

Digitálne podpisy a certifikáty

- základný princíp, využitie
- algoritmus DSA
- certifikáty a ich využitie

Primárny zdroj informácií k dnešnej prednáške:

[1] prof. Ing. Dušan Levický, CSc.

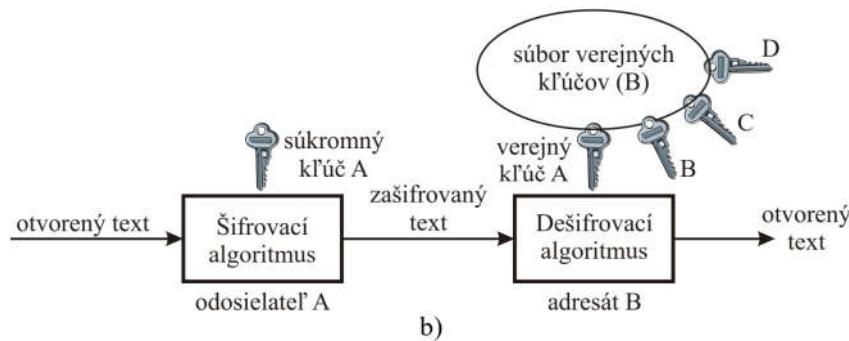
APLIKOVANÁ KRYPTOGRAFIA

od utajenia správ ku kybernetickej bezpečnosti

Elfa, Košice, 2018 (str.202-223, 164-175)

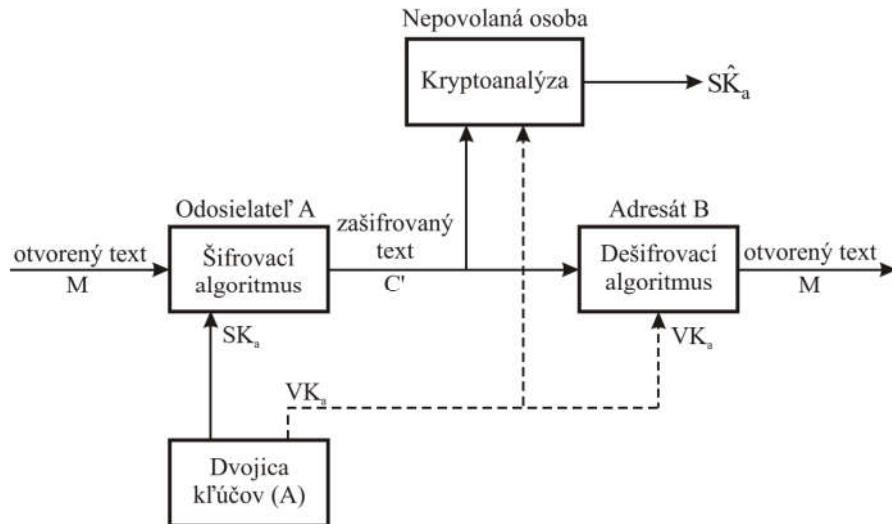
Základný princíp (opakovanie)

Autentizácia v kryptografii s verejným klúčom sa rieši inverzne ako šifrovanie. Ak otvorený text zašifruje odosielateľ A svojim súkromným klúčom, dešifrovanie možno realizovať iba verejným klúčom A čo znamená, že správu zašifroval účastník A (Obr. 7.1b).



Obr. 7.1 Kryptografia s verejným klúčom, b) autentizácia

Princíp kryptografického systému s verejným kľúčom, ktorý umožňuje autentizáciu otvoreného textu, resp. odosielateľa je uvedený na Obr. 7.3.



Obr. 7.3 Kryptografický systém s verejným kľúčom (autentizácia)

Odosielateľ zašifruje otvorený text M svojím súkromným kľúčom SK_a , čím sa získa zašifrovaný text C' . Šifrovanie možno zapísť v tvare

$$C' = E_{SK_a}(M) \quad (7.3)$$

Zašifrovaný text C' sa prenáša k adresátovi B, ktorý prijatý zašifrovaný text dešifruje verejným kľúčom VK_a . Tento kľúč je dostupný a dešifrovanie má tvar

$$M = D_{VK_a}(C') = D_{VK_a}(E_{SK_a}(M)) \quad (7.4)$$

Pretože otvorený text bol zašifrovaný súkromným kľúčom SK_a a možno ho dešifrovať iba verejným kľúčom VK_a , autorom správy je A. Zašifrovaný text C' má v tomto prípade charakter **digitálneho podpisu** (digital signature). Zároveň z toho vyplýva, že modifikácia správy (otvoreného textu) bez prístupu k súkromnému kľúču SK_a je nemožná, teda tento kryptografický systém s verejným kľúčom zabezpečuje autentizáciu zdroja správy aj integritu prenášaných dát.

Elektronické a digitálne podpisy

Kryptografia s verejným kľúčom, resp. technológia **PKI (Public Key Infrastructure)** umožňujú efektívne realizovať autorizáciu dát, autentizáciu zdroja a integritu dát.

V uvedených oblastiach sa vyčlenili dva základné pojmy, ktoré sa často zamieňajú, preto je ich potrebné rozlišovať. Sú to pojmy:

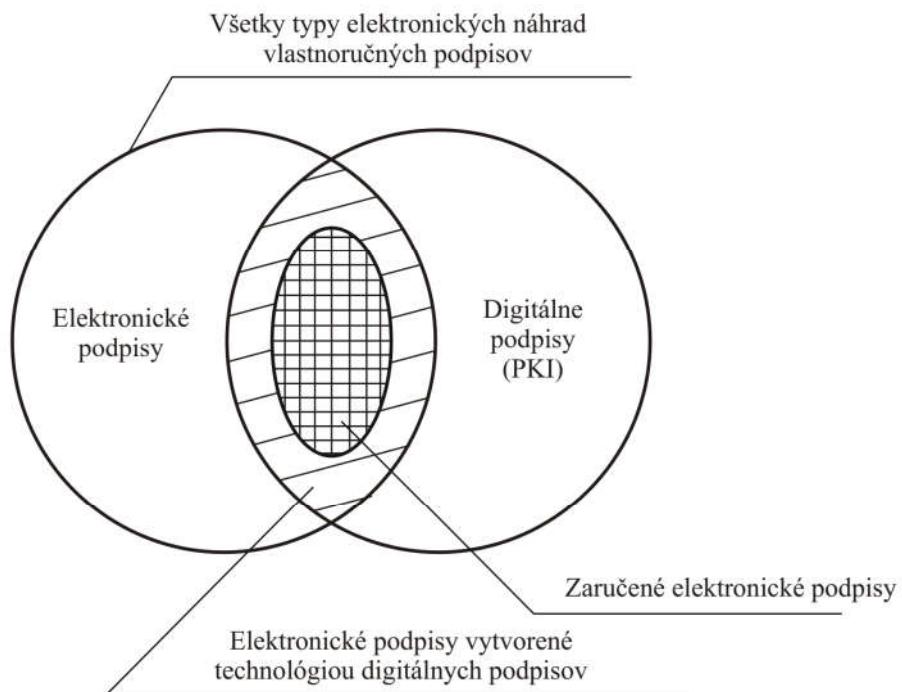
- elektronický podpis (electronic signature)
- digitálny podpis (digital signature).

Elektronický podpis je údaj v elektronickej podobe, ktorý je pripojený alebo logicky spojený s inými elektronickými dátami a ktorý slúži ako dôkaz, že uvedené dátá boli vytvorené konkrétnou osobou alebo konkrétnym elektronickým systémom, teda slúži ako metóda overenia ich pravosti.

Digitálny podpis je elektronický podpis vytvorený na báze kryptografie s verejným kľúčom a technológiou PKI.

Elektronické podpisy

Elektronické podpisy zahrňujú všetky typy elektronických náhrad vlastnoručných podpisov. Podmnožinou elektronických podpisov sú elektronické podpisy vytvorené technológiou digitálneho podpisu Obr. 11.1.



Obr. 11.1 Rozdelenie elektronických podpisov

Pretože elektronické podpisy môžu nahradíť vlastnoručné podpisy, bude užitočné definovať tento pojem.

Vlastnoručný podpis (handwritten signature) je podpis, ktorý vyhotovila (podpísala) fyzická osoba vlastnou rukou.

Vlastnoručné podpisy by mali splňať tieto požiadavky:

- **podpis je nefalšovateľný** – podpis by sa nemal dať napodobniť, resp. prípadný pokus o falzifikát podpisu by mal byť jednoduchým porovnaním odhalený
- **podpis je prostriedkom autentizácie** – podpis jednoznačne identifikuje držiteľa podpisu, ktorý dobrovoľne a vedome označil dokument svojim podpisom
- **podpis je neprenosný** – podpis je súčasťou dokumentu a nepovolaná osoba nemôže presunúť podpis na iný dokument
- **podpísaný dokument nemožno meniť** – dokument po podpísaní nemožno meniť, upravovať
- **podpis nemožno poprietať** – osoba, ktorá je držiteľom podpisu, nemôže poprietať podpísanie označeného dokumentu.

Elektronický podpis môže za určitých podmienok plne nahradzovať vlastnoručný podpis. Tento druh elektronického podpisu sa označuje ako **zaručený elektronický podpis** (advanced electronic signature) - **ZEP⁽¹⁾**. Zaručený elektronický podpis v zmysle smernice európskeho parlamentu 1999/93 ES z roku 1999 sa definuje ako elektronický podpis, ktorý spĺňa tieto požiadavky:

- je **jednoznačne spojený** s podpisujúcou osobou,
- umožňuje **zistiť totožnosť** podpisujúcej osoby,
- je vytvorený s využitím **prostriedkov**, ktoré podpisujúca osoba môže mať **plne pod svojou kontrolou**,
- je **spojený s dátami**, ku ktorým sa vzťahuje tak, aby bolo možné zistiť akúkoľvek následnú **zmenu týchto dát**.

Je potrebné poznamenať, že niektoré právne normy rozširujú požiadavky na zaručený elektronický podpis tak, že zaručený elektronický podpis možno vyhotoviť len s použitím **bezpečného zariadenia na vyhotovenie elektronického podpisu**, ktoré splňa podmienky stanovené príslušnou legislatívou. Okrem toho verejný kľúč patriaci k súkromnému kľúču použitému na vyhotovenie zaručeného elektronického podpisu musí byť vydaný **kvalifikovaný certifikát fyzickej osoby**. Kvalifikovaný certifikát fyzickej osoby je certifikát, ktorý vydala akreditovaná certifikačná autorita fyzickej osobe, je v ňom uvedené, že je kvalifikovaný a má v sebe uvedené obmedzenia na jeho použitie, ak tretia strana také obmedzenia rozlišuje. Telo certifikátu je podpísané zaručeným elektronickým podpisom akreditovanej certifikačnej autority, ktorý bol vytvorený použitím súkromného kľúča určeného na tento účel.

Poznámka:

⁽¹⁾ Podľa aktuálnej legislatívy sa **ZEP** nazýva **kvalifikovaný elektronický podpis (KEP)**. Pozri napr. <https://www.slovensko.sk/sk/faq/faq-zep#moze4>

Digitálne podpisy

Jednou z foriem elektronických podpisov sú digitálne podpisy realizované na báze technológie PKI. Digitálne podpisy by mali splňať **tieto požiadavky**:

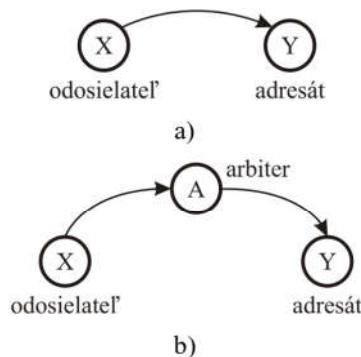
- digitálny podpis by mal mať formu **skupiny bitov**, ktorých hodnoty sú **závislé na podpísanej správe**
- digitálny podpis využíva určitú **jedinečnú informáciu**, ktorá je **vlastníctvom držiteľa** podpisu a zabezpečuje ochranu pred falšovaním a odmietnutím
- realizácia a **implementácia** digitálneho podpisu by mala byť **relatívne ľahká**
- **falšovanie** digitálneho podpisu by malo byť **výpočtovo obtiažné** v tom zmysle, že by malo byť obtiažné vytvoriť novú správu pre existujúci digitálny podpis alebo vytvoriť falošný digitálny podpis pre danú správu
- **uloženie kópie** digitálneho podpisu v pamäti by malo byť **jednoduché**.

Digitálne podpisy možno rozdeliť do dvoch kategórií. Sú to:

- **priame digitálne podpisy** (direct digital signature)
- **verifikované digitálne podpisy** (arbitrated digital signatures).

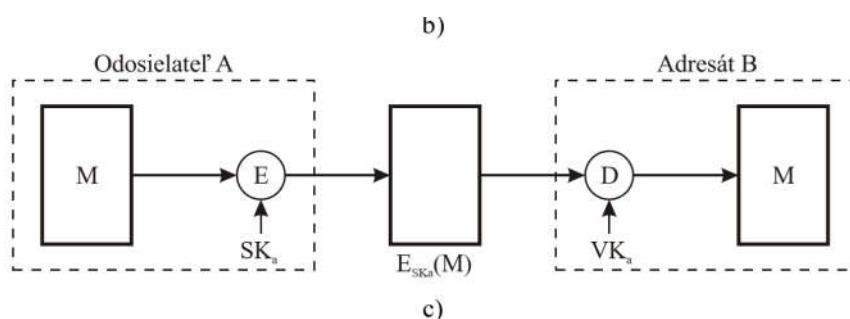
Priame digitálne podpisy

Priame digitálne podpisy (*Obr. 11.2a*) sú určené na komunikáciu, resp. výmenu dokumentov medzi dvoma subjektami (odosielateľ, adresát), pričom sa predpokladá, že oba subjekty vlastnia rovnaký tajný kľúč, ak sa komunikácia realizuje v kryptografickom systéme s tajným kľúčom alebo adresát pozná verejný kľúč, ak sa komunikácia realizuje v kryptografickom systéme s verejným kľúčom.



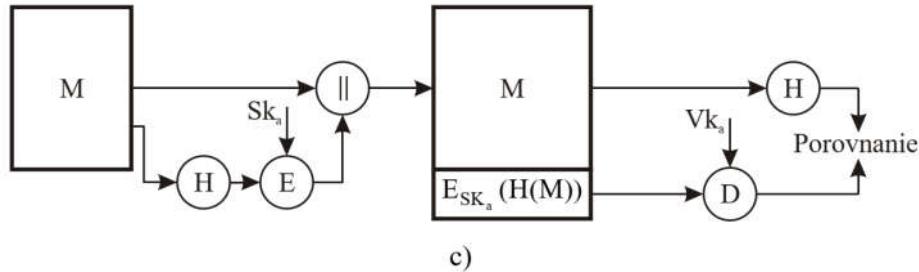
Obr. 11.2 a) komunikácia na báze priamych digitálnych podpisov
b) komunikácia na báze verifikovaných digitálnych podpisov

Digitálny podpis možno vytvoriť šifrovaním celej správy súkromným kľúčom odosielateľa, teda $E_{SK_x}(M)$ (*Obr. 9.1c*) alebo šifrovaním hašovacieho kódu správy M súkromným kľúčom odosielateľa,



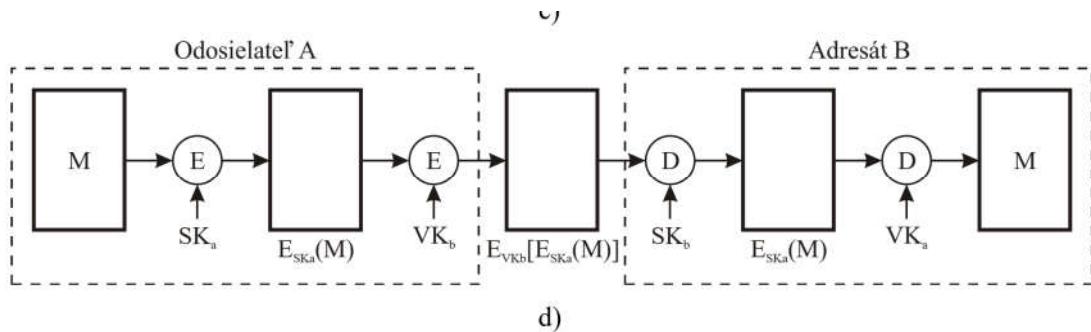
Obr. 9.1 Šifrovanie a dešifrovanie správy
c) Asymetrické šifrovanie: autentizácia a podpis

teda $E_{SK_x}(H(M))$ (Obr. 9.4c).

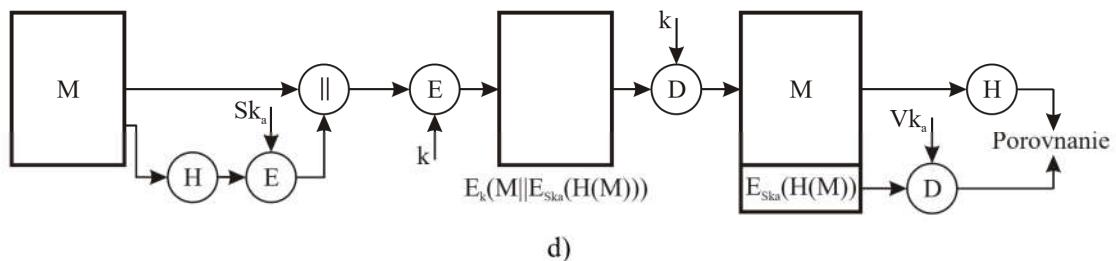


Obr. 9.4 Základný spôsob použitia hašovacej funkcie

Dôvernosť správy možno zabezpečiť nasledovným šifrovaním podpísanej správy verejným kľúčom adresáta, t. j. $E_{VK_y}(E_{SK_x}(M))$ v kryptografickom systéme s verejným kľúčom (Obr. 9.1d) alebo tajným kľúčom, t. j. $E_k(M \parallel E_{SK_x}(H(M)))$ a šifrovaním hašovacieho kódu správy M (Obr. 9.4d).



Obr. 9.1 Šifrovanie a dešifrovanie správy
d) Asymetrické šifrovanie: utajenie, autentizácia a podpis



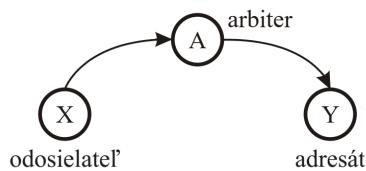
Obr. 9.4 Základný spôsob použitia hašovacej funkcie

V kryptografických systémoch zabezpečujúcich dôvernosť správy a digitálny podpis je nevyhnutné zachovať poradie operácií tak, že najprv je potrebné generovať digitálny podpis a až potom realizovať operácie na zabezpečenie dôvernosti správy.

Všetky postupy na generovanie digitálnych podpisov majú spoločnú **slabú stránku** a to je skutočnosť, že sú závislé na **bezpečnosti súkromného kľúča** odosielateľa, ktorá môže byť **ohrozená jeho stratou alebo odcudzením**.

Verifikované digitálne podpisy

Verifikované digitálne podpisy využívajú pri výmene dokumentov tretí dôverný subjekt (arbiter), ktorý rieši problémy spojené s generovaním priamych digitálnych podpisov (*Obr. 11.2b*).



Verifikované digitálne podpisy sú generované nasledovným postupom. Každá podpísaná správa odosielateľa X určená adresátovi Y sa **najprv odošle arbitrovi A**, ktorý podrobí správu a jej digitálny podpis **testom ich pôvodnosti**. Správa sa potom označí **časovým údajom** a odošle sa adresátovi Y s označením, že podpis **bol verifikovaný arbitrom**. Osvedčenie arbitrom vylučuje možnosť, že X nie je pôvodcom správy. Arbiter v metóde verifikovaných digitálnych podpisov má rozhodujúcu úlohu a uvedený prístup je založený **na dôvere komunikujúcich účastníkov k tomuto subjektu**.

Metóda verifikovaných digitálnych podpisov môže využívať tri základné postupy. Sú to:

- symetrické šifrovanie bez utajenia správy
- symetrické šifrovanie s utajením správy
- šifrovanie verejným kľúčom s utajením správy.

Symetrické šifrovanie bez utajenia správy predpokladá, že odosielateľ X a arbiter A vlastnia tajný kľúč k_{xa} a adresát Y a arbiter A vlastnia tajný kľúč k_{ay} . Odosielateľ X vytvára a odošle arbitrovi A správu v tvare

Symetrické šifrovanie bez utajenia správy predpokladá, že odosielateľ X a arbiter A vlastnia tajný kľúč k_{xa} a adresát Y a arbiter A vlastnia tajný kľúč k_{ay} . Odosielateľ X vytvára a odošle arbitrovi A správu v tvare

$$A \leftarrow X : M \| E_{k_{xa}}(ID_x \| H(M))$$

kde ID_x je identifikátor odosielateľa X

$E_{k_{xa}}(ID_x \| H(M))$ je digitálny podpis správy M

Arbiter A dešifruje digitálny podpis a vykoná kontrolu hašovacieho kódu prijatej správy a dešifrovanej hodnoty $H(M)$. Potom A vytvorí a odošle adresátovi Y správu v tvare

$$Y \leftarrow A : E_{k_{ay}}(ID_x \| M \| E_{k_{xa}}(ID_x \| H(M)) \| T)$$

Správa zašifrovaná kľúčom k_{ay} obsahuje identifikátor ID_x , originálnu správu M priatú od X, digitálny podpis overený arbitrom A a časovú pečiatku T.

Adresát Y priatú správu dešifruje kľúčom k_{ay} a získa identifikátor ID_x , ktorý dokazuje, že pôvodcom správy je X, originálnu správu M, jej digitálny podpis a časovú pečiatku T. Časová pečiatka T potvrzuje čas vytvorenia správy arbitrom A, teda to, že správa je časovo aktuálna a nie je to časovo oneskorený záznam správy.

$$A \leftarrow Y : E_{k_{ay}}(ID_x \| M \| E_{k_{xa}}(ID_x \| H(M)))$$

Arbiter A dešifruje túto správu kľúčom k_{ay} a získa ID_x , správu M a jej digitálny podpis, ktorý dešifruje kľúčom k_{xa} , čo mu umožní verifikovať hašovací kód $H(M)$ vytvorený odosielateľom X.

V uvedenom postupe adresát Y teda nemôže priamo realizovať verifikáciu digitálneho podpisu X a považuje správu M za autentickú, pretože pochádza od A. Tento postup je založený na dôvere X a Y k arbitrovi, teda, že:

- arbiter A neprezradí kľúč k_{xa} a teda nikto okrem X nemôže vytvoriť digitálny podpis v tvare $E_{k_{xa}}(ID_x \| H(M))$
- arbiter A posiela správu v tvare $E_{k_{ay}}(ID_x \| M \| E_{k_{xa}}(ID_x \| H(M)))$, iba ak hašovací kód $H(M)$ je správny a podpis bol generovaný odosielateľom X.

Zároveň je potrebné poznamenať, že v uvedenom postupe arbiter A je schopný čítať správu M, ktorá sa prenáša v otvorenom tvare, čo však znamená, že správa M nie je chránená pred monitorovaním (odpočúvaním) nepovolaným subjektom.

Symetrické šifrovanie s utajením správy oproti predošlému postupu zabezpečuje aj utajenie správy. V tomto postupe sa predpokladá, že navyše X a Y vlastnia rovnaký tajný kľúč k_{xy} , pričom X a A vlastnia kľúč k_{xa} , resp. Y a A vlastnia kľúč k_{ay} .

Odosielateľ X v tomto postupe vytvára a odošle arbitrovi A správu v tvare

$$A \leftarrow X : ID_x \| E_{k_{xy}}(M) \| E_{k_{xa}}\left(ID_x \| H(E_{k_{xy}}(M))\right)$$

Správa obsahuje identifikátor ID_x , správu M šifrovanú kľúčom k_{xy} a digitálny podpis šifrovanej správy M , vytorený X. Arbitr A dešifruje digitálny podpis zašifrovanej správy M , ktorý obsahuje ID_x a hašovací kód. V tomto postupe arbiter A pracuje so zašifrovanou verziou správy M , čo mu znemožňuje prístup k jej otvorenému tvaru.

Arbiter A potom vytvára správu, ktorá obsahuje všetko, čo prijal od X a pripojí ešte časovú pečiatku T . Túto správu zašifruje kľúčom k_{ay} a odošle adresátovi Y. Správy má teda tvar

$$Y \leftarrow A : E_{k_{ay}}\left(ID_x \| E_{k_{xy}}(M) \| E_{k_{xa}}\left(ID_x \| H(E_{k_{xy}}(M))\right)\| T\right)$$

Hoci arbiter A nie je schopný čítať správu M , ostáva napriek tomu v pozícii tretej dôvernej strany, ktorá zabraňuje falšovaniu zo strany odosielateľa X aj adresáta Y. Aj v tomto prípade je postup založený na dôvere k arbitrovi A.

Šifrovanie verejným kľúčom s utajením správy rieši všetky problémy, ktoré sú spojené so symetrickým šifrovaním. Jeden z možných postupov v šifrovaní verejným kľúčom používa tento sled operácií.

Odosielateľ X najprv šifruje správu M svojim súkromným kľúčom SK_x a výsledok potom šifruje verejným kľúčom adresáta Y, teda VK_y . Výsledok dvojnásobného šifrovania predstavuje podpísanú verziu správy M . Odosielateľ X potom vytvorí a odošle arbitroví správu v tvare

$$A \leftarrow X : ID_x \| E_{SK_x} (ID_x \| E_{VK_y} (E_{SK_x} (M)))$$

Arbiter A dešifruje časť správy verejným kľúčom VK_x , aby sa uistil, že správa pochádza od odosielateľa X, pretože iba X vlastní súkromný kľúč SK_x , ktorým bola táto časť správy zašifrovaná. Zvyšnú časť správy arbiter A nemôže dešifrovať, lebo nepozná súkromný kľúč adresáta Y, teda túto časť môže dešifrovať iba adresát Y.

Zároveň adresát A preverí skutočnosť, či pári kľúčov súkromný a verejný, ktorý bol vydaný odosielateľovi X je platný a verifikuje tak správu. Potom arbiter A odošle adresátori Y správu zašifrovanú svojim súkromným kľúčom SK_a v tvare

$$Y \leftarrow A : E_{SK_a} (ID_x \| E_{VK_y} (E_{SK_x} (M)) \| T)$$

Správy obsahuje identifikátor ID_x , dvojnásobne zašifrovanú správu a časovú pečiatku T .

Tento prístup má viacero výhod oproti predchádzajúcim postupom. Uvedené výhody spočívajú najmä v tom, že :

1. pred komunikáciou nie je potrebné definovať medzi komunikujúcimi stranami spoločné kľúče, ktoré v prípade kompromitácie narušia bezpečnosť systému. Každý účastník má pridelený verejný a súkromný kľúč
2. obsah správy od adresáta X je utajený nielen pred arbitrom, ale aj pred akýmkolvek ďalším subjektom.

Zároveň je však potrebné poznamenať, že nevýhodou tohto postupu je dvojnásobné šifrovanie, ktoré je typické pre šifrovanie algoritmami s verejným kľúčom.

Prehľad postupov vo verifikovaných digitálnych podpisoch je uvedený v Tab. 11.1.

Tab. 11.1 Verifikované digitálne podpisy

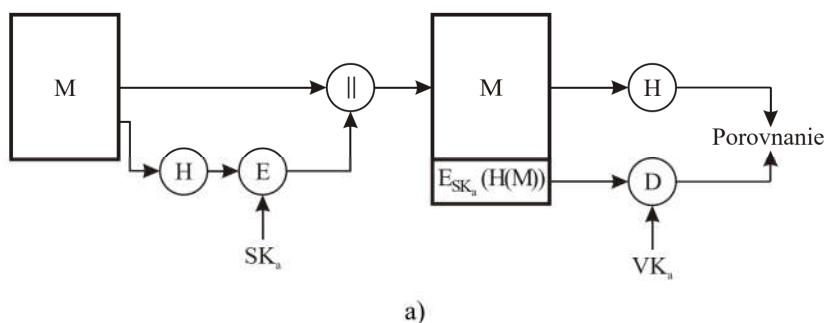
a. Symetrické šifrovanie bez utajenia správy
$A \leftarrow X : M \ E_{k_{xa}}(ID_x \ H(M))$
$Y \leftarrow A : E_{k_{ay}}(ID_x \ M \ E_{k_{xa}}(ID_x \ H(M)) \ T)$
b. Symetrické šifrovanie s utajením správy
$A \leftarrow X : ID_x \ E_{k_{xy}}(M) \ E_{k_{xa}}(ID_x \ H(E_{k_{xy}}(M)))$
$Y \leftarrow A : E_{k_{ay}}(ID_x \ E_{k_{xy}}(M) \ E_{k_{xa}}(ID_x \ H(E_{k_{xy}}(M))) \ T)$
c. Šifrovanie verejným kľúčom s utajením správy
$A \leftarrow X : ID_x \ E_{SK_x}(ID_x \ E_{rK_y}(E_{SK_x}(M)))$
$Y \leftarrow A : E_{SK_a}(ID_x \ E_{rK_y}(E_{SK_x}(M)) \ T)$

Štandardy pre digitálne podpisy

Prvý štandard pre digitálne podpisy publikovaný NIST v **roku 1991** bol štandard označovaný ako **DSS (Digital Signature Standard)** a používal algoritmus **DSA (Digital Signature Algorithm)**. Tento štandard bol revidovaný v roku 1993, resp. v roku 1996 a rozšírený v roku 2000. Najnovšia verzia zahrnuje aj algoritmus **digitálneho podpisu na báze RSA** a na **báze eliptických kriviek**.

V štandarde DSS sa používajú algoritmy, ktoré umožňujú **realizovať iba funkciu digitálnych podpisov a nemožno ich použiť na šifrovanie a distribúciu kľúčov**. To je rozdiel oproti postupu, ktorý na digitálny podpis využíva algoritmus RSA.

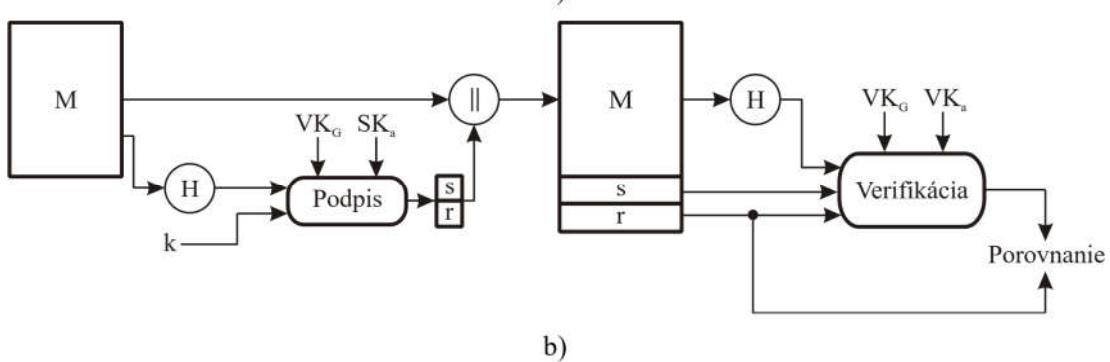
Porovnanie postupov DSS a RSA v digitálnych podpisoch je uvedené na *Obr. 11.3.*



Obr. 11.3 Postupy v digitálnych podpisoch
a) Digitálny podpis na báze RSA

V digitálnych podpisoch na báze RSA je správa M , ktorá sa má podpísat' vstupom pre hašovaciu funkciu H , ktorá produkuje hašovací kód $h=H(M)$ s konštantnou dĺžkou. Tento hašovací kód je potom zašifrovaný súkromným kľúčom odosielateľa a pripojí sa k správe M . Odosielateľ odosiela správu M a pripojený digitálny podpis tvorený $E_{SK_a}(H(M))$.

Adresát po obdržaní podpisanej správy dešifruje digitálny podpis verejným kľúčom odosielateľa VK_a čím získa $H(M)$. Z priatej správy vypočíta hašovací kód $H(M)$ a tento porovná s dešifrovanou hodnotou $H(M)$. Ak sa hašovacie kódy zhodujú, prijatá správa M je akceptovaná ako autentická, pretože iba odosielateľ vlastní, resp. pozná súkromný kľúč SK_a , ktorým bol realizovaný digitálny podpis.



Obr. 11.3 Postupy v digitálnych podpisoch
b) Digitálny podpis na báze DSS

Digitálny podpis na báze DSS využíva tiež hašovaciu funkciu, pričom hašovací kód predstavuje jeden zo vstupov funkcie, ktorá realizuje digitálny podpis (*Obr. 11.3b.*). Ďalšími vstupmi tejto funkcie je náhodné číslo k , generované pre konkrétny digitálny podpis, súkromný kľúč odosielateľa SK_a a verejný kľúč VK_G , ktorý môže používať skupina používateľov. Výsledok generovanie digitálneho podpisu je dvojica parametrov r, s , ktoré sa pripoja k originálnej správe M .

Na strane adresáta sa z priatej správy vypočíta hašovací kód, ktorý vstupuje do funkcie na verifikovanie digitálneho podpisu. Ďalšími vstupmi tejto funkcie sú prijaté parametre r, s , verejný kľúč odosielateľa VK_a a verejný kľúč VK_G . Výstup funkcie na verifikovanie digitálneho podpisu je hodnota, ktorá sa musí v prípade autentického podpisu rovnať parametru r .

Je potrebné tiež poznamenať, že funkcia na generovanie digitálneho podpisu sa vyznačuje tým, že iba odosielateľ, ktorý vlastní súkromný kľúč SK_a môže generovať autentický digitálny podpis.

Algoritmus digitálneho podpisu El Gamal

Bezpečnosť algoritmu DSA je založená na obtiažnosti výpočtu diskrétnych logaritmov a vychádza z algoritmu El Gamal.

Princíp použitia algoritmu El Gamal na digitálny podpis je uvedený na *Obr. 11.4.*

Algoritmus pozostáva z troch fáz. Sú to generovanie dvojice kľúčov (*VK* a *SK*), generovanie digitálneho podpisu, resp. podpísanie originálnej správy *M* a verifikácia digitálneho podpisu.

Generovanie súkromného a verejného kľúča je totožné s algoritmom El Gamal, ktorý sa používa na šifrovanie. Súkromný kľúč predstavuje číslo *x*, čísla *y*, *g* a *p* predstavujú verejný kľúč, pričom čísla *g* a *p* môže používať skupina používateľov.

Generovanie kľúčov odosielateľa	
Výber <i>p</i>	<i>p</i> – prvočíslo
Zvoľ <i>g</i> , <i>x</i>	náhodné čísla <i>g</i> < <i>p</i> , <i>x</i> < <i>p</i>
Vypočítaj	$y = g^x \text{ mod } p$
Verejný kľúč	$VK = \{y, g, p\}$
Súkromný kľúč	$SK = \{x\}$

Generovanie digitálneho podpisu	
Výber <i>k</i>	náhodné číslo, ktoré nie je súdeliteľné s $(p-1)$
Originálna správa	<i>M</i>
Podpis (dvojica <i>a</i> , <i>b</i>)	$a = g^k \text{ mod } p$ <i>b</i> je číslo, pre ktoré platí $M = (x.a + k.b) \text{ mod } (p-1)$

Verifikácia podpisu	
Podpis	<i>a</i> , <i>b</i>
Platnosť ak	$y^a a^b \text{ mod } p = g^{M'} \text{ mod } p$
<i>M'</i>	prijatá správa

Obr. 11.4 Princíp digitálneho podpisu na báze algoritmu El Gamal

Na generovanie digitálneho podpisu originálnej správy *M* je potrebné najprv zvoliť náhodné číslo *k*, ktoré nie je súdeliteľné s číslom $(p-1)$. Digitálny podpis je tvorený dvojicou parametrov *a*, *b*, pre ktoré platí

$$a = g^k \text{ mod } p$$

pričom parameter *b* musí spĺňať rovnicu

$$M = (xa + kb) \text{ mod } (p-1)$$

Verifikácia digitálneho podpisu je založená na overení platnosti vzťahu

$$y^a a^b \text{ mod } p = g^{M'} \text{ mod } p$$

kde *M'* – je prijatá verzia správy *M*.

↑
g!

Algoritmus DSA

Prvou fázou algoritmu DSA je generovanie troch parametrov, ktoré sú verejné a môže ich používať skupina používateľov. Sú to parametre p , q a g . Prvočíslo p sa volí v rozmedzí 512 až 1024 bitov, pričom je vždy násobkom 64, prvočíslo q má dĺžku 160 bitov, pričom je deliteľom čísla $(p-1)$. Číslo g možno vyjadriť v tvare $g = h^{(p-1)/q}$, pričom h je celé číslo v rozmedzí 1 až $(p-1)$ a zároveň pre h platí $h^{(p-1)/q} \bmod p > 1$.

Generovanie spoločných prvkov verejného kľúča	
p	prvočíslo, pričom $2^{L-1} \leq p \leq 2^L$ a zároveň platí $512 \leq L \leq 1024$, pričom L je vždy násobkom 64
q	prvočíslo, ktoré je deliteľom čísla $(p-1)$, pričom platí $2^{159} < q < 2^{160}$, t. j. q má dĺžku 160 bitov
g	číslo, pre ktoré platí $g = h^{(p-1)/q}$ pričom $1 < h < (p-1)$ a zároveň $h^{(p-1)/q} \bmod p > 1$

Generovanie kľúčov odosielateľa	
Súkromný kľúč	$SK_a = \{x\}$, pričom x je náhodné, resp. pseudonáhodné číslo, pre ktoré platí $0 < x < q$
Verejný kľúč	$VK_a = \{y\}$, pričom $y = g^x \bmod p$

Generovanie digitálneho podpisu	
k	pseudonáhodné číslo, pričom $0 < k < q$, ktoré musí byť utajené
Podpis (dvojica r, s)	$r = (g^k \bmod p) \bmod q$ $s = (k^{-1} (H(M) + r \cdot x)) \bmod q$ $H(M)$ – hašovacia funkcia SHA-1

Verifikácia digitálneho podpisu	
Výpočet w, u_1, u_2, v	$w = (s')^{-1} \bmod q$ $u_1 = (H(M') \cdot w) \bmod q$ $u_2 = (r' \cdot w) \bmod q$ $v = ((g^{u_1} \cdot y^{u_2}) \bmod q) \bmod p$
?	Test $v = r'$, pričom M', r', s' – prijaté verzie M, r, s

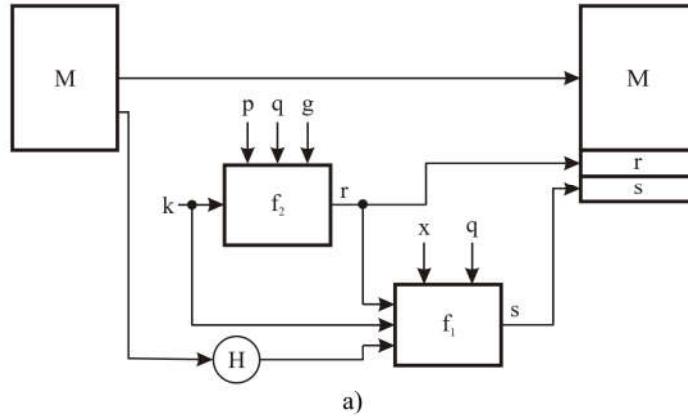
Obr. 11.5 Algoritmus DSA

Druhou fázou algoritmu DSA je generovanie súkromného a verejného kľúča odosielateľa. Súkromný kľúč SK_a je tvorený číslom x , pričom x je náhodné, resp. pseudonáhodné číslo v rozmedzí 1 až $(q-1)$. Verejný kľúč VK je tvorený číslom y , ktoré sa vypočita zo súkromného kľúča podľa vzťahu $y = g^x \text{ mod } p$. Je zrejmé, že výpočet y pre dané x a g , resp. p je relatívne ľahký. Zároveň platí, že výpočet x z y je obtiažný, pretože x je diskrétnym logaritmom y so základom g v module p .

Digitálny podpis je tvorený dvojicou hodnôt r, s , ktoré sú funkiami prvkov (p, q, g) , súkromného kľúča x , hašovacieho kódu $h=H(M)$ a náhodného, resp. pseudonáhodného čísla k , ktoré je jedinečné pre každý podpis.

Verifikácia digitálneho podpisu na prijímacej strane spočíva vo výpočte parametra w, u_1, u_2 , resp. v z prijatých verzií M' , r' , s' podľa vzťahov, ktoré sú uvedené na Obr. 11.5. Platnosť digitálneho podpisu potvrzuje rovnosť $v=r'$.

Struktúra generovania a verifikácie digitálneho podpisu na báze algoritmu DSA je uvedená na Obr. 11.6a, resp. Obr. 11.6b.

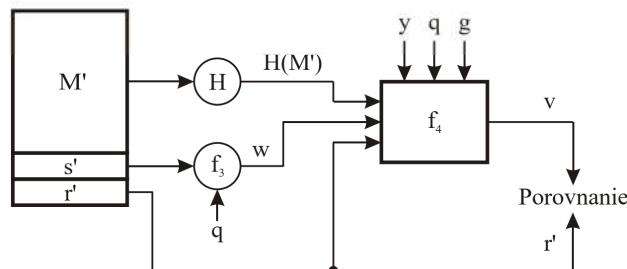


a)

$$s = f_1(H(M), k, x, r, g) = (k^{-1}(H(M) + x \cdot r)) \bmod q$$

$$r = f_2(k, p, q, g) = (g^k \bmod p) \bmod q$$

$H(M)$ – hašovacia funkcia SHA-1



b)

$$w = f_3(s', q) = (s')^{-1} \bmod q$$

$$v = f_4(y, q, g, H(M), w, r')$$

Obr. 11.6 a) generovanie digitálneho podpisu pomocou DSA
b) verifikácia digitálneho podpisu pomocou DSA

Uvedená štruktúra algoritmu odhaluje určité zvláštnosti, ktoré nie sú zrejmé bez podrobnejšej analýzy matematických vzťahov.

Zo štruktúry generovania digitálneho podpisu napr. vyplýva, že hodnota r , ktorá sa využíva na test autentičnosti podpisu na prijímacej strane vôbec nezávisí na správe M , ale je funkciou prvkov (p, q, g) , resp. čísla k . Parameter r možno teda vypočítať v predstihu. Zároveň je potrebné uviesť, že aj hodnota $y = g^k \text{ mod } p$ nezávisí na správe M , teda aj túto hodnotu možno vypočítať v predstihu. To isté platí aj pre výpočet inverzného čísla k^{-1} .

Digitálne podpisy na báze eliptických kriviek

Eliptické krivky možno použiť aj na účely digitálnych podpisov. Algoritmus pre digitálny podpis na báze eliptických kriviek sa označuje ako **algoritmus ECDSA** (Elliptic Curve Digital Signature Algorithm) a je určitou analógiou k algoritmu DSA.

Ak sa zúži výber eliptických kriviek pre ECDSA na malú množinu, potom sa **znížia náklady** na implementáciu a **nároky na energetickú náročnosť** technických prostriedkov systému na báze ECDSA, čo umožňuje implementáciu v čipových kartách a mobilných telefónoch.

Americký štandard FIPS 186–2 odporúča použitie 15 eliptických kriviek s rôznou úrovňou bezpečnosti pre aplikácie v štátnej správe. Uvedené krivky možno rozdeliť do troch skupín [42]. Sú to:

- prvočíselné eliptické krivky nad konečným poľom $GF(p)$
- binárne eliptické krivky nad konečným poľom $GF(2^n)$
- Koblitzove eliptické krivky nad konečným poľom $GF(2^n)$.

Podrobnejšie sa algoritmom ECDSA a eliptickými krivkami budeme zaoberať v **inžinierskom štúdiu**.

Porovnanie ekvivalentnej bezpečnosti DSA s ďalšími kryptografickými algoritmami je v nasledujúcej tabuľke.

Tab. 11.6 Ekvivalentná bezpečnosť kryptografických algoritmov

Ekvivalentná bezpečnosť [b]	Symetrické algoritmy	Algoritmy DSA DH	Algoritmus RSA	Eliptické krivky	Hašovacie funkcie
80	2DES	VK=1024 SK=160	$n = 1024$	$n = 160 - 223$	SHA-1
112	3DES	VK=2048 SK=224	$n = 2048$	$n = 224 - 255$	SHA-224
128	AES-128	VK=3072 SK=256	$n = 3072$	$n = 256 - 383$	SHA-256
192	AES-192	VK=7680 SK=384	$n = 7680$	$n = 384 - 511$	SHA-384
256	AES-256	VK=15360 SK=512	$n = 15360$	$n > 512$	SHA-512

Praktické skúsenosti s digitálnym podpisom - ROCA útok

<https://nukib.cz/cs/infoservis/hrozby/1460-roca-zranitelnost-v-generovani-rsa-klicu/>

Výskumníci z Masarykovej univerzity odhalili problémy s generovaním **RSA klúčov** v čipe použitom napr. aj v **SK občianskych preukazoch**. Podstata spočíva v tom, že aj napriek dostatočne kvalitnému TRNG, ktorý je implementovaný v použitom čipe, bol použitý rýchlejší **SW algoritmus generovania prvočísel**, ktorý mal podstatne **menšiu entropiu**. Problém s generovaním bol odhalený **bez znalosti a analýzy** použitej kryptografickej knižnice len s **využitím štatistickej analýzy** veľkého množstva verejných klúčov.

Následne opísaný útok umožnil z verejného klúča (aj veľkosti 2048 bitov) vypočítat' súkromný klúč. Na realizáciu útoku je potrebná výpočtová kapacita, ktorá je v dnešných podmienkach dostupná (aj keď nie úplne bežne resp. za zanedbateľnú cenu).

ROCA útok poukázal na **veľké zlyhanie** pri tvorbe elektronického podpisu a je **typickým príkladom ako implementácia kryptografických algoritmov v praxi nesmie realizovať**.

Manažment kľúčov v kryptografii s verejným kľúčom, využitie cerifikátov

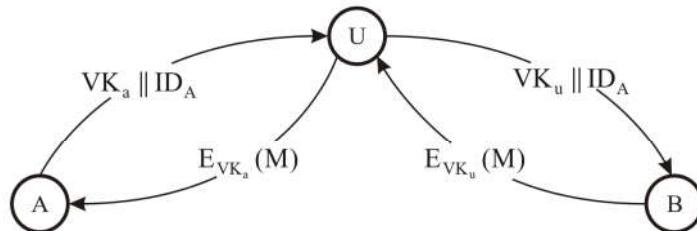
Veľký zlom v oblasti distribúcie tajných kľúčov priniesol **algoritmus Diffie–Hellman**, ktorý zároveň vytvoril podmienky na rozvoj kryptografie s verejným kľúčom.

Distribúcia kľúčov v kryptografii s verejným kľúčom zahŕňa dva aspekty. Sú to:

- distribúcia verejných kľúčov
- použitie šifrovania s verejným kľúčom na distribúciu tajných kľúčov.

Distribúcia verejných kľúčov

S distribúciou verejných kľúčov súvisí možnosť podvrhnutia **verejného kľúča**, ktorá predstavuje ohrozenie bezpečnosti kryptografických systémov s verejným kľúčom. Princíp podvrhnutia verejného kľúča je uvedený na Obr. 8.1.



Obr. 8.1 Podvrhnutie verejného kľúča

Subjekt A zašle svoj verejný kľúč VK_a spolu so svojim identifikátorom ID_A , t. j. správu v tvare $VK_a||ID_A$ subjektu B. Nepovolaný subjekt (útočník) U, ktorý má prístup k verejnemu kanálu zachyti správu vysielanú subjektom A, vytvorí novú správu v tvare $VK_u||ID_A$ a odošle ju subjektu B. Nepovolaný subjekt U teda podvrhol svoj verejný kľúč VK_u subjektu B, ktorý takto predpokladá, že $VK_u=VK_a$.

Dôsledky podvrhnutia verejného kľúča subjektu U sú také, že subjekt B zašifruje každú správu M kľúčom VK_u , t. j. vytvorí zašifrovanú správu v tvare $E_{VK_u}(M)$ a odošle ju A. Nepovolaný subjekt U zachyti túto správu, dešifruje ju svojim súkromným kľúčom SK_u a získa tak správu M . Pretože subjekt U pozná verejný kľúč A, vytvorí a odošle A správu v tvare $E_{VK_a}(M)$.

Podvrhnutie verejného kľúča subjektu U teda umožňuje tomuto subjektu čítať korešpondenciu medzi subjektom A a B bez toho, aby jeho činnosť bola detegovateľná.

Distribúciu verejných kľúčov možno realizovať viacerými technikami, ktoré zahŕňajú tieto všeobecné postupy:

- zverejnenie verejných kľúčov (public announcement)
- verejne dostupný adresár (publicly available directory)
- autorita pre verejné kľúče (public-key authority)
- **certifikácia verejných kľúčov** (public-key certificates).

V ďalšej časti opíšeme len **certifikáty** „verejných kľúčov“, ich štruktúru a význam. Tieto informácie budú využité v cvičeniaciach pri **generovaní certifikátov** napr. pomocou **OpenSSL**.

Techniky distribúcie verejných kľúčov a techniky distribúcie tajných kľúčov sú podrobnejšie opísané v [1, str.165-175].

Využitie certifikátov a certifikačnej autority

Použitie certifikátov predstavuje alternatívny prístup v **distribúcii verejných kľúčov**, ktoré umožňujú realizovať výmenu kľúčov bez kontaktu s tretou dôverou stranou.

Uvedený prístup vyžaduje definovať dva pojmy a to:

- **certifikáty** (certificates)
- **certifikačná autorita** (certification authority).

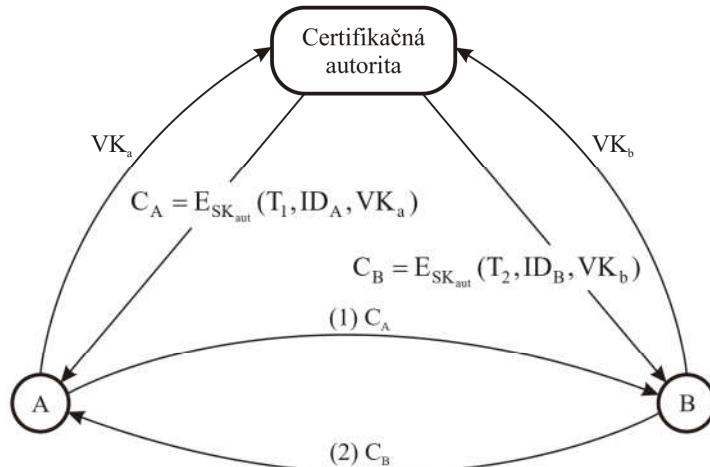
Certifikát je údajová štruktúra, ktorá obsahuje verejný kľúč žiadateľa, resp. držiteľa certifikátu, identifikačné údaje držiteľa certifikátu, časový údaj, ktorý sa vzťahuje k dobe platnosti certifikátu a iné údaje vytvorené certifikačnou autoritou. Táto štruktúra je podpísaná súkromným kľúčom certifikačnej autority (SK_{aut}), pričom akýkoľvek účastník môže verifikovať obsah certifikátu pomocou verejného kľúča certifikačnej autority (VK_{aut}).

Certifikačná autorita je tretia dôverná strana, ktorá na základe žiadosti vydáva a aktualizuje certifikáty, pričom každý účastník môže verifikovať to, že certifikát bol vytvorený certifikačnou autoritou pomocou jej verejného kľúča (VK_{aut}).

Žiadosť o vydanie certifikátu možno certifikačnej autorite doručiť osobne alebo elektronicky s využitím bezpečnej komunikácie. Prijímanie žiadosti, kontrolovanie súladu údajov v žiadosti o vydanie certifikátu a odovzdávanie certifikátov žiadateľom sa realizuje **registračnou autoritou**.

Výmena verejných kľúčov na báze certifikátov

Princíp výmeny verejných kľúčov na báze certifikátov je uvedený na Obr. 8.4.



Obr. 8.4 Distribúcia verejných kľúčov pomocou certifikátov

Účastník A pred započatím akejkoľvek komunikácie požiada certifikačnú autoritu o vydanie certifikátu na svoj verejný kľúč VK_a . Certifikačná autorita vydá certifikát C_A pre účastníka A, ktorý obsahuje dobu platnosti certifikátu (T_1), identifikačné údaje A (ID_A) a verejný kľúč A (VK_a). Túto štruktúru podpiše svojim súkromným kľúčom SK_{aut} a odošle A. Certifikát vydaný pre A má potom tvar

$$C_A = E_{SK_{aut}}(T_1, ID_A, VK_a)$$

Certifikát v uvedenej forme možno poskytnúť účastníkovi, ktorý ho môže zverejniť, pretože obsah certifikátu možno čítať, resp. verifikovať verejným kľúčom certifikačnej autority. Teda platí

$$D_{VK_{aut}}(C_A) = D_{VK_{aut}}\left(E_{SK_{aut}}(T_1, ID_A, VK_a)\right) = (T_1, ID_A, VK_a)$$

Proces dešifrovania certifikátu verejným kľúčom certifikačnej autority VK_{aut} je zároveň verifikáciou toho, že bol vytvorený certifikačnou autoritou. Dešifrovaním sa získa meno a verejný kľúč držiteľa certifikátu, pričom časový údaj T_1 potvrzuje platnosť certifikátu, resp. vymedzuje dobu platnosti certifikátu.

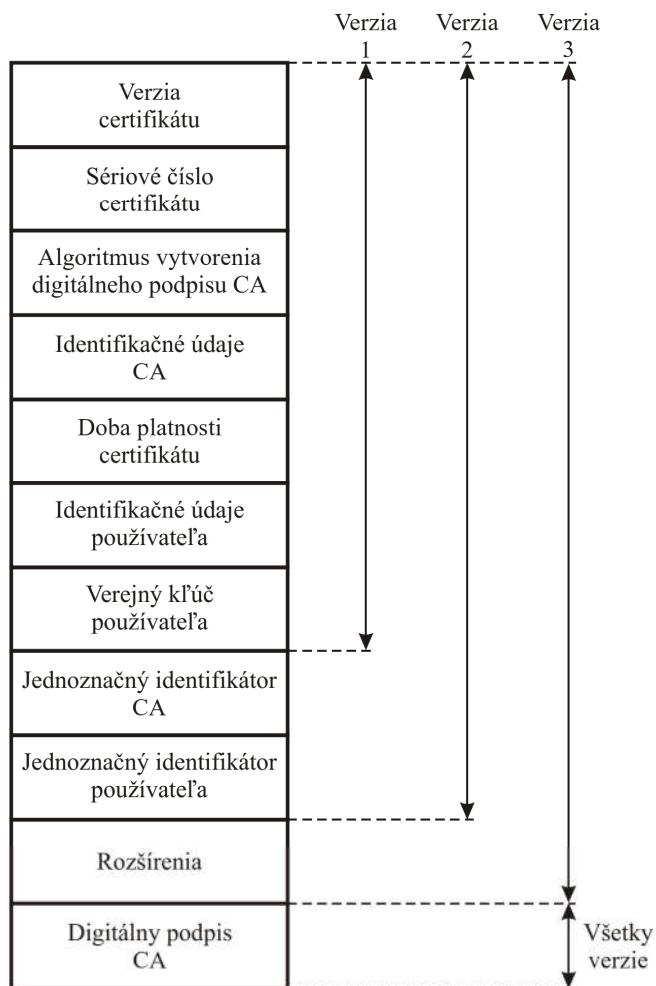
Analogicky požiada o vydanie certifikátu aj účastník B, pričom C_B má rovnakú štruktúru ako C_A .

Distribúcia verejných kľúčov spočíva potom vo výmene certifikátov medzi účastníkmi komunikácie.

Certifikáty podľa odporúčania X.509

Formáty certifikátov určuje odporúčanie ITU-T X.509, ktoré je časťou odporúčania X.500. Odporúčanie X.509 definuje tiež **autentizačné protokoly**, ktoré sa používajú v rôznych **typoch sietí** a v rôznych **aplikáciách sieťovej bezpečnosti**.

Všeobecný formát certifikátov podľa odporúčania X.509 je uvedený na *Obr. 8.5* a obsahuje tieto položky:



Obr. 8.5 Formáty certifikátov podľa odporúčania X.509

Verzia certifikátu (Version) udáva jednu z troch verzií certifikátu (1, 2 alebo 3), ktoré sa líšia celkovým počtom položiek certifikátu a sú definované v odporúčaní X.509.

Sériové číslo certifikátu (Serial number) je definované ako celé nezáporné číslo, ktoré je pridelené na označenie daného certifikátu certifikačnou autoritou (CA). Sériové číslo musí byť v rámci danej certifikačnej autority jednoznačné, t. j. certifikačná autorita nesmie vydať dva certifikáty s rovnakým sériovým číslom.

Algoritmus vytvorenia digitálneho podpisu CA (Signature algorithm identifier) je položka, ktorá obsahuje informácie o algoritme, ktorý bol použitý na podpis certifikátu a príslušné parametre tohto podpisu.

Identifikačné údaje CA (Issuer) je položka, ktorá obsahuje meno CA v zmysle odporúčania X.500, ktorá vydala certifikát. Certifikačná autorita CA by mala mať jednoznačnú identifikáciu, t. j. jedinečné meno v rámci všetkých certifikačných autorít.

Doba platnosti certifikátu (Period of validity) je položka určujúca platnosť certifikátu, obsahuje dva časy, t. j. odkedy a dokedy certifikát platí.

Identifikačné údaje používateľa (Subject name) je položka, ktorá obsahuje jedinečné meno subjektu, ktorému je certifikát vydaný, t. j. obsahuje identifikáciu držiteľa certifikátu, ktorý je vlastníkom súkromného kľúča zodpovedajúceho certifikovanému verejnemu kľúču.

Verejný kľúč používateľa (Subject's public-key) je položka, ktorá obsahuje dve položky a to identifikátor algoritmu, pre ktorý je verejný kľúč určený a samotný verejný kľúč.

Odporúčanie X.509 vo verzii 2 definuje ďalšie dve položky certifikátu. Sú to:

Jednoznačný identifikátor CA (Issuer unique identifier) je položka určená pre jednoznačnú identifikáciu CA v prípade, že meno CA v položke Identifikačné údaje CA (Issuer) bolo použité v rôznych CA, resp. keď táto položka nepostačuje na jednoznačnú identifikáciu CA.

Jednoznačný identifikátor používateľa (Subject unique identifier) je obdobná položka ako predošlá a týka sa používateľa, t. j. držiteľa certifikátu.

Položka **Rozšírenie** (Extension) definovaná vo verzii 3 obsahuje ďalšie informácie o kľúčoch CA a používateľa, o identifikátoroch CA a používateľa ako aj o certifikačnej politike a obmedzeniach týkajúcich sa vydávania certifikátov.

Digitálny podpis CA (Signature of CA) obsahuje hašovací kód⁽¹⁾ ostatných položiek certifikátu, ktorý je zašifrovaný súkromným kľúčom CA.

Certifikáty používateľov vydávané certifikačnou autoritou musia mať tieto vlastnosti:

- ktorýkoľvek účastník prostredníctvom verejného kľúča CA môže verifikovať certifikované verejné kľúče iných účastníkov
- žiadny iný subjekt než CA **nemôže modifikovať** vydané certifikáty.

Pretože certifikáty sú nefalšovateľné, teda môžu sa **umiestňovať** v **adresári CA**, ktorý je prístupný všetkým používateľom, pričom **adresár nevyžaduje osobitnú ochranu**. To platí v prípade, že všetci používatelia používajú služby jedinej (spoločnej) CA.

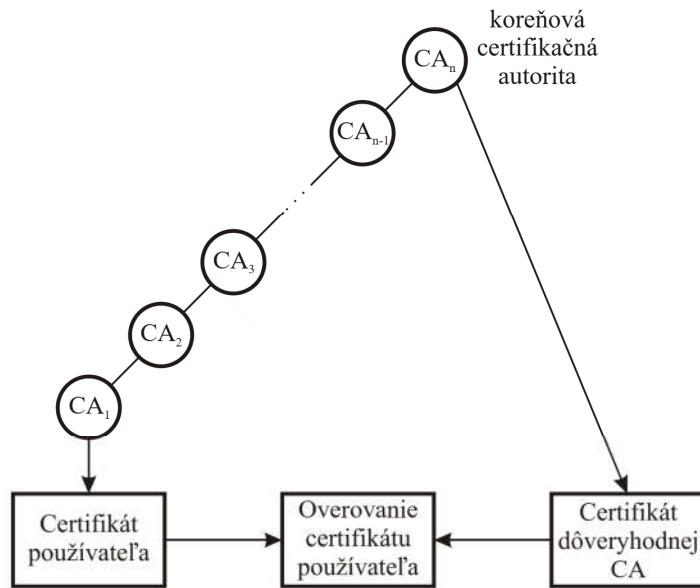
Uvedená koncepcia je **nevýhodná** pri **veľkom počte používateľov**. Pretože CA podpisuje všetky certifikáty svojim súkromným kľúčom, každý používateľ musí mať kópiu verejného kľúča CA, ktorý je potrebný na verifikáciu podpisu CA. Pri **veľkom počte** používateľov je preto výhodnejšie **vytvoriť viaceré certifikačné autority**, ktoré by vydávali certifikáty pre určitý okruh používateľov.

Vytvorenie viacerých certifikačných autorít však generuje problém certifikátov vydaných rôznymi certifikačnými autoritami, resp. problém distribúcie verejných kľúčov pomocou certifikátov vydaných rôznymi CA.

Predpokladajme napr., že používateľ A získal certifikát od certifikačnej autority CA₁ a používateľ B získal certifikát od certifikačnej autority CA₂. Pretože používateľ A nepozná verejný kľúč CA₂, nemôže používateľ A verifikovať certifikát používateľa B a naopak používateľ B nemôže verifikovať certifikát používateľa A. Riešením je certifikácia CA₁ a CA₂ treťou certifikačnou autoritou CA₃, čím vzniká **certifikačný strom**. Koreň stromu reprezentuje **koreňová certifikačná autorita**, ktorá vlastní **koreňový certifikát**. Koreňový certifikát je podpísaný súkromným kľúčom koreňovej certifikačnej autority, **teda sebou samým**.

Postupnosť certifikátov od certifikátu používateľa k certifikátu koreňovej certifikačnej autority sa nazýva **reťaz certifikátov**.

Na Obr. 8.6 je znázornený prípad, kde CA_n je koreňová certifikačná autorita. Medzi používateľom a touto koreňovou certifikačnou autoritou sa nachádzajú certifikačné autority $CA_1, CA_2, \dots, CA_{n-1}$. Reťaz certifikátov teda pozostáva z certifikátu používateľa, z certifikátov $CA_1, CA_2, \dots, CA_{n-1}$ a koreňového certifikátu CA_n , ktorý je podpísaný CA_n .

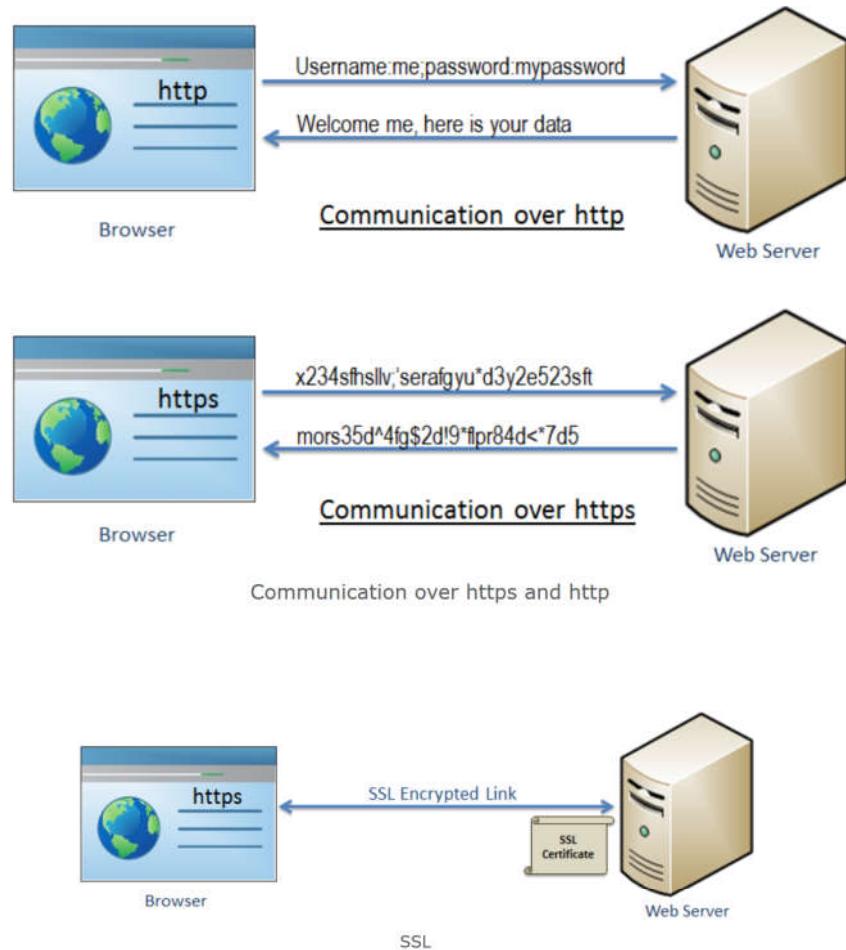


Obr. 8.6 Ret'az certifikátov

Za dôveryhodný certifikát nie je vždy nutné prehlásiť koreňový certifikát. Ak sa za dôveryhodný certifikát prehlási niektorý z certifikátov v reťazci certifikátov, potom sa overovanie platnosti realizuje iba k tomuto dôveryhodnému certifikátu a proces overovania sa týmto zrýchli.

Praktický príklad využitia certifikátov v sietovej komunikácii – https protokol a SSL certifikáty

<https://www.tutorialsteacher.com/https/what-is-https>



http vs https

http	https
Transfers data in hypertext (structured text) format	Transfers data in encrypted format
Uses port 80 by default	Uses port 443 by default
Not secure	Secured using SSL technology
Starts with <code>http://</code>	Starts with <code>https://</code>

V praxi sa najčastejšie stretávame s takýmto zobrazením certifikátov (napr. pri spojení na <https://mail.tuke.sk>)

The image contains two side-by-side screenshots of a web browser window. Both screenshots show the URL <https://mail.tuke.sk/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fmail.tuke.sk%2fowa%2f%23authRedirect%3dtrue>.

Screenshot 1 (Left): Site Information for mail.tuke.sk

- Connection:** Secure Connection
- Content Blocking:** Standard (Standard)
- Permissions:** You have not granted this site any special permissions.
- Buttons:** Clear Cookies and Site Data...

Screenshot 2 (Right): Outlook Login Screen

- Outlook Logo:** Outlook
- Fields:** User name: [redacted], Password: [redacted]

Screenshot 3 (Bottom Left): Site Security

- Site:** mail.tuke.sk (Secure Connection)
- Verifier:** Verified by: TERENA
- Buttons:** More Information

The screenshot shows the Microsoft Edge 'Page Info' dialog box for the URL <https://mail.tuke.sk/owa/auth/logon.aspx?replaceCurrent=1&url=https://mail.tuke.sk>. The tabs at the top are General, Media, Permissions, and Security, with Security selected. The 'Website Identity' section shows the website as mail.tuke.sk and notes that ownership information is not supplied. It was verified by TERENA and expires on Thursday, May 7, 2020. A 'View Certificate' button is available. The 'Privacy & History' section includes questions about previous visits (Yes, 11 times), cookie storage (Yes, cookies and 1.9 MB of site data), and saved passwords (No). Buttons for 'Clear Cookies and Site Data' and 'View Saved Passwords' are present. The 'Technical Details' section states that the connection is encrypted using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 with 128 bit keys, and TLS 1.2. It also mentions that the page was encrypted before transmission over the Internet. A note explains that encryption makes it difficult for unauthorized people to view information traveling between computers.

Certificate Detail

General Details

This certificate has been verified for the following uses:

- SSL Client Certificate**
- SSL Server Certificate**

Issued To

Common Name (CN) mail.tuke.sk
 Organization (O) Technická univerzita v Košiciach
 Organizational Unit (OU)
 Serial Number 08:41:D9:5B:25:00:90:5D:C5:EA:1B:90:D4:28:BF:47

Issued By

Common Name (CN) TERENA SSL CA 3
 Organization (O) TERENA
 Organizational Unit (OU)

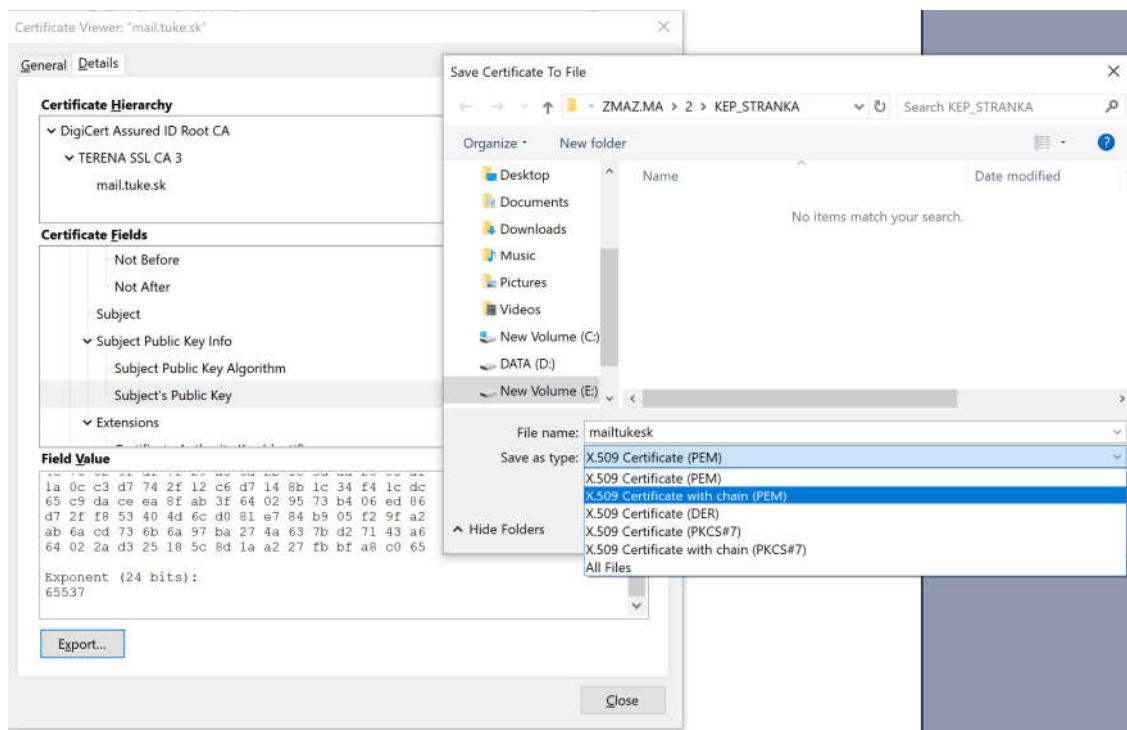
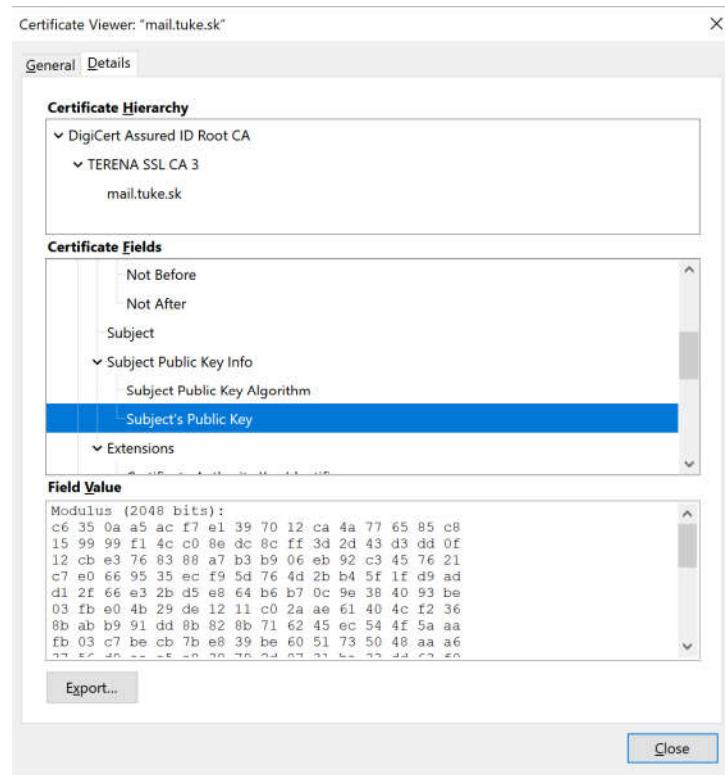
Period of Validity

Begins On Thursday, May 3, 2018
 Expires On Thursday, May 7, 2020

Fingerprints

SHA-256 Fingerprint	36:0D:E1:4B:EB:84:C4:88:28:95:C9:9F:90:70:FB:9A: 42:B4:37:E0:2C:5E:B1:5D:0C:F3:86:A9:2D:CD:09:02
SHA1 Fingerprint	D0:8F:E3:7E:BE:6C:84:53:71:87:92:00:72:ED:9D:43:41:28:C9:39

OK



Operačný systém a tiež **inštalované prehliadače** obsahujú **predinštalované verejné klúče** vybraných **certifikačných autorít** (napr. Verisign, TERRENA, ...).

Užívateľ môže do systému nahráť aj **verejný klúč vlastnej CA**. Klúče pre PKI infraštruktúru a **certifikáty** je možné generovať vo vhodných nástrojoch. Na cvičení bude využívaný **nástroj OpenSSL**.