľubovoľnej učebnici kryptológie, stručný vo Wikipédii

- varovanie - táto časť je intelektuálne náročná a poznatky uvedené v nej sa v ďalšom výklade nevyužívajú a možno ju preskočiť
- **začiatok skoku** $\Rightarrow$
- algoritmus sa zakladá na modulárnom umocňovaní (prirodzené číslo sa umocní na kladný celočíselný exponent a vydelí kladným celočíselným modulom, výsledkom je zvyšok po delení modulom)
- existujú také prirodzené čísla e, d, n, že pre každú správu m; kde správy sú reprezentované celými číslami a $0 \leq m < n$ platí

$$(m^e)^d = m \mod n$$

- verejný a súkromný kľúč sú trocha zložitejšie ako v definícii poďme hľadať kľúče:

RSA

- nájdeme dve rôzne prvočísla p, q, ktoré utajíme
- vypočítame súčin $n = pq$
  - n je modul aj pre súkromné aj pre verejné kľúče, určuje dĺžku kľúča
  - n je súčasťou verejného kľúča
- vypočítame $\lambda(n) = (p-1)(q-1)$ a utajíme ho
- zvolíme e také, že $1 < e < \lambda(n)$ $\gcd(\lambda(n), e) = 1$ a zverejníme ho (exponent verejného kľúča)
- vypočítame $d = e^{-1} \mod \lambda(n)$; d je exponent súkromného kľúča

kľúče:

- verejný: n, e
- súkromný: d.
- parametre $p, q, \lambda(n)$ už nepotrebujeme, ale nesmú sa zverejniť, lebo by sa dal vypočítať tajný kľúč, d.

- $p = 17, q = 19$
- $n = 323$
- $\lambda(n) = 288$
- $e = 5$
- $d = 173 = (10101101)_2$
- môžeme šifrovať čísla $0 \leq m < 232$ vybrali sme číslo 23
- **šifrovanie**: počítame $23^5 \mod 323$

i	$23^i \mod 323$
1	23
2	206
4	123

$$23^5 \mod 323 = 23 \times 123 \mod 323 = 245$$

dešifrovanie:

i	$245^i \mod 323$
1	245
2	270
4	225
8	237
16	290
32	120
64	188
128	137

teraz vypočítame $245^{173} \mod 323$ (pomocou binárneho vyjdrenia exponentu $173 = (10101101)_2$:

$$245 \times 225 \times 237 \times 120 \times 137 \mod 323 = 23.$$

$\Leftarrow$ koniec skoku

Digitálny podpis

- Prekvapujúci nápad – použiť asymetrický kryptosystém „naopak“ – šifrovať pomocou súkromného kľúča a dešifrovať pomocou verejného
- Čo to umožňuje:
  - Len držiteľ súkromného kľúča je schopný šifrovania
  - Každý, kto má k dispozícii verejný kľúč, je šifrovú informáciu schopný dešifrovať
- použitie: autentifikácia, digitálny podpis
- Doteraz sme pomocou kryptografie riešili dôvernosť správ
- teraz: autentickosť a integritu a od nich odvodené bezpečnostné požiadavky
- Hľadáme analógiu vlastnoručného podpisu pre elektronické dokumenty = „elektronický podpis“

Ideálne funkcie podpisu

- Zatiaľ budeme pod pojmom elektronický podpis rozumieť bližšie neurčenú analógiu vlastnoručného podpisu dokumentu v elektronickej podobe
- Pozrieme sa na funkcie vlastnoručného podpisu a na požiadavky, ktoré by jeho elektronická analógia mala spĺňať
- Funkcia vlastnoručného podpisu: vyjadrenie súhlasu podpísanej osoby s obsahom dokumentu
- vlastnosti (ideálne)
  - nefalšovateľnosť
  - neprenositeľnosť na iný dokument
  - možnosť zistiť dodatočnú zmenu obsahu dokumentu
  - identifikácia podpisovateľa

Špecifiká elektronických dokumentov

Pripomenieme špecifiká elektronických dokumentov relevantné pre vytváranie elektronickej analógie vlastnoručného podpisu:

- nie je možné odlíšiť kópiu elektronického dokumentu od originálu
- elektronické dokumenty je možné ľahko upravovať
- jednoducho možno preniesť časť jedného elektronického dokumentu do iného

Nutné požiadavky na „elektronický“ podpis

- na jeho vytvorenie musí byť potrebná nejaká tajná informácia
- to znamená, že ho môže vytvoriť len ten, kto túto informáciu pozná
- musí závisieť od obsahu dokumentu
- lebo inak by sa dal prenášať z jedného dokumentu na iný a nedala by sa zistiť zmena dokumentu
- každý, kto to potrebuje, ho musí byť schopný skontrolovať

pojem zaviedla Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

(4) Electronic communication and commerce necessitate " electronic signatures" and related services allowing data authentication; *divergent rules with respect to legal recognition of electronic signatures and the accreditation of certification-service providers in the Member States may create a significant barrier to the use of electronic communications and electronic commerce; on the other hand, a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies; legislation in the Member States should not hinder the free movement of goods and services in the internal market;*

- *"electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;*
- *2. "advanced electronic signature" means an electronic signature which meets the following requirements:*
  (a) it is uniquely linked to the signatory;
  (b) it is capable of identifying the signatory;
  (c) it is created using means that the signatory can maintain under his sole control; and
  (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

`https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093`

Elektronický vs. digitálny podpis

- elektronický podpis = všeobecný pojem označujúci informáciu, ktorá spĺňa stanovené požiadavky Direktívy
- slúži ako metóda autentifikácie údajov (ale pojem autentifikácie nebol v Direktíve definovaný)
- pokročilý elektronický podpis: autentickosť dokumentu a identifikácia podpisovateľa
- digitálny podpis = konkrétny kryptologický prostriedok, ktorý sa využíva na realizáciu elektronických podpisov (v súčasnosti jediný známy spôsob ako stanovené požiadavky splniť)
- pracovne budeme používať pojmy elektronický a digitálny podpis ako synonymá

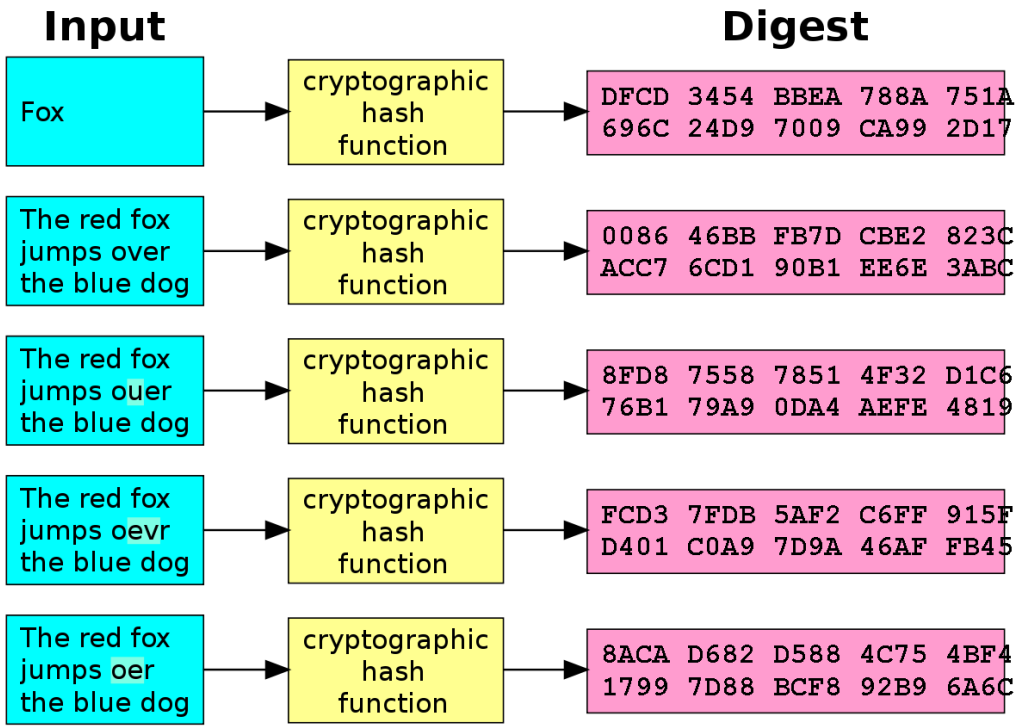
Princíp digitálneho podpisu (1)

- Pripomenieme „obrátené“ použitie kľúčov asymetrického šifrovacieho systému:
  - Súkromný na šifrovanie a verejný na dešifrovanie
  - Keďže šifrový text je schopný vytvoriť len držiteľ súkromného kľúča, ale overiť každý, ktorý má prístup k verejnému kľúču, môže zašifrovaný rozumne vybratý text predstavovať digitálny podpis dokumentu
- Čo šifrovať?
  - text, ktorý sa šifruje, by mal nejako súvisieť s dokumentom, pre ktorý sa digitálny podpis vytvára
  - Tento text by nemal byť príliš dlhý, lebo asymetrické šifrovanie je zložité a šifrovanie dlhého textu by mohlo trvať dlho
  - Riešenie: hašovacia hodnota (digitálny odtlačok) dokumentu

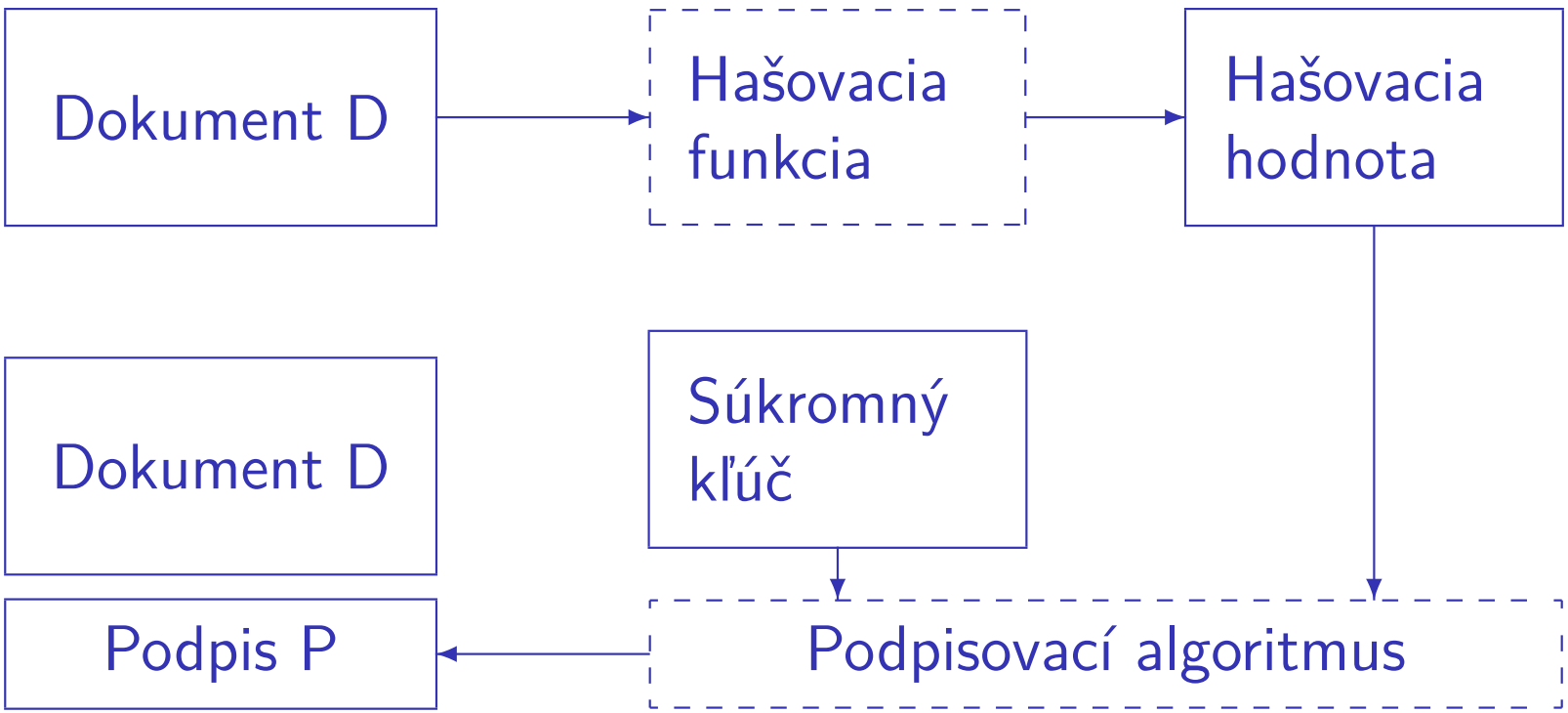
Hašovacia funkcia

- Funkcia, ktorá textu ľubovoľnej konečnej dĺžky priradí číslo pevnej dĺžky (hašovaciu hodnotu)
- Naviac, musí mať nasledujúce vlastnosti:
  - Pre ľubovoľnú správu/dokument sa hašovacia hodnota počíta ľahko
  - Pre hašovaciu hodnotu je ťažké nájsť správu, ktorá sa na ňu transformuje
  - Je ťažké nájsť dve rozličné správy s rovnakou hašovacou hodnotou
- Digitálny podpis sa potom pre danú správu počíta tak, že sa súkromným kľúčom podpisovateľa zašifruje hašovacia hodnota dokumentu (pozri nasledujúci obrázok)

Príklad hašovacej funkcie



Vytváranie digitálneho podpisu

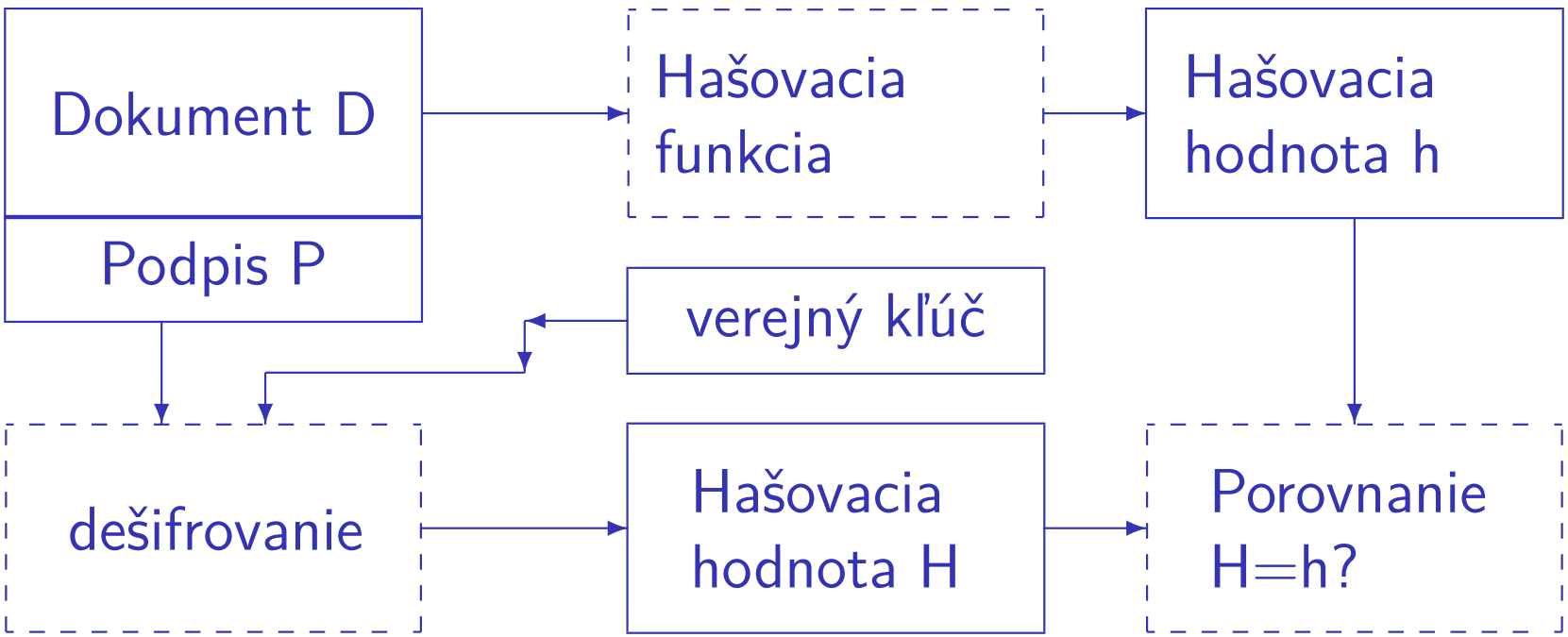


Subject: Podpisana sprava
Content-Type: multipart/signed;
protocol="application/x-pkcs7-signature";
micalg=sha1;
boundary="————ms6F9AFCDB3150C4CB33D9D648"
This is a cryptographically signed message in MIME format.
————ms6F9AFCDB3150C4CB33D9D648
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Tento text je elektronicky podpisany. Ak by ho niekto zmenil, prijemca by to zistil.
————ms6F9AFCDB3150C4CB33D9D648
Content-Type: application/x-pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature

Príklad digitálne podpísanej správy

MIIG7gYJKoZIhvcNAQcCoIIG3zCCBtsCAQExCzAJBgUrDgMCGgUAMA
BHYwggRyMIID26ADAgECAgECMA0GCSqGSIb3DQEBBAUAMIHfMQ
A1UECBMIU2xvdmFraWExEzARBgNVBAcTCkJyYXRpc2xhdmExRDBC
TWF0aGVtLiwgUGh5cy4gYW5kIEluZm9ybWF0aWNzLCBDb21lbml1cy
JQYDVQQLEx5EZXBhcnRtZW50IG9mIENvbXB1dGVyIFNjaWVuY2Ux
... SIb3DQEJARYZamFuYWNla0BkY3MuZm1waC51bmliYS5zawIBAjA
CSqGSIb3DQEJAzELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XD
lwYJKoZIhvcNAQkEMRYE-
FLlviSXJMge9Yzook1+gDhhXxQifMFIGCSqGSIb3DQEJDzFFMEMw
CCqGSIb3DQMCAgEoMA0GCSqGSIb3DQEBAQUABIGA0HVIVwURVZ
YKLFOaIvr4das+udU4ODG4y9g5gOPsKXlg7uph9lyr9wbmD7pQQxcJCe
aEStU0ZKLXwnJ+CNVRbq6EOTYG3sLHlX47EpeLSX41mpxu9EdMlDY
————ms6F9AFCDB3150C4CB33D9D648–

Overovanie digitálneho podpisu



Prečo to funguje?

- na vytvorenie podpisu je potrebná znalosť súkromného kľúča
  - Nikto okrem podpisovateľa (Alice) nepozná Alicin súkromný kľúč
  - Ak by Eva chcela vytvoriť Alicin digitálny podpis, musela by napr. z Alicinho verejného kľúča odvodiť jej súkromný kľúč, čo je teoreticky možné, ale prakticky nerealizovateľné

  pomocou verejného kľúča sa dá spoľahlivo overiť, či sa predložený dokument zhoduje s originálom (tým, ku ktorému bol vytvorený podpis použitím zodpovedajúceho súkromného kľúča)
- Tu sa zasa využívajú vlastnosti hašovacej funkcie: akákoľvek zmena dokumentu sa s vysokou pravdepodobnosťou prejaví v hašovacej hodnote dokumentu

Porovnanie digitálneho podpisu s ideálnym

- Ak je súkromný kľúč utajený a verejný kľúč je overovateľovi známy, tak digitálny podpis
  - je nefalšovateľný,
  - je neprenositeľný na iný dokument,
  - umožňuje zistiť dodatočnú zmenu v dokumente.
- Čo ešte chýba:
  - bezpečná distribúcia verejných kľúčov,
  - identifikácia podpisovateľa
- riešenie: certifikát verejného kľúča a PKI

Certifikát verejného kľúča

- je elektronický dokument, ktorým jeho vydavateľ potvrdzuje, že v certifikáte uvedený verejný kľúč patrí osobe (príp. inému subjektu), ktorej identifikačné údaje (meno) sú tiež v certifikáte uvedené (držiteľ certifikátu),
- vydáva ho dôveryhodná tretia osoba, certifikačná autorita,
- umožňuje riešiť problém bezpečnej distribúcie verejných kľúčov a identifikáciu podpisovateľa
- Formát certifikátu upravuje štandard X509

Obsah certifikátu

- identifikačné číslo certifikátu
- identifikačné údaje vydavateľa certifikátu
- identifikačné údaje držiteľa certifikátu
- dátum a čas začiatku a konca platnosti certifikátu
- verejný kľúč držiteľa certifikátu
- identifikáciu algoritmov, pre ktoré je kľúč určený
- elektronický podpis certifikačnej autority

Ďalšie údaje uvedené v certifikáte

- obmedzenie použitia páru kľúčov, ku ktorému je certifikát vydaný
- obmedzenie použitia certifikátu obmedzenie zodpovednosti za použitie elektronického podpisu overeného na základe tohto certifikátu
- informácie o možných spôsoboch overenia pravosti a platnosti certifikátu

Ako plní certifikát verejného kľúča svoje funkcie

- Spojenie osoby podpisovateľa s verejným kľúčom:
  - Podpisovateľ je jediným držiteľom súkromného kľúča
  - Súkromný kľúč tvorí dvojicu s verejným kľúčom
  - CA pri vydávaní certifikátu si overila totožnosť osoby, uvedenej v certifikáte
  - CA si overila, či žiadateľ o certifikát pozná súkromný kľúč prislúchajúci k verejnému kľúču uvedenému v certifikáte
- Certifikát podpísala CA, t.j. digitálny podpis CA zaručuje integritu a autentickosť certifikátu

Overenie digitálneho podpisu pomocou certifikátu

- Alica posiela Bobovi digitálne podpísanú správu. K správe pripojí aj certifikát svojho verejného kľúča, ktorý použila na vytvorenie digitálneho podpisu
- Bob z certifikátu verejného kľúča vyberie verejný kľúč a použije ho na overenie digitálneho podpisu správy
- Ak sa zhodujú obe hašovacie hodnoty (vypočítaná a dešifrovaná), digitálny podpis je overený
- V čom je problém?
  Eva by si mohla vyrobiť falošný certifikát Alicinho verejného kľúča a potom mohla Bobovi podsunúť fingovanú správu podpísanú v Alicinom mene

Overenie platnosti certifikátu

- Aby sa Bob mohol spoľahnúť na verejný kľúč obsiahnutý v certifikáte, musí overiť platnosť certifikátu:
  - Či bol platný v čase vytvorenia Alicinho digitálneho podpisu
  - Či ho vydala CA, ktorá je ako vydavateľ certifikátu uvedená
  - Či certifikát nebol modifikovaný
  - Či certifikát nebol zrušený
- Kľúčové pre overenie platnosti certifikátu je overenie digitálneho podpisu vydavateľa certifikátu (certifikačnej autority) na certifikáte. To predpokladá, že Bob má k dispozícii z dôveryhodného zdroja verejný kľúč certifikačnej autority
- Ak je úspešne overený elektronický podpis certifikačnej autority na certifikáte, t.j. certifikát je pravý; Bob môže overovať ostatné informácie, ktoré certifikát obsahuje (doba platnosti)
- Špeciálnym problémom je predčasné ukončenie platnosti certifikátu

Zrušenie certifikátu

- Aj keď je v záujme držiteľa certifikátu chrániť si svoj súkromný kľúč, môže dôjsť k jeho strate, alebo prezradeniu
- Na zamedzenie problémov vyplývajúcich z možného zneužitia cudzieho súkromného kľúča slúži mechanizmus revokácie (rušenia) certifikátov
- Ak držiteľ certifikátu zistí, že pravdepodobne došlo ku kompromitácii jeho súkromného kľúča, zablokuje jeho používanie tým, že požiada vydavateľa certifikátu príslušného verejného kľúča o zrušenie daného certifikátu
- CA zruší daný certifikát verejného kľúča a zaradí ho na zoznam zrušených certifikátov (Certificate revocation list, CRL)
- Keď Bob bude overovať Alicin digitálny podpis, musí zistiť, či sa Alicin certifikát nenachádza na CRL, resp. presnejšie, či sa tam nenachádzal v čase, keď bol vytvorený Alicin digitálny podpis. Ak áno, Alicin podpis zamietne

Zoznam zrušených certifikátov (CRL)

- je elektronický dokument, ktorým certifikačná autorita oznamuje predčasné skončenie platnosti certifikátu,
- obsahuje najmä:
  - identifikačné údaje certifikačnej autority,
  - dátum a čas vydania CRL,
  - dátum a čas najneskoršieho vydania nového CRL,
  - zoznam identifikačných čísel zrušených certifikátov,
  - elektronický podpis certifikačnej autority.

- Používanie digitálnych/elektronických podpisov nie je súkromnou záležitosťou Alice a Boba
- Ak majú dôveryhodne komunikovať aj neznámi ľudia z rozličných koncov sveta, bude potrebné vytvoriť infraštruktúru, ktorá umožní overovať ich podpisy
- Infraštruktúra verejných kľúčov, alebo infraštruktúra verejného kľúča, Public key infrastructure plní túto funkciu
- Pozostáva najmä z certifikačných autorít, registračných autorít a iných poskytovateľov certifikačných služieb (napr. vydavateľ časových pečiatok)

Certifikačná autorita

Certifikačná autorita je základom PKI

- vydáva certifikáty
- ruší certifikáty
- vydáva zoznamy zrušených certifikátov
- zverejňuje certifikáty
- poskytuje službu časových pečiatok
- poskytuje rôzne služby na overovanie certifikátov
- robí osvetu

Registračná autorita

Registračná autorita je “predĺžená ruka” certifikačnej autority

- informuje klientov o podmienkach certifikačnej autority
- preberá žiadosti o vydanie certifikátov
- overuje totožnosť klientov
- odovzdáva overené žiadosti certifikačnej autorite
- odovzdáva certifikáty klientom

Postup pri získaní certifikátu

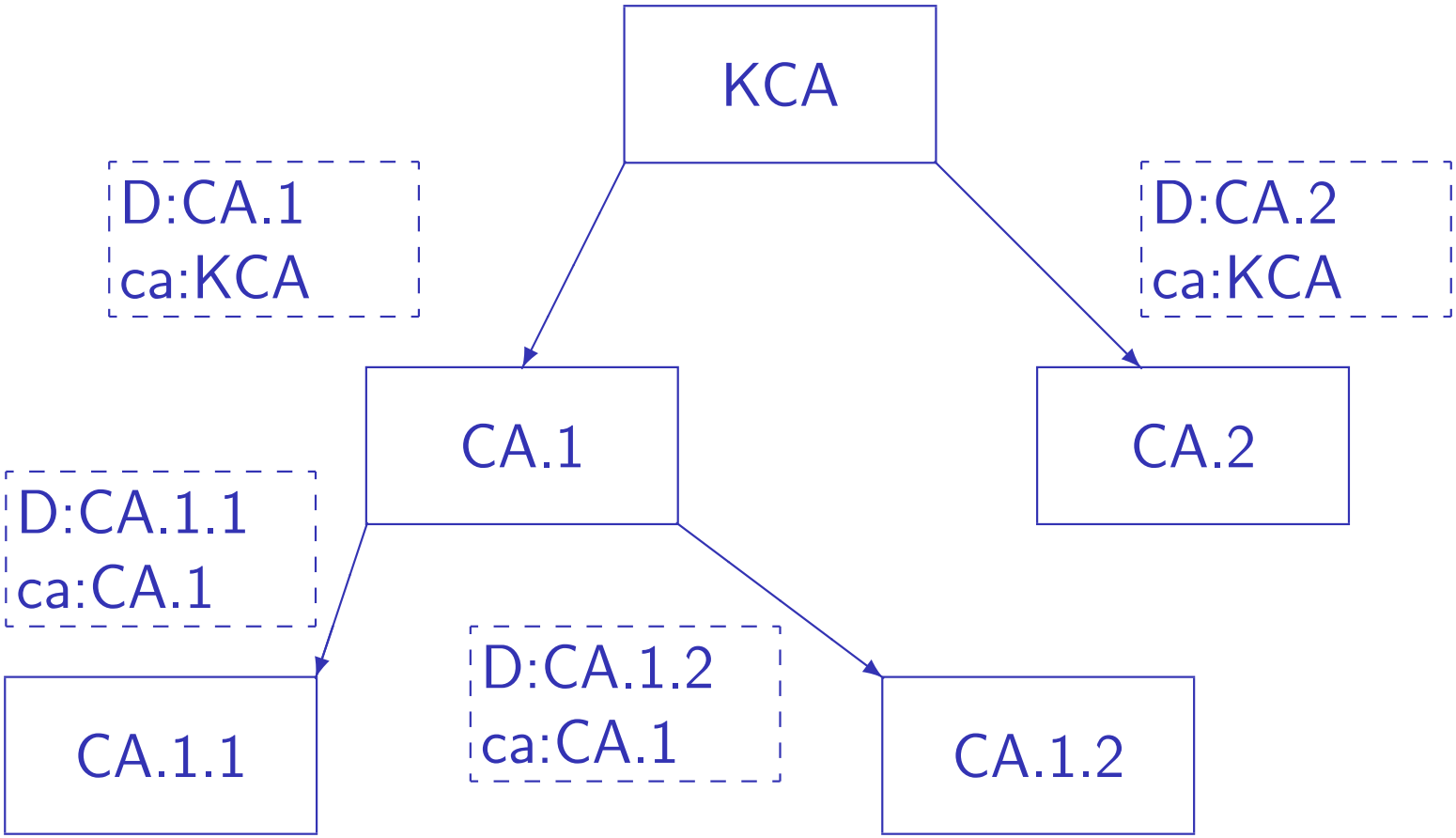
- vytvorenie dvojice kľúčov (klient pomocou poskytnutého softvéru, alebo v špeciálnom zariadení)
- vyplnenie žiadosti o vydanie certifikátu
- elektronické podpísanie žiadosti
- preukázanie totožnosti na registračnom mieste – registračnej autorite
- Podpísanie zmluvy
- vydanie certifikátu
- Prevzatie CPS a iných dokumentov upravujúcich výkon certifikačných služieb (a definujúcich podrobnejšie povinnosti klienta a záväzky CA)
- Prevzatie certifikátu

Overovanie elektronického/digitálneho podpisu Certifikačnej autority

- problém: na overenie Alicinho digitálneho/elektronického podpisu Bob potreboval overiť platnosť certifikátu verejného kľúča
- Na to potreboval overiť minimálne 2 podpisy CA – na certifikáte Alicinho verejného kľúča a na zozname zrušených certifikátov CA
- Ak aj mal k dispozícii certifikát verejného kľúča CA z dôveryhodného zdroja (napr. od samotnej CA), musel by sa presvedčiť, či tento certifikát nebol zrušený, t.j. skontrolovať nejaké CRL, podpísané iným kľúčom, atď.
- Táto reťaz nemôže byť nekonečná, musí existovať pevný bod, na ktorom to celé stojí
- Ďalší problém: čo ak Alicin certifikát verejného kľúča vydala CA, ktorej verejný kľúč Bob nepozná?
- Overovanie verejného kľúča CA závisí od architektúry PKI, do ktorej CA patrí

- Sú možné dve základné riešenia a kombinácie základných riešení:
  - Hierarchická štruktúra (obr.)
  - Mesh
- Základom hierarchickej štruktúry je koreňová CA, ktorej klientami sú CA nižšej úrovne; K-CA robí manažment certifikátov verejných kľúčov bezprostredne podriadených CA
- Každá CA môže byť koreňovou CA nejakého podstromu hierarchickej PKI Na najnižšej hierarchickej úrovni sú CA, ktorých klientami sú koncoví používatelia

Certifikáty certifikačných autorít – hierarchický model



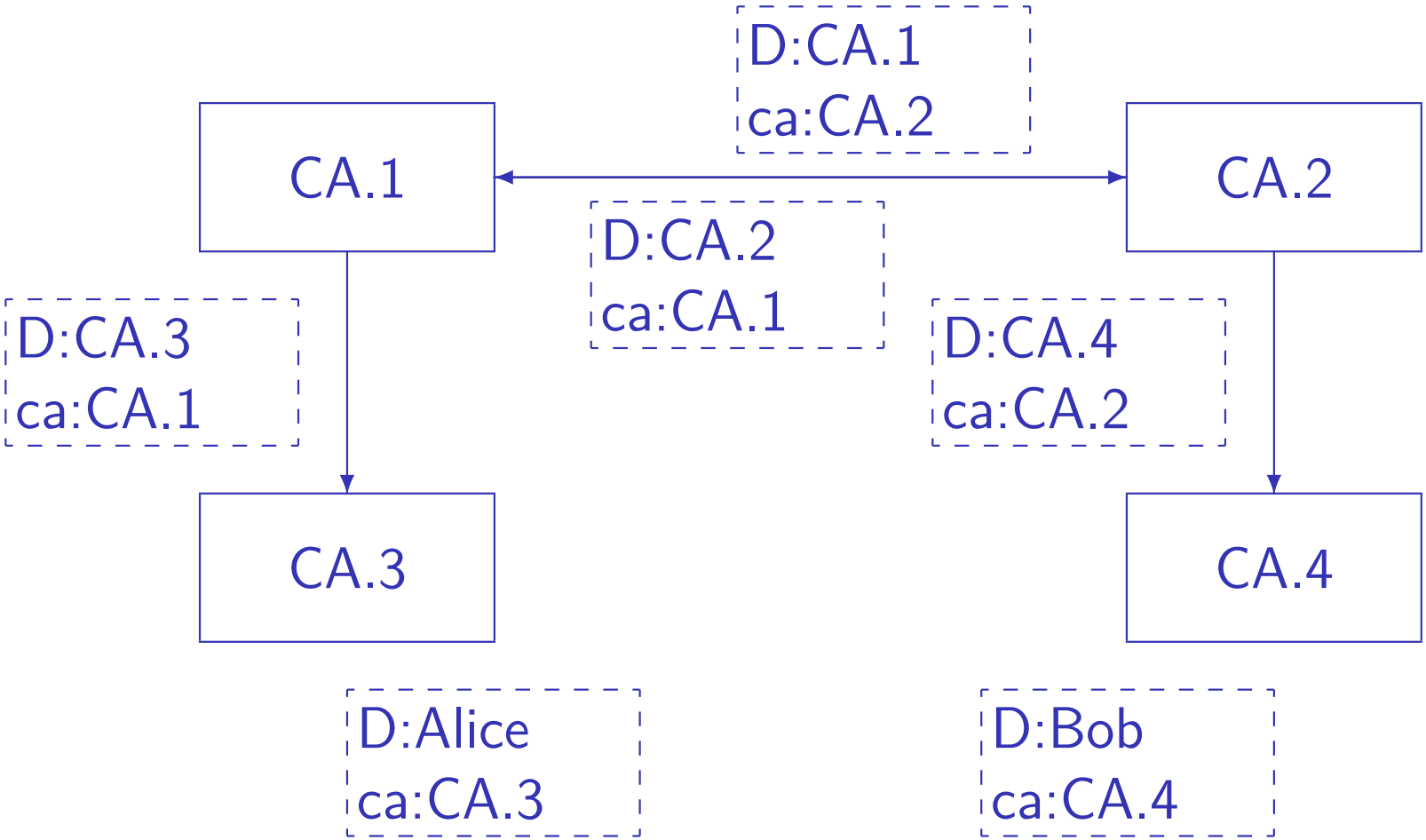
Architektúra typu Mesh

- nemá koreňovú CA
- Pozostáva zo samostatných domén v ktorých pôsobí jedna CA
- CA z rozličných domén si vydávajú na svoje verejné kľúče certifikáty (krížová certifikácia)

Verejný kľúč K-CA

- v hierarchickej PKI je pevným bodom, na ktorom je postavená dôvera vo všetky digitálne/elektronické podpisy verejný kľúč koreňovej CA
- KCA ho zverejňuje aspoň dvoma spôsobmi
  - V certifikáte verejného kľúča, ktorý si sama vydá a podpíše ho pomocou súkromného kľúča, prislúchajúceho k verejnému kľúču, na ktorý vydáva certifikát
  - V tlači alebo spôsobom, ktorý v krajnom prípade umožní overenie verejného kľúča
- Overením digitálneho/elektronického podpisu K-CA na CRL vydávanom K-CA a certifikáte verejného kľúča CA možno pri overovaní elektronického/digitálneho podpisu prejsť o úroveň nižšie a po konečnom počte krokov overiť Alicin elektronický/digitálny podpis

Certifikáty certifikačných autorít – krížová certifikácia



Verejný kľúč CA v nehierarchickej PKI

- CA v doméne PKI funguje ako K-CA – sama zverejňuje svoj verejný kľúč a vydáva si naň certifikát
- Predpokladajme, že Alica je z domény, v ktorej pôsobí CA-A, Bobovi vydala certifikát CA-B. CA-A a CA-B si vzájomne vydali krížové certifikáty verejných kľúčov
- Bob na overenie Alicinho elektronického/digitálneho podpisu potrebuje overiť podpis CA-A
- Dokáže overiť podpis CA-B, pomocou neho overí platnosť krížového certifikátu, ktorý CA-B vydala na verejný kľúč CA-A a z tohto certifikátu získa verejný kľúč potrebný na overenie elektronického/digitálneho podpisu CA-A
- Existujú aj kombinácie oboch prístupov (lokálne časti PKI sú hierarchické, alebo existujú špeciálne CA prepájajúce lokálne časti PKI – bridge CA, atď.)

Časové pečiatky

- Doteraz sme predpokladali, že Alica a Bob konali čestne
- Alica uzatvára s Bobom zmluvu a chce ho podviesť:
  - Pošle mu zmluvu podpísanú elektronickým/digitálnym podpisom
  - Vzápätí požiada CA o zrušenie svojho certifikátu a vyhlási, že je zmluva neplatná
- Časový údaj je v tomto prípade kľúčový: k čomu došlo skôr – k podpísaniu zmluvy, alebo k žiadosti o zrušenie certifikátu?
- Časový údaj musí byť objektívny (nemôže ho vytvárať podpisujúci, nemôže byť odvodený od systémového času,...)
- funkciu objektívneho časového údaju viazaného na dokument plní časová pečiatka

Časové pečiatky

- Časová pečiatka vydaná na daný dokument = digitálne/elektronicky podpísané nasledujúce údaje

> hašovacia hodnota dokumentu, na ktorý sa má časová pečiatka vydať, časový údaj

- Časovú pečiatku vydáva CA, alebo dôveryhodný poskytovateľ časových pečiatok, ktorý má na to patričné vybavenie
- Na čom potom stroskotá Alica: Bob si nechá vydať časovú pečiatku na zmluvu a až potom ju akceptuje, Alica sa síce pokúsi zrušiť svoj certifikát, ale pri dokazovaní sa ukáže, že zmluva existovala už v čase, keď ešte platil Alicin certifikát verejného kľúča

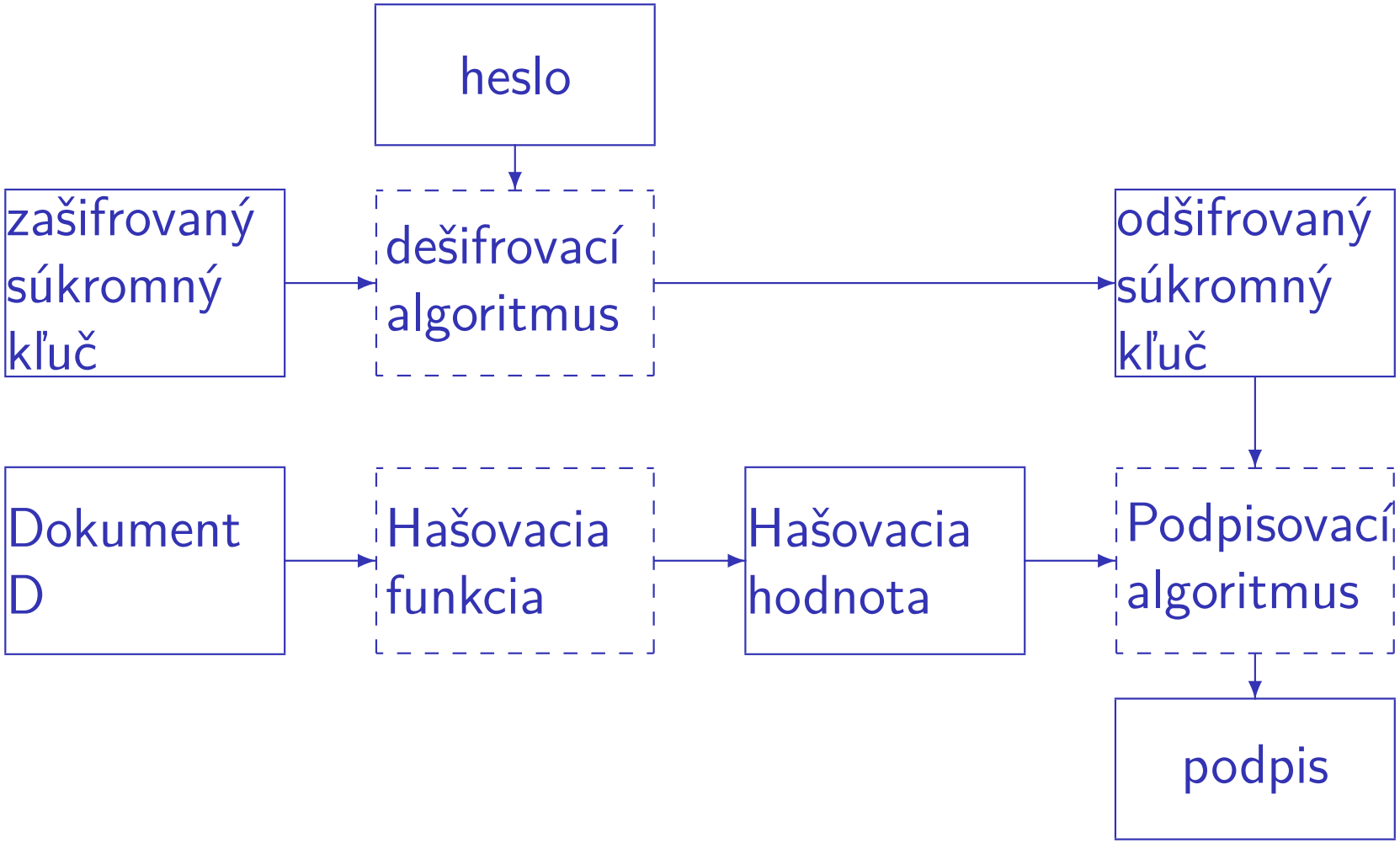
Bezpečnosť elektronického podpisu

- Vytvoriť digitálny podpis bez znalosti súkromného kľúča je prakticky nemožné.
- Znalosť súkromného kľúča (alebo možnosť jeho použitia) umožňuje komukoľvek vytvoriť pravý digitálny podpis
- digitálny podpis nenesie, na rozdiel od vlastnoručného, žiadne biometrické chrakteristiky, na základe ktorých by bolo možné určiť, kto ho vytvoril.

Ochrana súkromného kľúča

- veľmi od nej závisí bezpečnosť elektronického podpisu
- dôležitá je kvalita generátora kľúčov
- súkromný kľúč sa zvyčajne ukladá v šifrovanej podobe
- dôležité je udržať šifrovacie heslo v tajnosti
- vhodné je používať špeciálne zariadenia (napr. kryptografické čipové karty) na vytváranie, ukladanie a používanie súkromného kľúča

Čo sa deje so súkromným kľúčom ?



Riziká pri vytváraní elektronických podpisov

- použitie nekvalitného generátora kľúčov
- získanie zašifrovaného súkromného kľúča a dešifrovacieho hesla
- získanie súkromného kľúča po odšifrovaní
- možnosť podstrčenia iného dokumentu alebo hašovacej hodnoty
- zmena (poškodenie) súkromného kľúča tiež môže viesť k jeho prezradeniu

Vytváranie elektronického podpisu len pomocou bežného počítača

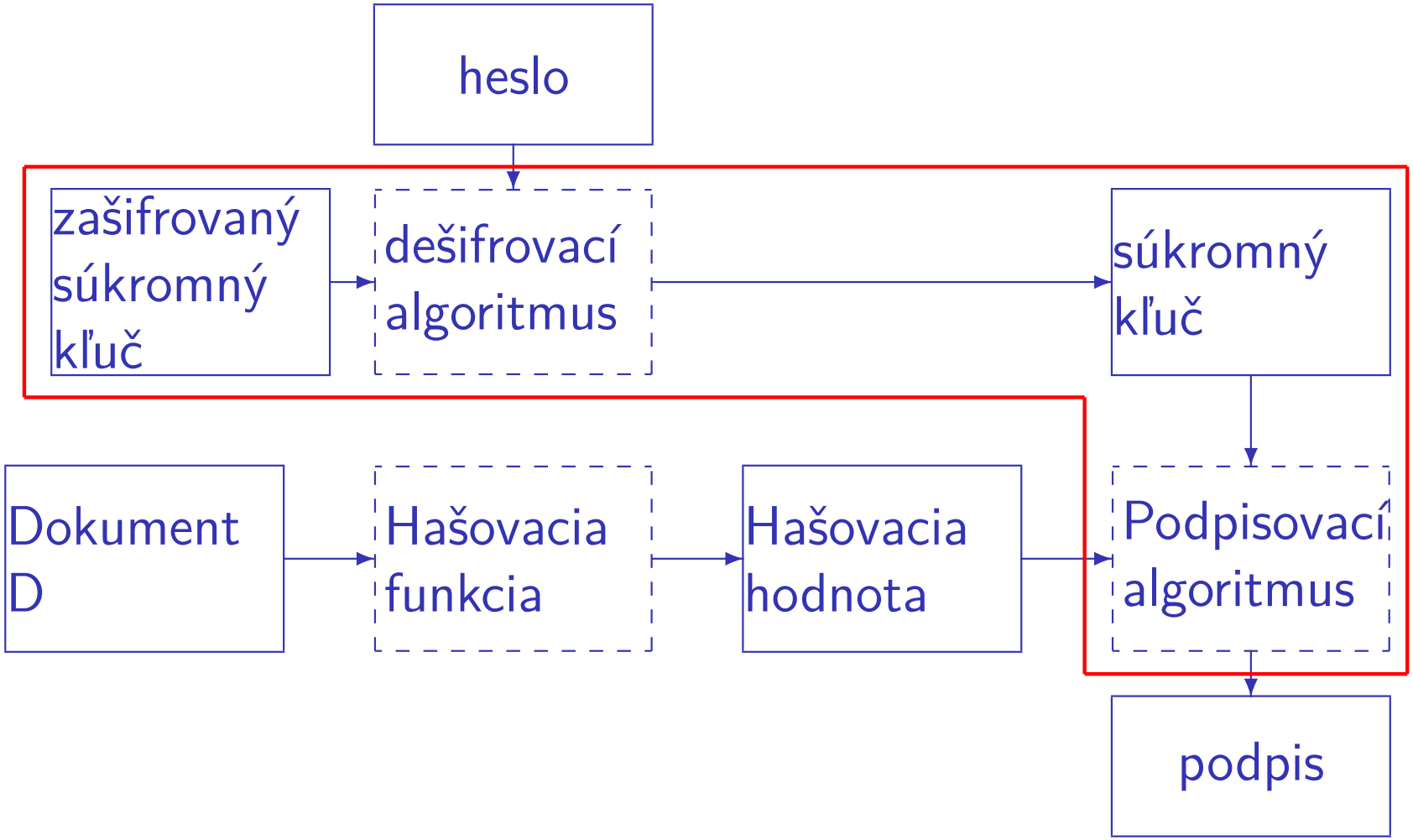
- predpoklady:
  - bežný počítač používaný aj na iné účely
  - pár kľúčov vytvorený programom v počítači
  - súkromný kľúč uložený na disku alebo USB
  - heslo zadávané z klávesnice
  - podpis vytváraný programom v počítači
- riziká: vo všetkých fázach, ak má cudzia osoba možnosť spustiť svoj program

Použitie kryptografickej karty

predpoklady:

- bežný počítač používaný aj na iné účely
- kryptografická karta vytvára a ukladá kľúče, počíta podpis
- heslo sa zadáva cez počítač
- hašovacia hodnota sa počíta v počítači a posiela do karty alebo sa do karty posiela celý dokument

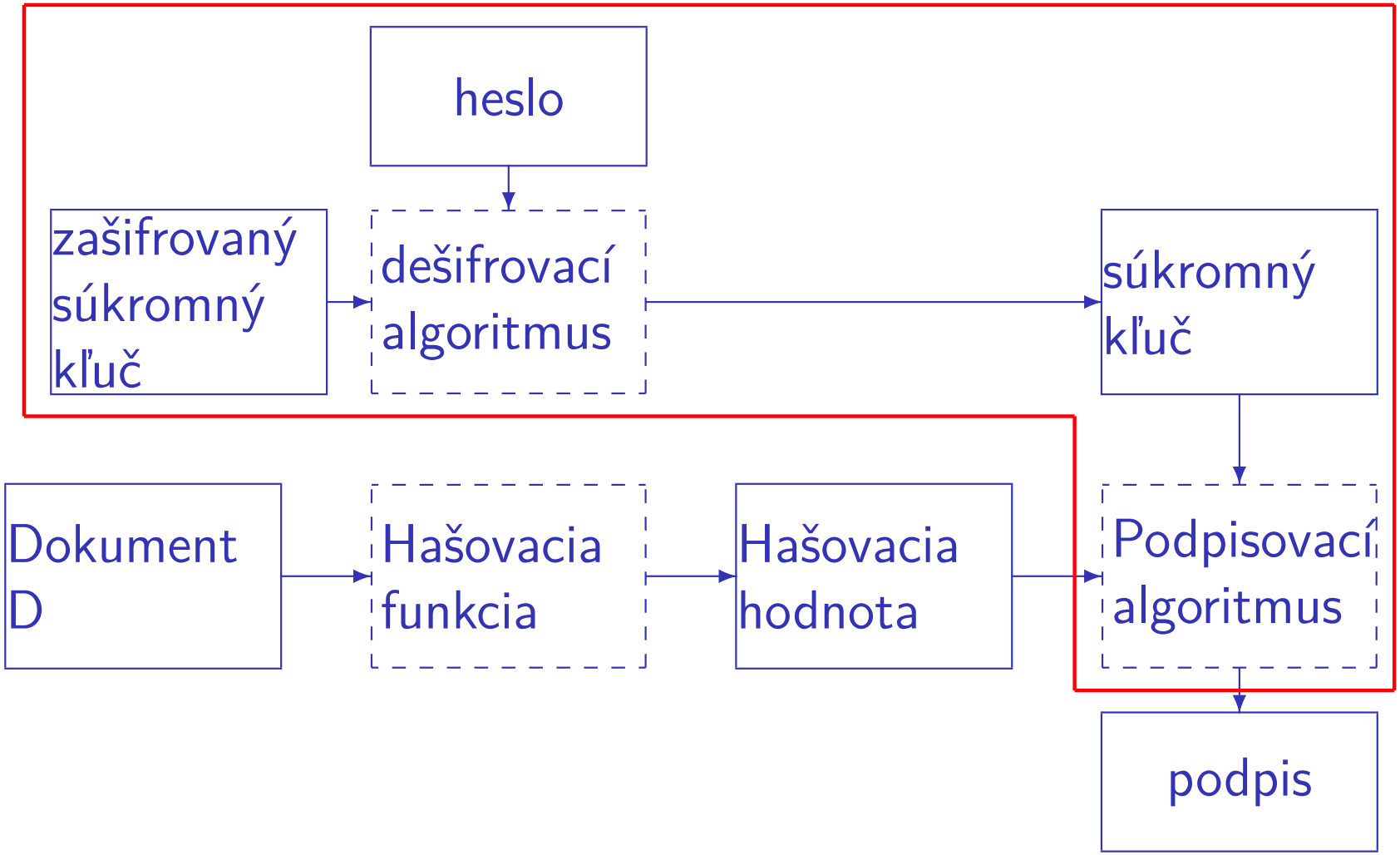
Použitie kryptografickej karty



Použitie kryptografickej karty

- odstránené riziká:
  - možnosť získať súkromný kľúč
  - bez pripojenej karty nie je možné vytvoriť podpis
- zostávajúce riziká:
  - možnosť zistenia hesla
  - možnosť podstrčenia iného dokumentu
  - ak už útočník pozná heslo, možnosť použiť kartu, keď je pripojená

Použitie kryptografického zariadenia s vlastným vstupom



Použitie kryptografického zariadenia s vlastným vstupom

- odstránené riziká:
  - možnosť získať súkromný kľúč
  - bez pripojenej karty nie je možné vytvoriť podpis
  - možnosť získať heslo
- zostávajúce riziká:
  - možnosť podstrčenia iného dokumentu
- na odstránenie tohto problému by zariadenie muselo byť schopné zobraziť podpisovaný dokument

Napadnuteľnosť bežného počítača

- chyby v operačnom systéme a aplikáciach
- trójske kone, vírusy a červy
  - šírené elektronickou poštou
  - skryté na WWW stránkach
  - zanesené spúšťaním programov z nespoľahlivých zdrojov (napr. stiahnutých z Internetu)
- využitím fyzického prístupu k počítaču
  - najmä verejné a zdieľané počítače

Viete, čo podpisujete?

- Zložitejšie formáty dokumentov (ako napr. MS Word) môžu často obsahovať informácie, ktorých zobrazenie je závislé od nastavenia parametrov programu, ktorý s nimi pracuje.
- Ak o tom človek nevie, je možné mu poslať na podpis dokument, ktorý obsahuje ukryté informácie, ktoré si ten človek nevšimne.
- Ako sa chrániť:
  - podpisovať len jednoduché typy dokumentov (napr. čistý text – dá sa otvoriť napr. v NOTEPAD-e)
  - explicitne špecifikovať, akým programom a pri akých nastaveniach sa má dokument čítať

Odporúčania pre používanie elektronických podpisov

- Ak sa dá, vyhnite sa podpisovaniu cudzích zložitých dokumentov.
- Na generovanie kľúčov, uloženie súkromného kľúča a vytváranie elektronických podpisov využívajte bezpečné (alebo aspoň bezpečnejšie) zariadenia.
- Nepoužívajte v súvislosti s elektronickými podpismi verejné počítače.
- Chráňte svoje počítače proti napadnutiu cudzím programom – použite operačný systém umožňujúci definovať prístupové práva a nastavte ich tak, aby boli programy a súbory súvisiace s el. podpismi chránené proti neoprávnenému prístupu. Na ich používanie si vytvorte samostatné konto, ktoré nebudete používať na žiadne iné účely.

Elektronický podpis

- Digitálny podpis založený na asymetrickej kryptografii je známy od polovice 70-tych rokov
- 90-te roky – rozvoj Internetu, elektronickej komunikácie Elektronický obchod sa z bezpečných uzavretých systémov dostáva do prostredia Internetu
- Potreba zaistenia dôveryhodnosti elektronických dokumentov Je potrebná aj právna úprava
- Používajú sa rozličné riešenia (problémy s bezpečnosťou, kompatibilitou a cenou existujúcich riešení)

Elektronický podpis

- Elektronický podpis „electronic signature means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication“
- Takejto špecifikácii vyhovuje meno pod elektronickým dokumentom, alebo naskenovaný vlastnoručný podpis pripojený k dokumentu
- Hľadanie dôveryhodných riešení (založených na digitálnych podpisoch)

Z histórie elektronického podpisu (1)

- 1991 ISO/IEC 9796: prvý medzinárodný štandard pre digitálne podpisy
  - Založený na asymetrickom šifrovaní
  - Nešpecifikuje konkrétny algoritmus (príklad RSA)
  - Správy obmedzenej dĺžky, nevyžaduje sa hašovacia funkcia
  - Poskytuje message recovery
  - padding
- Súkromné štandardizačné iniciatívy orientované skôr na technickú stránku (PKI): RSA Laboratories - PKCS
- 90-te roky: národné zákony (Utah, Singapore, Nemecko,...)

Z histórie elektronického podpisu (2)

- 1996-98 UNCITRAL – vzorový zákon o elektronickom podpise
- 1998 EU: EESSI (ETSI+CEN) príprava európskych štandardov pre elektronický podpis
- 1999 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
- `http://www.ict.etsi.org/sec/eessi/e-sign_directive.pdf`
- Do 19.júla 2001 členské krajiny EU musia zosúladiť svoju legislatívu s Direktívou

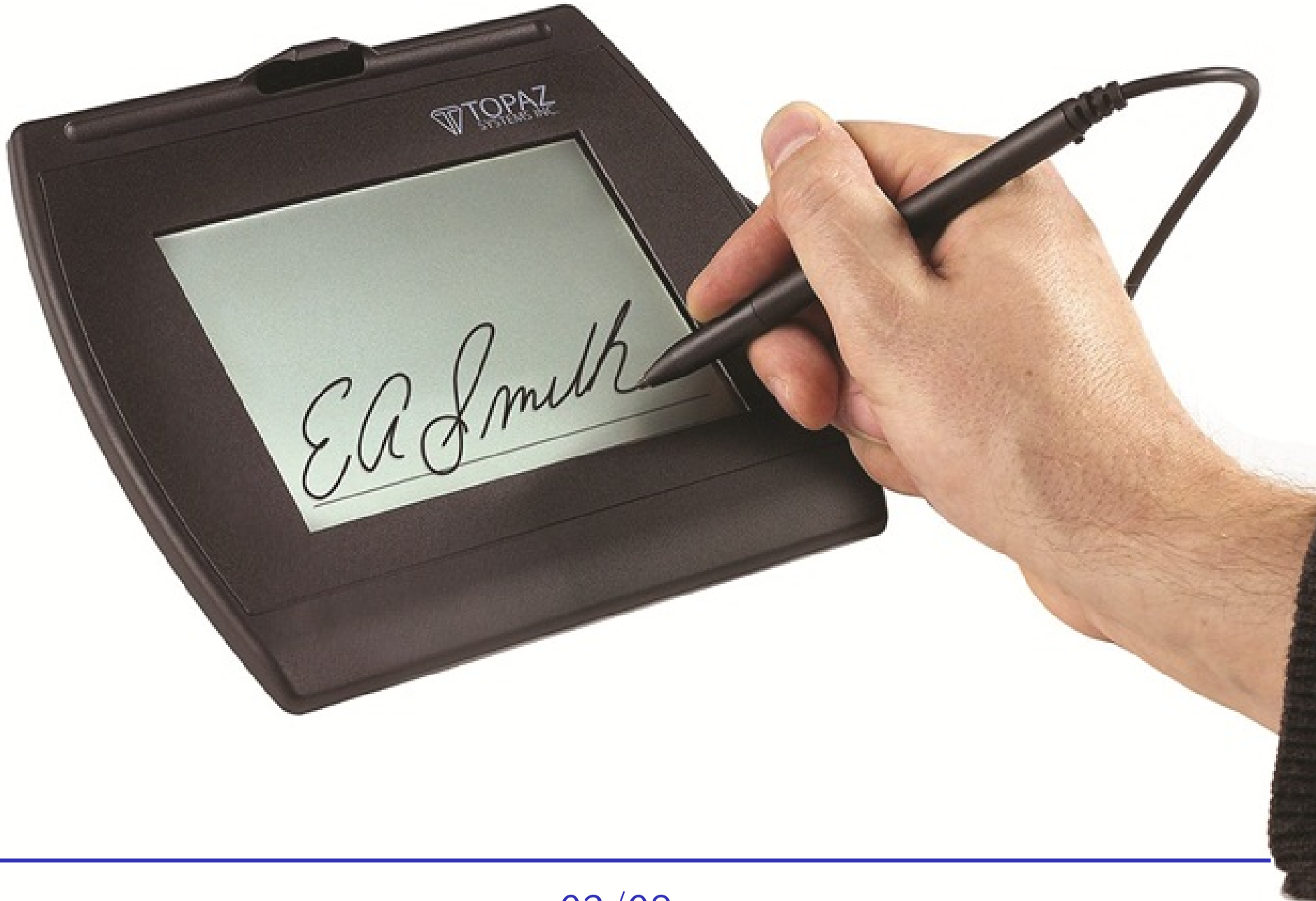
Z histórie elektronického podpisu (2)

- eIDAS (electronic IDentification, Authentication and trust Services) EU Regulation 910/2014 of 23 July 2014 on electronic identification and repeals directive 1999/93/EC from 13 December 1999
- Účinný od 1. júla 2016
- Interoperabilita poskytovateľov digitálnych služieb od 29. septembra 2018

- NBÚ (legislatíva, koreňová CA, ...)
- Elektronické občianske preukazy
- Osobné elektronické schránky
- Podmienky:
  - Technická infraštruktúra (technické vybavenie)
  - Aplikácie (na čo sa elektronický podpis dá použiť)
  - Legislatíva, elementárna kvalifikácia personálu
  - Bezpečnosť

Digitalizovaný vlastnoručný podpis

- objavili sa rôzne podpisovacie tablety
- človek vytvára podpis na tablete, podpis (?) sa digitalizuje
- hovorí sa tomu biometrický digitálny podpis
- presnejšie označenie by bolo digitalizovaný vlastnoručný podpis
- čo všetko sa dá pri vlastnoručnom podpise zaznamenať
  - tvar podpisu (obrázok)
  - dynamika podpisu (rýchlosť vytvárania častí podpisu)
  - tlak na podložku
  - sklon pera
  - charakteristík je niekoľko desiatok, pozri Biometric Handwritten Signature Recognition `https://www.ida.liu.se/~TDDD17/oldprojects/2009/projects/006.pdf`


TOPAZ
SYSTEMS INC.

Vytváranie digitalizovaného vlastnoručného podpisu

- čas vytvárania vlastnoručného podpisu je konečný
- ohraničme ho 10 sekundami
- v každej stotine sekundy bude tablet zaznamenávať
  - pozíciu pera na tablete - súradnice x,y
  - naklonenie pera (uhly v rovine xz a yz)
  - tlak na podložku
  - (a možno aj iné parametre)
- keby sme ostali len pri týchto parametroch, a pri každom rozlišovali 1024 hodnôt, z podpisu získame 50.000 bitov (= biometrické údaje)
- podobne ako pri odtlačkoch prstov sa z biometrických údajov vytvorí podstatne kratšia biometrická vzorka podpisu (vlastnoručného podpisu)

Bezpečnosť digitalizovaného vlastnoručného podpisu

- ako to je s bezpečnostnými požiadavkami na podpis?
- Pripomenieme základné požiadavky na vlastnoručný podpis
  1. nefalšovateľnosť
  2. neprenositeľnosť na iný dokument
  3. možnosť zistiť dodatočnú zmenu obsahu dokumentu
  4. identifikácia podpisovateľa
- ak je podpis dostatočne stabilný a sú známe charakteristiky podpisu, potom by biometrická vzorka mohla stačiť na identifikáciu podpisovateľa (človek sa podpíše na tablete a takto získaná vzorka sa porovná so vzorkou-podpisovým vzorom.)
- ak je biometrická vzorka dostatočne kvalitná (veľkosť, parametre) dá sa predpokladať, že falšovateľovi sa nepodarí vytvoriť podpis inej osoby
- s ostatnými požiadavkami to je horšie

neprenositeľnosť na iný dokument

- už pri samotnom podpisovaní nemá podpisujúci istotu, čo vlastne podpisuje
- na obrazovke síce vidí nejaký dokument, ale podpis vytvára na tablete a nemá záruku, že sa podpis spojí len s dokumentom, ktorý mu ukázali, že dokument videl v plnom rozsahu a že vzorka sa nedá priložiť k inému dokumentu
- ak je biometrická vzorka vytvorená len na základe podpisu, chýba väzba na dokument, čo v súčasnosti vieme zaistiť len pomocou hašovacej funkcie a digitálneho podpisu

možnosť zistiť dodatočnú zmenu obsahu dokumentu

- keďže samotný digitalizovaný podpis, resp. z neho odvodená biometrická vzorka nesúvisí s dokumentom, dokument je možné zmeniť
- opäť by to bolo potrebné riešiť pomocou kryptografických prostriedkov

identifikácia podpisovateľa

- za predpokladu, že je biometrická vzorka dostatočne kvalitná a organizácia, ktorá potrebuje zistiť identitu podpisovateľa má k dispozícii jeho digitálny podpisový vzor, je na základe zhody medzi týmito vzorkami možné identifikovať podpisovateľa
- ak chýba podpisový vzor, alebo sa podpisujúci pokúsil sfalšovať cudzí podpis, identifikovať ho len na základe biometrickej vzorky odvodenej z podpisu na tablete asi nebude možné

Závery

- Informatizácia tradičných postupov – dlhodobý a náročný proces
- Možno ho urýchliť – vytváraním aplikácií, osvojovaním nových technológií, vzdelávaním
- Od začiatku je potrebné myslieť na bezpečnosť;
- t,j, skôr ako sa zavedie nejaké riešenie (podpisový tablet), treba naň spraviť bezpečnostný projekt (analýza rizík a návrh, následne implementácia bezpečnostných opatrení)