

# Informačná bezpečnosť (10)

Elektronický podpis a PKI  
princípy, aplikácie a legislatíva

# Abstrakt

Elektronický podpis je bezpečnostná funkcia zaist'ujúca ochranu integrity a autenticity digitálneho dokumentu. Aby sme ho mohli široko používať, potrebujeme vybudovať infraštruktúru verejného kľúča, public key infrastructure, PKI

# Obsah a organizácia prednášky

Prednáška má pokryť 5 tém

1. Úvod: písomné dokumenty a požiadavky na ich bezpečnosť
2. kryptografické princípy elektronického podpisu
3. Technologické podmienky pre aplikáciu elektronického podpisu (PKI)
4. Bezpečnosť a vierohodnosť elektronicky podpísaných správ
5. Legislatíva

# Písomné dokumenty

- ▶ informácie sú uchovávané a často aj prenášané v písomnej podobe (údaje v písomnej podobe – ***písomnosť, dokument***)
- ▶ dôvod: relatívna nemennosť obsahu, trvácnosť záznamu, hodnovernosť, právna váha
- ▶ Podstatný na písomnom dokumente je jeho 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 sa používajú čoraz viac ***elektronické dokumenty***
- ▶ Ako zaistiť bezpečnosť elektronických dokumentov na porovnateľnej úrovni ako je zabezpečenie papierových dokumentov?

# Informačné procesy a prenos informácie

- ▶ 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)
- ▶ Základná schéma: vysielajúca strana (Alica) – prenosový kanál – prijímajúca strana (Bob)
- ▶ Kanál môže byť ovplyvnený šumom, alebo k nemu môže mať prístup nepovolaná tretia strana (Eva);

# Bezpečnostné požiadavky na písomné dokumenty

- ▶ Požiadavky na dokument:
  - **Nemennosť** (prijatý dokument by mal byť totožný s odvysielaným dokumentom – **integrita**)
  - Utajenie obsahu (nepovolaná osoba by sa nemala dostať k obsahu dokumentu – **dôvernosť**)
  - Určenie autorstva (malo byť jasné, kto dokument vytvoril – **autenticnosť**)
- ▶ 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
- ▶ Tretia požiadavka predpokladá pripojenie znaku jedinečného pre danú osobu (autora dokumentu) k dokumentu
- ▶ **Realita:** absolútne spoľahlivý kanál neexistuje, dostatočne spoľahlivé kanály sú drahé a majú malú kapacitu
- ▶ **riešenie:** šifrová ochrana proti Eve a samoopravné kódy proti prírode
- ▶ Autenticnosť dokumentu: ochranné znaky, pečate, podpisy

# Elektronické (virtuálne) dokumenty

- ▶ Čo to vlastne je?
- ▶ = Dokumenty v elektronickej alebo optickej podobe, ktoré nie sú pevne viazané na nosič (zaznamenané na elektromagnetických médiách, prenášané sieťami, prostredníctvom satelitov, dokumenty v pamäti počítača)
- ▶ Prečo sa objavili?
- ▶ Objem informácií, ktoré spoločnosť na svoje fungovanie potrebuje, nie je zvládnuteľný klasickými prostriedkami
- ▶ Preto:
  - najprv mechanické diernoštítkové stroje
  - Telegraf, telefón, rádio, televízia
  - Počítače a počítačové siete
  - A koncom 20. storočia syntéza do podoby Informačných a komunikačných technológií (IKT)
- ▶ Vývoj používania elektronických dokumentov
  - z papierovej do elektronickej podoby, spracovanie v elektronickej podobe a potom spätná transformácia (tlač)
  - Elektronická forma rovnocenná s papierovou
  - Prevládajúca elektronická forma

# Výhody a nevýhody elektronických dokumentov

## výhody:

- Veľký objem informácií na malom priestore
- Jednoduchá možnosť modifikácie
- Rýchle a nepozorovane sa dajú kopírovať
- Rýchly prenos na veľké vzdialenosti

## nevýhody:

- Veľký objem informácií na malom priestore
- Jednoduchá možnosť modifikácie
- 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
- ▶ Bezpečnostné požiadavky na informáciu:
  - Dôvernosť (confidentiality)
  - Integrita (integrity)
  - Dostupnosť (availability)
  - Autentickosť (authenticity)
  - Zodpovednosť (accountability)
  - Súkromie (privacy)
  - Nepopretie pôvodu (nonrepudiation of origin)
  - Nepopretie prijatia (nonrepudiation of receipt)
  - A ďalšie

# Riešenie bezpečnosti elektronických dokumentov

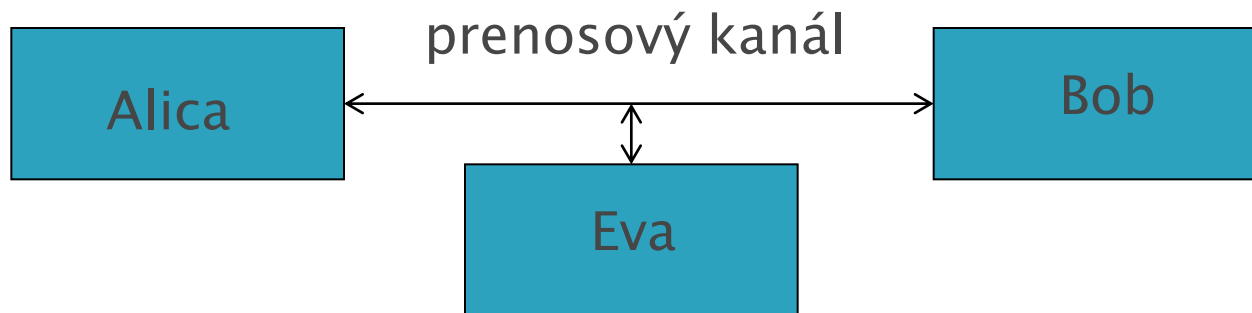
- ▶ Univerzálne, jednorazové riešenie informačnej bezpečnosti nexistuje
- ▶ Riešenia:
  - Organizačné (jasné stanovenie práv a povinností, ochrana prístupu k informačnému systému,...)
  - Právne (legislatíva: elektronický podpis, elektronický obchod, ochrana osobných údajov, ochrana utajovaných skutočností,...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

# Kryptografické riešenia pre informačnú bezpečnosť

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

# Kryptologické minimum (1)

- ▶ Vychádzajme z modelovej situácie: Alica chce poslať Bobovi nejakú správu prostredníctvom prenosového kanálu, na ktorého spoľahlivosť sa nemôže spoľahnúť
- ▶ Alica a Bob = oprávnené osoby
- ▶ 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.



# Kryptologické minimum (2)

- ▶ Správa = dokument, ktorý posiela Alica Bobovi alebo Bob Alici, predpokladáme, že je v textovej podobe. Ak je správa v čitateľnej podobe, hovoríme, že ide o otvorený text, *cleartext*. Konkrétnu (otvorenú) správu označíme  $m$ , množinu všetkých možných otvorených správ symbolom  $M$
- ▶ Kryptografická transformácia = zobrazenie (predpis), ktorý jednoznačne transformuje ľubovoľný text
- ▶ Kryptografická transformácia má dva parametre (vstupné hodnoty) = text a kryptografický kľúč ( $k$ )
- ▶ Množina kryptografických kľúčov  $K$  musí byť dostatočne veľká, aby sa nedali prebrať všetky možnosti
- ▶ Rozlišujeme dve kryptografické transformácie:
  - Šifrováciu
  - Dešifrováciu
- ▶ Šifrovacia transformácia na základe kryptografického kľúča (šifrovacieho kľúča  $k_1$ ) transformuje správu  $m$  na šifrový text  $c$

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

# Kryptologické minimum (3)

- ▶ Množinu všetkých možných šifrových správ označíme symbolom  $C$ .
- ▶ Dešifrovacia transformácia  $D$  šifrový text (šifrovú správu)  $c$  pomocou kryptografického (dešifrovacieho) kľúča dešifruje na pôvodnú správu  $m$ :
- ▶ Kľúče tvoria dvojicu a v mnohých šifrovacích systémoch  $E = D^{-1}$  (na chvíľu budeme predpokladať, že skutočne  $E = D^{-1}$ )
- ▶ množinu dvojíc transformácií (šifrovacích a dešifrovacích)

a pre ľubovoľnú správu  $m$  z  $M$  platí

budeme nazývať kryptosystémom (šifrou)

- ▶ Kryptosystém, v ktorom sa zhoduje šifrovací a dešifrovací kľúč, sa nazýva symetrický kryptosystém

# Kryptologické minimum (4)

- ▶ 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 poučovať.
  - 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 šifrovaných textov, využijúc ďalšie informácie, ktoré sa jej podarilo získať (napr. použitý textový editor)
  - Evina činnosť = kryptoanalýza, Eva = kryptoanalytička
  - Pokus o odhalenie obsahu šifrovanej správy = kryptoanalytický útok
  - Existuje viacero typov kryptoanalytických útokov, nebudeme ich s jednou výnimkou rozoberať

# Kryptologické minimum (5)

- ▶ 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 šifrovaných textov)
- ▶ Kryptológia = kryptografia + kryptoanalýza

# Asymetrické kryptosystémy (1)

- ▶ Klasické kryptosystémy: šifrovací kľúč = dešifrovací kľúč
- ▶ 1976 Diffie a Hellman: idea kryptosystému, v ktorom šifrovací kľúč  $\neq$  dešifrovací kľúč, navyiac 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 zverejní (!), dešifrovací kľúč 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 a zverejní svoj verejný kľúč
- ▶ Alica bude teraz posilať Bobovi správy šifrované Bobovým verejným kľúčom, Bob si ich bude dešifrovať pomocou svojho súkromného kľúča.
- ▶ Bob bude posilať Alici správy šifrované Aliciným verejným kľúčom a ona si ich bude dešifrovať pomocou svojho súkromného kľúča
- ▶ Ak by aj Eva zachytila šifrovanú 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
- ▶ Bežne sa nepoužívajú na šifrovanie celých správ
- ▶ Šifrujú sa nimi kryptografické kľúče pre symetrické kryptosystémy (kľúče na správu)

# Asymetrické kryptosystémy (3)

- ▶ Prekvapujúca možnosť – 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 podpisovateľa s obsahom dokumentu
- ▶ vlastnosti
  - nefalšovateľnosť
  - neprenositelnosť na iný dokument
  - možnosť zistiť dodatočnú zmenu obsahu dokumentu
  - identifikácia podpisovateľa

# Aké garancie vlastne dáva vlastnoručný podpis?

- ▶ odlíšenie pravého podpisu od falošného
  - pre laika to môže byť problém, ale grafológ to dokáže
- ▶ kopírovanie podpisu na iný dokument
  - odlíšiť sa dá kópia podpisu od originálu, ale nie kópia dokumentu, ktorý bol podpísaný, od kópie dokumentu, kam bol podpis prenesený (spor o Markízu)
- ▶ zmena dokumentu po podpísaní
  - čiastočne možná (závisí skôr od technickej realizácie dokumentu)
- ▶ identifikácia podpisovateľa (zistenie mena osoby z podpisu) – nie je

# 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 bez toho, aby to na dokumente zanechalo nejaké viditeľné stopy
  - časť jedného elektronického dokumentu možno jednoducho preniesť do iného

# Nutné požiadavky na „elektronický“ podpis

- ▶ na jeho vytvorenie musí byť potrebná nejaká tajná informácia
  - potom ho môže vytvoriť len ten, kto túto informáciu pozná
- ▶ musí závisieť od obsahu dokumentu
  - 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

# Elektronický vs. digitálny podpis

- ▶ elektronický podpis
  - všeobecný pojem označujúci informáciu, ktorá spĺňa stanovené požiadavky
  - *DIRECTIVE 1999/93/EC: '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**;*
- ▶ digitálny podpis
  - konkrétny kryptologický prostriedok, ktorý sa využíva na realizáciu elektronických podpisov (v súčasnosti jediný známy spôsob ako stanovené požiadavky splniť)
- ▶ V závere prednášky sa ešte dostaneme aj k histórii zákona o elektronickom podpise, štandardizačným aktivitám v oblasti elektronických podpisov. Dovtedy budeme používať pojmy elektronický a digitálny podpis ako synonymá

# Princíp digitálneho podpisu (1)

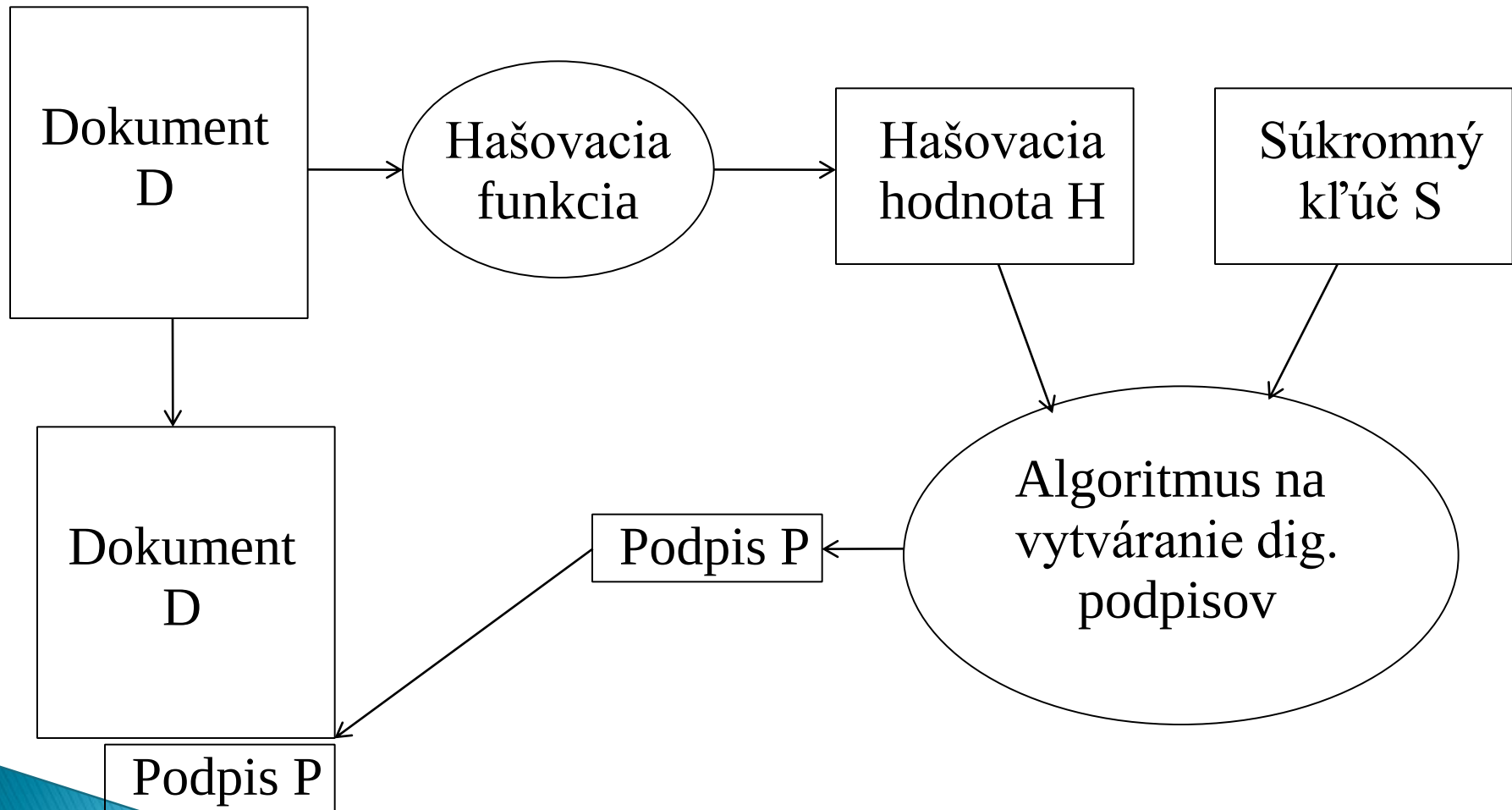
- ▶ Pripomeniem „obrátené“ použitie kľúčov asymetrického šifrovacieho systému:
  - Súkromný na šifrovanie a verejný na dešifrovanie
  - Keďže šifrový text je schopný vytvoriť len držiteľ súkromného kľúča, ale overiť každý, ktorý má prístup k verejnému kľúču, môže zašifrovaný rozumne vybraný text predstavovať 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

# Princíp digitálneho podpisu (2)

## hašovacia funkcia

- ▶ Funkcia, ktorá textu ľubovoľnej dĺžky priradí číslo pevnej dĺžky (hašovaciú hodnotu)
- ▶ Navyše, musí mať nasledujúce vlastnosti:
  - Pre ľubovoľnú správu sa hašovacia hodnota počíta ľahko
  - Pre hašovaciú 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)

# Vytváranie digitálneho podpisu



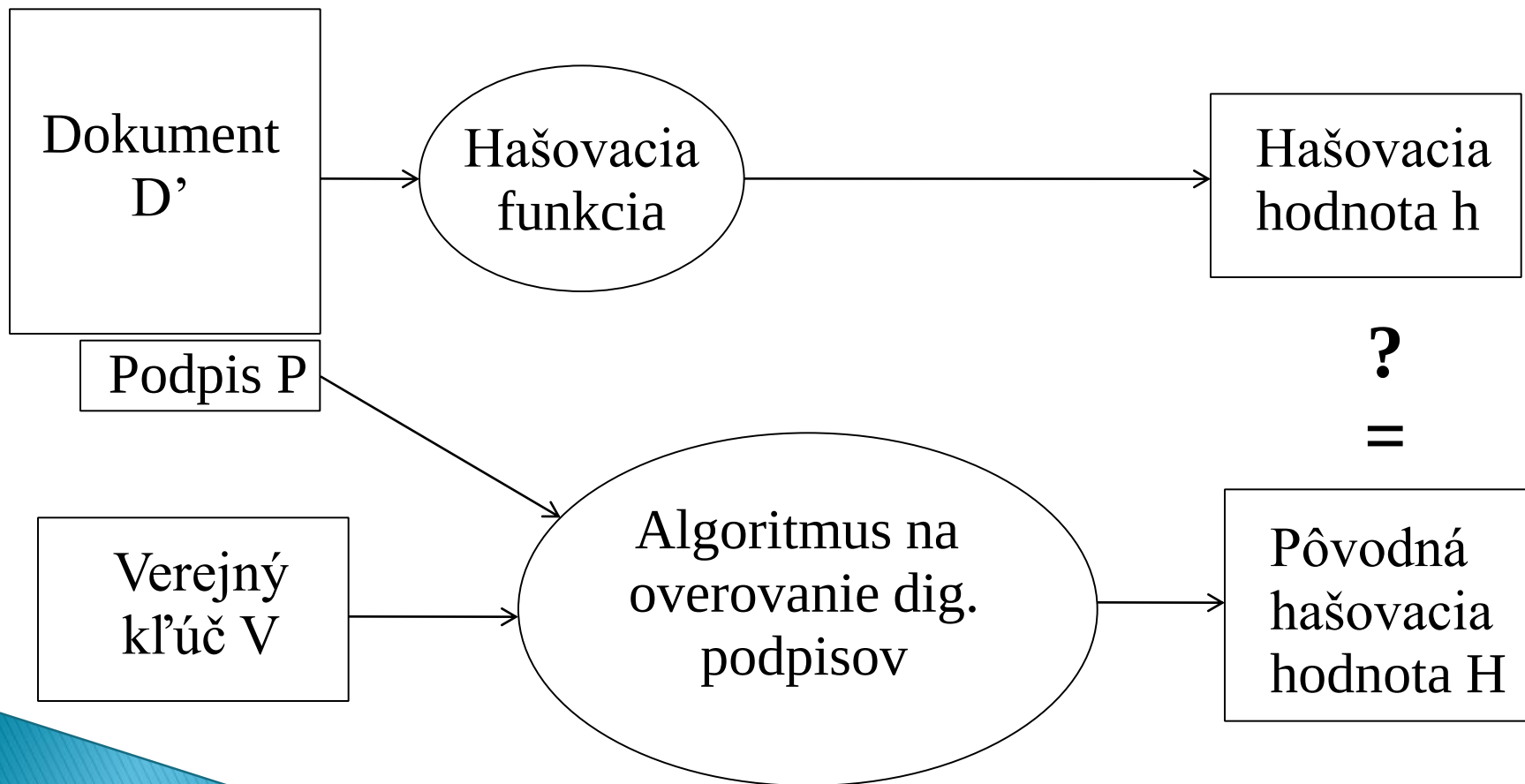
# Príklad digitálne podpísanej správy (1)

- ▶ 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 podpísany. 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
- ▶ -----ms6F9AFCDB3150C4CB33D9D648--

# Príklad digitálne podpísanej správy (2)

- ▶ MIIG7gYJKoZlhvcNAQcColIG3zCCBtsCAQExCzAJBgUrDgMCGGUAMAsGCSqGSib3DQEHAaCC
- ▶ BHYwggRyMIID26ADAgECAgECMA0GCSqGSib3DQEBBAUAMIHfMQswCQYDVQQGEwJTSzERMA8G
- ▶ A1UECBMIU2xvdmFraWExEzARBgNVBAcTCKJyYXRpc2xhdmExRDBCBgNVBAoTO0ZhYy4gb2Yg
- ▶ TWF0aGVtLiwgUGh5cy4gYW5kiEluZm9ybWF0aWNzLCBDb21lbml1cyBVbml2ZXJzaXR5MScw
- ▶ JQYDVQQLEx5EZXBhcnRtZW50IG9mIENvbXB1dGVyIFNjaWVuY2UxDzANBgNVBAMTBkRDUyBD
- ▶ ...
- ▶ SIb3DQEJARYZamFuYWNla0BkY3MuZm1waC51bmliYS5zawlBAjAJBgUrDgMCGGUAAoIGxMBgG
- ▶ CSqGSib3DQEJAzELBgkqhkiG9w0BBwEwHAYJKoZlhvcNAQkFMQ8XDTAxMDczMTE4NDkwNVow
- ▶ lwYJKoZlhvcNAQkEMRYEFLlviSXJMge9Yzook1 +gDhhXxQifMFIGCSqGSib3DQEJDzFFMEMw
- ▶ CCqGSib3DQMCAgEoMA0GCSqGSib3DQEBAQUABIGA0HVIVwURVZpTL1ZiY6S5nm11wYNKHtQJ
- ▶ YKLFOalvr4das+udU4ODG4y9g5gOPsKXlg7uph9lyr9wbmD7pQQxcjCec0pJbgVLtv/EcaDo
- ▶ aEStU0ZKLXwnJ+CNVRbq6EOTYG3sLHIX47EpeLSX41mpxu9EdMIDYrynu5gBdmVxJFU=

# 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 neprenositelný 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, ktorá
  - Overí totožnosť žiadateľa
  - To či pozná súkromný kľúč tvoriaci dvojicu s verejným kľúčom, na ktorý vydáva certifikát
  - Prípadne iné údaje, ktoré majú byť v certifikáte
- ▶ 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 authority

# 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
- ▶ Pozri RFC 5380



cert.cer

# 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 kľúčovi 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 ho vydala CA, ktorá je ako vydavateľ certifikátu uvedená
  - Či bol platný v čase vytvorenia Alicinho digitálneho podpisu
  - Či certifikát nebol modifikovaný
  - Či certifikát nebol zrušený
- ▶ Kľúčové pre overenie platnosti certifikátu je overenie digitálneho podpisu vydavateľa certifikátu (certifikačnej authority) na certifikáte. To predpokladá, že Bob má k dispozícii z dôveryhodného zdroja verejný kľúč certifikačnej authority
- ▶ Ak je úspešne overený elektronický podpis certifikačnej authority na certifikáte, znamená to, že certifikát nie je podvrhnutý a 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 teraz 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.
- ▶ Formát CRL popisuje štandard X509 (aj RFC 5280)

# X.509 v2 CRL syntax

```
▶ CertificateList ::= SEQUENCE {
▶     tbsCertList      TBSCertList,
▶     signatureAlgorithm AlgorithmIdentifier,
▶     signatureValue    BIT STRING }
▶ TBSCertList ::= SEQUENCE {
▶     version          Version OPTIONAL,
▶                     -- if present, MUST be v2
▶     signature        AlgorithmIdentifier,
▶     issuer            Name,
▶     thisUpdate        Time,
▶     nextUpdate        Time OPTIONAL,
▶     revokedCertificates SEQUENCE OF SEQUENCE {
▶         userCertificate CertificateSerialNumber,
▶         revocationDate    Time,
▶         crlEntryExtensions Extensions OPTIONAL
▶                     -- if present, version MUST be v2
▶     } OPTIONAL,
▶     crlExtensions     [0] EXPLICIT Extensions OPTIONAL
▶                     -- if present, version MUST be v2
▶ }
▶ http://www.dtca.sk/actions/find\_commercial\_crl.php
```

## Certificate Revocation List (CRL):

Version 2 (0x1)

Signature Algorithm: sha1WithRSAEncryption

Issuer: /C=CZ/CN=I.CA – Standard root certificate/O=První  
certifikacní autorita a.s.

Last Update: Jan 18 20:58:02 2012 GMT

Next Update: Jan 19 21:58:02 2012 GMT

CRL extensions:

X509v3 Authority Key Identifier:

keyid:EB:37:A4:BE:B9:6F:60:17:FB:D3:FF:2D:60:E1:04:1E:AF:CF:C6:D3

X509v3 CRL Number:

37394

Revoked Certificates:

Serial Number: 18C280

Revocation Date: Mar 14 08:29:21 2011 GMT

Serial Number: 18C287

Revocation Date: May 26 11:58:05 2011 GMT

Serial Number: 19FDA1

Revocation Date: Dec 5 10:56:06 2011 GMT

Serial Number: 1A061F

Revocation Date: Dec 10 10:31:33 2011 GMT

Serial Number: 1A127D

Revocation Date: Dec 23 08:57:44 2011 GMT

Signature Algorithm: sha1WithRSAEncryption

69:0f:82:10:6e:11:3e:54:57:ca:37:a6:58:77:d4:7c:40:40:  
51:a4:fe:44:36:08:c9:bc:5a:0a:f6:24:fc:60:f9:94:e3:bb:  
db:9a:fd:a1:be:f8:ca:a2:60:47:a9:2f:d4:07:f7:97:6b:6a:  
27:76:c9:61:c7:94:d7:eb:d5:24:eb:54:cc:78:40:7b:42:3a:  
64:3b:9f:41:2a:f8:39:34:95:4a:b4:31:5c:e5:3f:bb:8b:e5:  
06:e0:50:90:73:8c:05:8a:a8:e9:a0:c0:f6:bb:4c:4d:92:80:  
f1:01:5b:42:d2:1f:5a:e0:0e:41:c6:7f:8e:79:cb:07:b8:52:  
75:a6:dc:b1:40:7b:52:8d:e3:56:78:78:b4:f3:51:44:20:ca:  
1f:c9:38:0a:e8:96:67:3e:dc:eb:ef:f5:99:95:5a:b7:f6:ab:  
96:d2:d5:9c:51:72:f7:da:04:5d:88:ea:f7:13:f1:36:66:b4:  
c4:88:74:54:94:6e:62:2d:0c:ff:09:36:23:7b:3e:2b:61:a7:  
6e:e0:f4:b7:43:02:41:91:5f:d7:31:58:6a:cd:bb:cb:61:a2:  
d9:1f:8d:cb:c4:30:7d:e3:49:69:25:60:ef:88:cb:d9:d2:d6:  
92:91:46:5c:7e:a4:d7:56:4b:ba:94:37:86:74:45:49:4c:2c:  
d1:63:b4:3d

# Public key infrastructure, PKI

- ▶ 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, Public key infrastructure plní túto funkciu
- ▶ Pozostáva najmä z certifikačných autorít, registračných autorít a iných poskytovateľov certifikačných služieb (napr. vydavateľ časových pečiatok)

# Certifikačná a Registračná 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 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

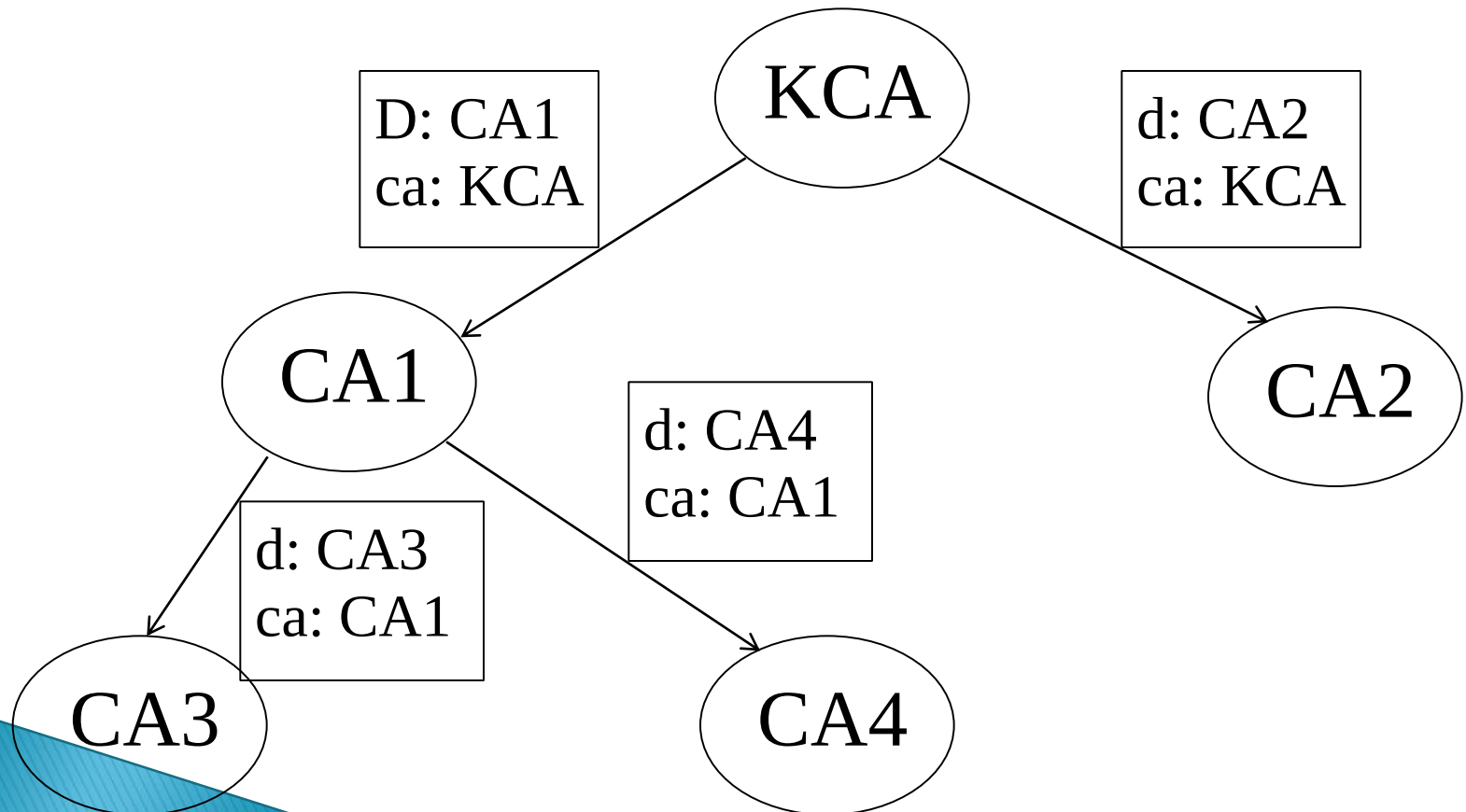
# Overovanie elektronického/digitálneho podpisu Certifikačnej authority

- ▶ 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

# Architektúra PKI

- ▶ 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
- ▶ 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)

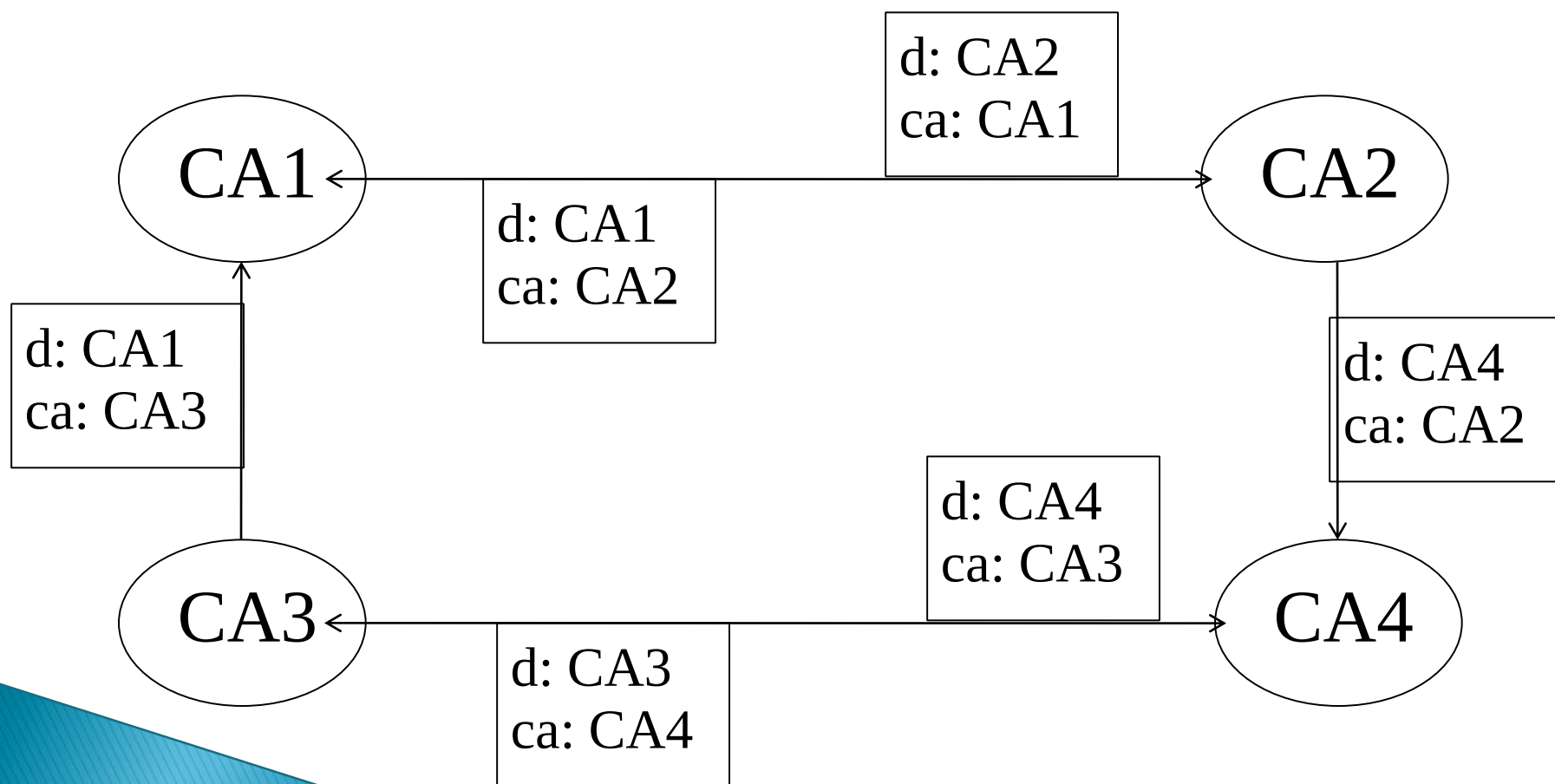
# Certifikáty certifikačních autorit – hierarchický model



# 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 kľúčový: k čomu došlo skôr – k podpísaniu zmluvy, alebo k čiadosti o zrušenie certifikátu?
- ▶ Časový údaj musí byť objektívny (nemôže ho vytvárať podpisujúci, nemôže byť odvodený od systémového času,...)
- ▶ 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

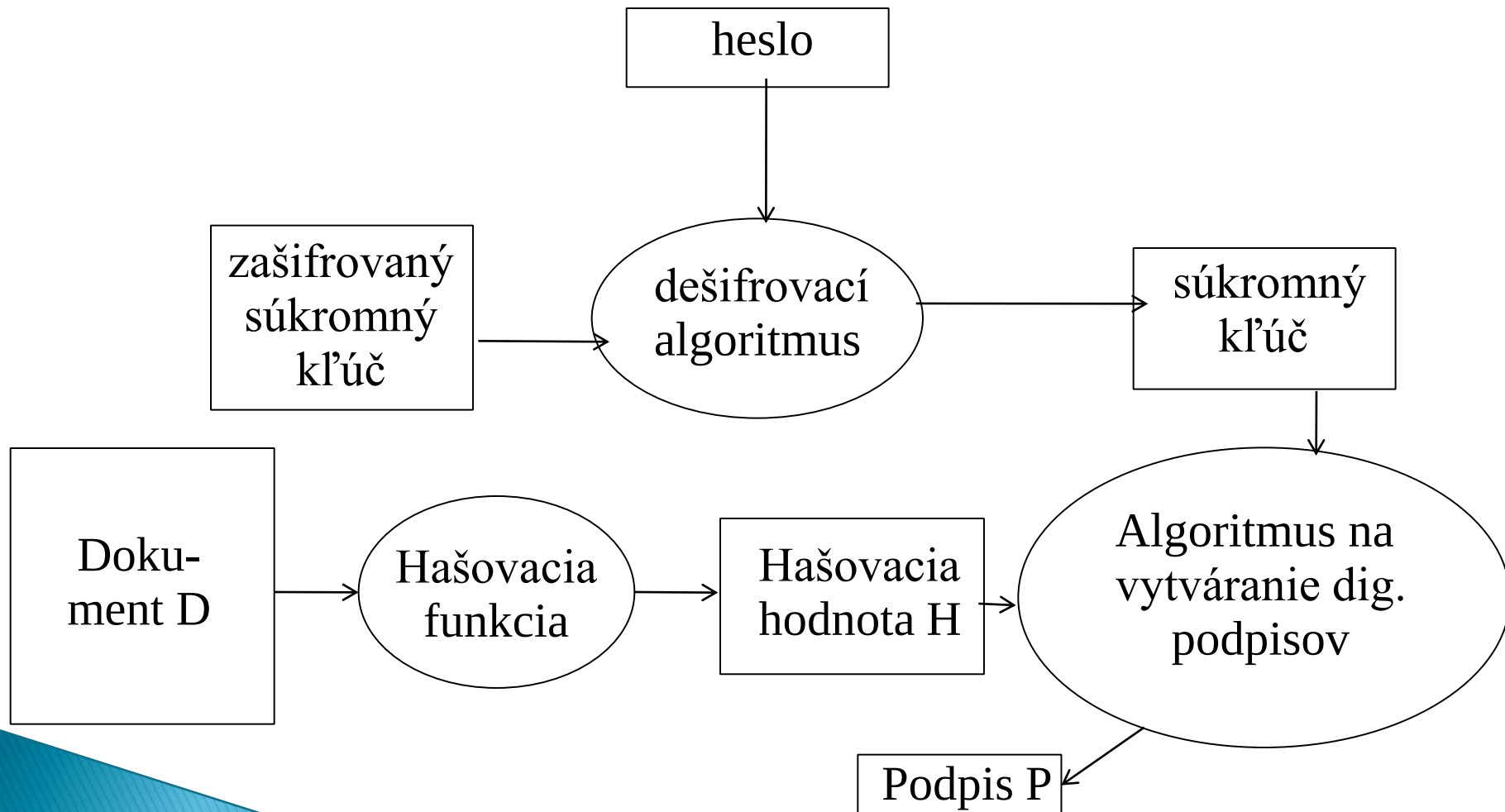
# Bezpečnosť elektronického podpisu

- ▶ 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 charakteristiky, 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 je vytvorený programom v počítači
- súkromný kľúč je uložený na disku alebo diskete
- heslo je zadávané z klávesnice
- podpis je vytváraný programom v počítači

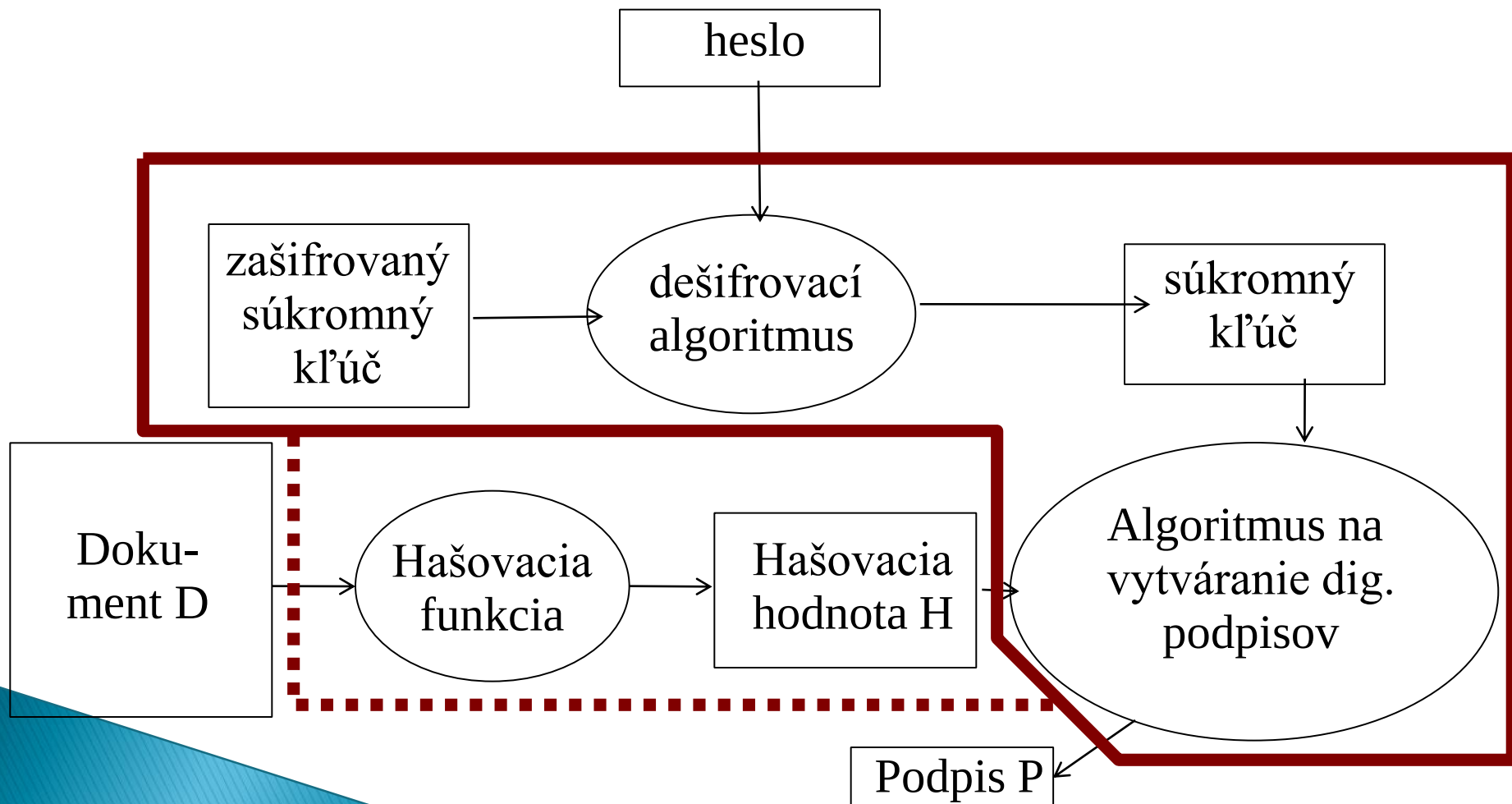
## ► riziká:

- 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

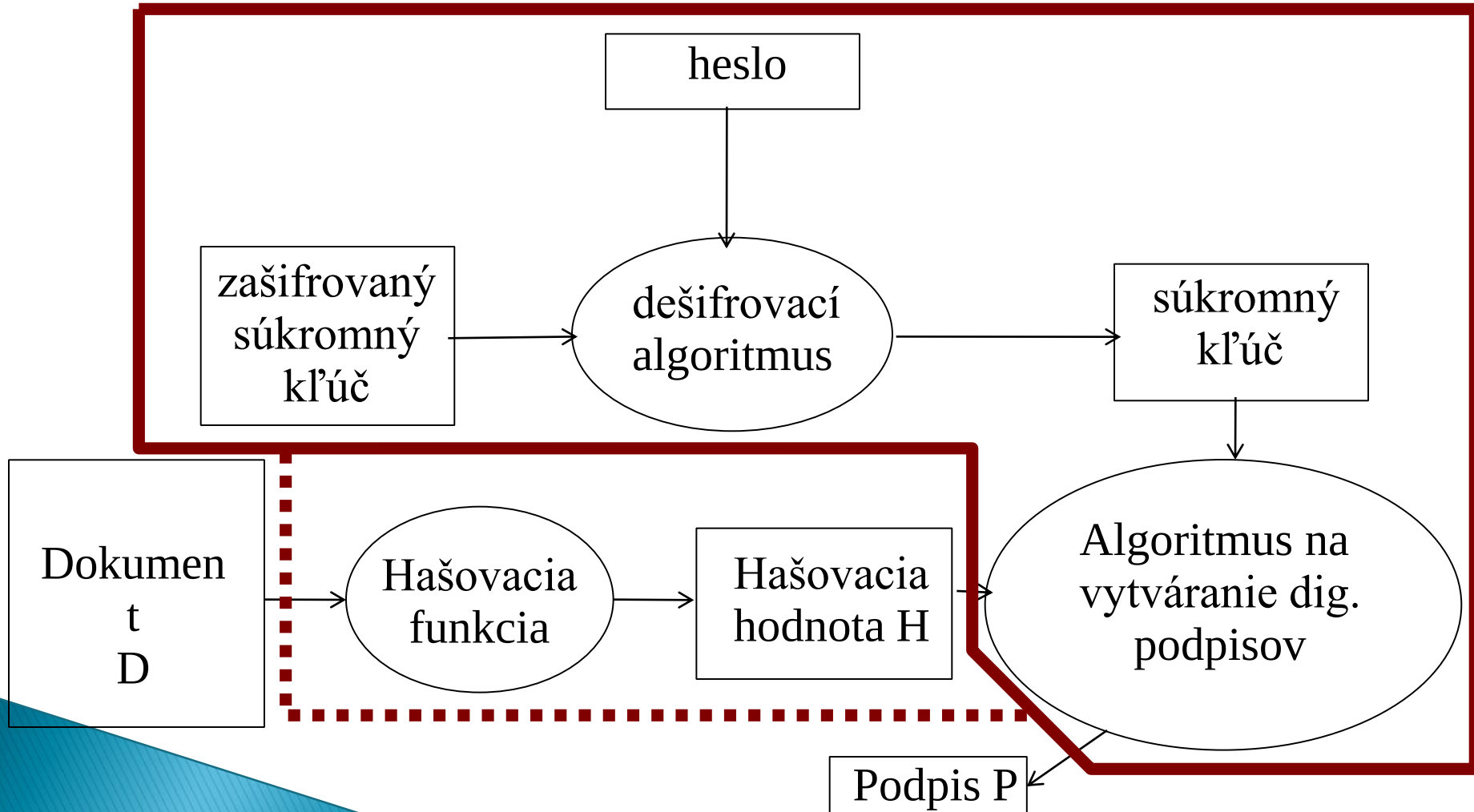
# Použitie kryptografickej karty



# 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 zobrazit' 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 „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](http://www.ict.etsi.org/sec/eessi/e-sign_directive.pdf)
- ▶ Do 19.júla 2001 členské krajiny EU musia zosúladiť svoju legislatívu s Direktívou

# Slovenský zákon o elektronickom podpise

- ▶ Ministerstvo hospodárstva SR začalo pripravovať zákon o elektronickom obchode v rokoch 1998/9
- ▶ Ukázalo sa, že najprv je potrebný zákon o elektronickom podpise
- ▶ Zákon pripravený MH SR mal vážne nedostatky
- ▶ Odborná skupina pri SIS ho pripomienkovala a v rokoch 2000–2001 pripravila alternatívny návrh zákona, ktorý po dlhých „bojoch“ NR SR napokon 15. marca 2002 (na 7. pokus) schválila a 11. apríla 2002 zákon o elektronickom podpise podpísal prezident
- ▶ Zákon platí od 1. mája 2002, v krátkom čase niekoľkých mesiacov boli vypracované vykonávacie predpisy a začiatkom roku 2003 NBU deklaroval, že sú pripravené podmienky na používanie elektronického podpisu

# PKI a elektronický podpis v SR

- ▶ Zákon o EP niekoľkokrát novelizovaný
- ▶ Naposledy (2009) aj vykonávacie predpisy

# Závery (1)

- Zákon o elektronickom podpise je jedným zo základných zákonov informačnej spoločnosti
- Umožní autentifikáciu osôb v digitálnom prostredí
- Jeho uplatňovanie si vyžiada
  - vybudovanie infraštruktúry (PKI)
  - Dobudovanie potrebnej legislatívy (vykonávacie vyhlášky, normy)
  - Vytvorenie aplikácií využívajúcich elektronický podpis
  - Prístup k Internetu a technické prostriedky u podpisovateľov
- Bezprostredne sa bude dať využiť v elektronickom obchode a v styku s úradmi
- Plnohodnotné uplatnenie až keď budú informatizované obchodné a administratívne procesy

# Závery (2)

- ▶ Informatizácia tradičných postupov – dlhodobý a náročný proces
- ▶ Možno ho urýchliť – vytváraním aplikácií, osvojovaním nových technológií, vzdelávaním

# Referencie

- ▶ Electronic Signature Policies RFC 3125
- ▶ ETSI TS 101 733 V1.3.1 Electronic signature formats
- ▶ Electronic Signature Formats for long term electronic signatures RFC 3126
- ▶ ETSI TS 102 023 V1.1.1 Policy requirements for time stamping authorities
- ▶ ETSI TS 101 861 V1.1.1 Time stamping profile
- ▶ Internet X.509 Public Key Infrastructure Time–Stamp Protocol (TSP) RFC 3161
- ▶ ETSI TS 101 903 draft V0.0.8 XML Advanced Electronic signatures (XAdES)
- ▶ ETSI Draft TR 101 XXX V0.4.2 Telecommunication Security; Electronic signature standardization report

# Užitečné adresy

- ▶ [http://www.icts.org/Working\\_Groups/EESSI/index.htm](http://www.icts.org/Working_Groups/EESSI/index.htm)
- ▶ <http://www.pki-page.info/>
- ▶ <http://www.nbusr.sk/sk/elektronicky-podpis/index.html>