



NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Sekcia informačnej bezpečnosti a elektronického podpisu

Budatínska č. 30, P.O. BOX 16, 850 07 Bratislava 57
tel: 02 - 6869 1111

<http://www.nbusr.sk/>
e-mail: info@nbusr.sk

Elektronický podpis

časť I. – Základy EP

Definícia elektronického podpisu

- **Elektronický podpis je informácia pripojená alebo logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:**
 - nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča a elektronického dokumentu,
 - na základe znalosti tejto informácie a verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení možno overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, je zhodný s elektronickým dokumentom použitým na jej vyhotovenie.

(§ 3 ods. 1 zákona NR SR č. 215/2002 Z.z. o elektronickom podpise)

Vzt'ah „podpis“ a „elektronický podpis“

- Formálne, z právneho hľadiska sú ekvivalentné. Elektronický podpis však zaručuje, že dokument od okamihu podpisu nebol zmenený, jednoznačne identifikuje podpisovateľa a, ak je to potrebné, aj čas podpisu.

Základné vlastnosti el. podpisu:

- **identifikácia autora**
- **integrita**
- **nepopierateľnosť autorstva**
- **nemožnosť podpísať prázdny dokument**

Identifikácia autora:

- spôsob vyhotovenia a overenia elektronického podpisu umožňuje spoľahlivo určiť, ktorá fyzická osoba el. podpis vyhotovila

Integrita:

- neporušenost' dokumentu
- pozitívne overenie el. podpis zaručuje, že dokument nebol po podpise, napr. počas prenosu zmenený, upravovaný alebo poškodený

Nepopierateľnosť autorstva:

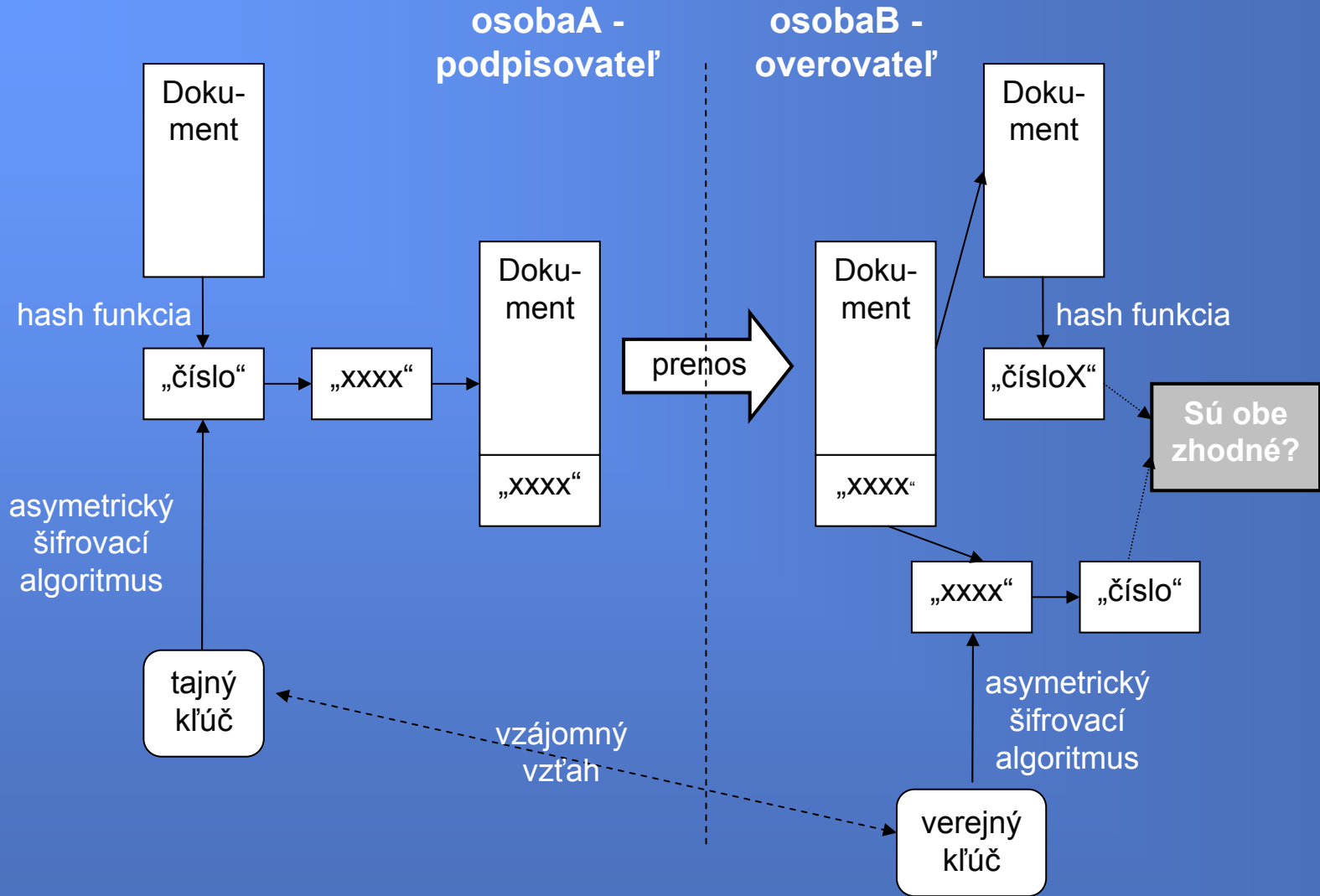
- jednoznačné priradenie autorstva dokumentu podpisovateľovi
- nemožnosť odoprenia autorstva dokumentu

Nemožnosť podpísať prázdny dokument :

- je vylúčené, resp. nie je možné podpísať „bianco“ dokumentu

Postup pri vyhotovovaní a overovaní el. podpisu

- **El. podpis má podobu krátkeho elektronického súboru. (Nie „zoskenovaný“ ručný podpis.) Vznikne spracovaním podpisovaného elektronického dokumentu a súkromného kľúča v prostriedku, ktorého jediným a výlučným vlastníkom je podpisovateľ. Takto spracovaný elektronický súbor sa napokon pripojí k podpisovanému dokumentu (vid'. obr. č. 1).**



Obr. 1.: Princíp elektronického podpisu

Hash funkcia (odtlačok):

- **matematická transformácia, ktorá digitálnym dokumentom rozličnej dĺžky priradí také čísla vopred ustanovenej nenulovej pevnej dĺžky, že umožňujú overiť integritu digitálneho dokumentu, z ktorého boli odvodené transformáciou a nemožno z nich spätne odvodiť digitálny dokument**

(§ 2 písm. e) vyhlášky NBÚ č. 537/2002 Z.z. o formáte a spôsobe vyhotovenia zaručeného el. podpisu, ...)

Základné vlastnosti hash funkcie:

- **jednocestná**
 - z hodnoty hash funkcie nemožno vypočítať dokument
- **jedinečná pre každý dokument**
 - každý jeden dokument má inú hodnotu hash funkcie
 - čiže aj dokumenty odlišujúce sa v čo len jednom jedinom znaku (bite) majú rozdielne hodnoty hash funkcie
 - pri (x) opakovaní výpočtu hodnoty hash funkcie toho istého dokumentu dostaneme vždy rovnakú hodnotu hash funkcie (neplatí pre použitie iného algoritmu výpočtu hodnoty hash funkcie)
- **konštantná dĺžka**
 - dĺžka hodnoty hash funkcie je pre každý dokument rovnaká (závisí od typu hash funkcie)

Základné typy hash funkcie:

- **MD5** (128 Bit)
- **SHA-1** (160 Bit)
- **RIPEMD-160** (160 Bit)

Šifrovanie:

- **symetrické šifrovanie**

- jeden kľúč sa používa aj na šifrovanie aj na odšifrovanie
- komunikujúce strany musia mať bezpečným spôsobom zabezpečenú výmenu tajných kľúčov
- na komunikáciu s (n) osobami musí byť stanovených (n) tajných kľúčov
- napr. DES, 3DES, BLOWFISH, IDEA, Rijndael, ...

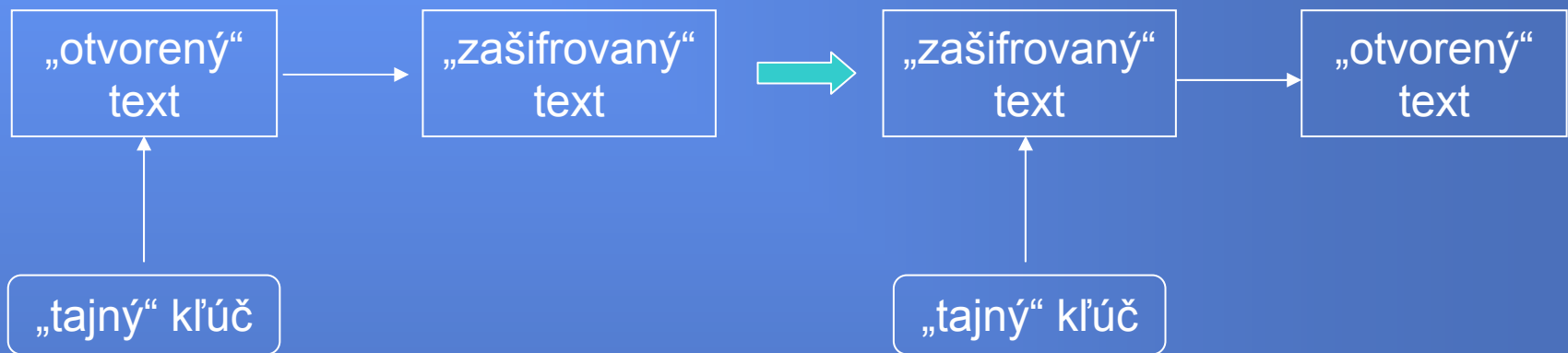
- **asymetrické šifrovanie**

- využíva sa tzv. kľúčový pár (tajný a verejný kľúč)
- jeden kľúč (verejný) sa používa na šifrovanie a druhý (tajný) na odšifrovanie
- verejným kľúčom príjemcu správy sa dokument zašifruje a len príjemca správy pomocou svojho tajného kľúča dokáže správu odšifrovať
- text zašifrovaný verejným kľúčom možno odšifrovať len prislúchajúcim tajným kľúčom
- text zašifrovaný verejným kľúčom už nemožno odšifrovať tým istým verejným kľúčom
- na komunikáciu s (n) osobami stačí použiť ten istý kľúčový pár
- napr. RSA, DSA, ECDSA-Fq, ECC, ElGamal, ...

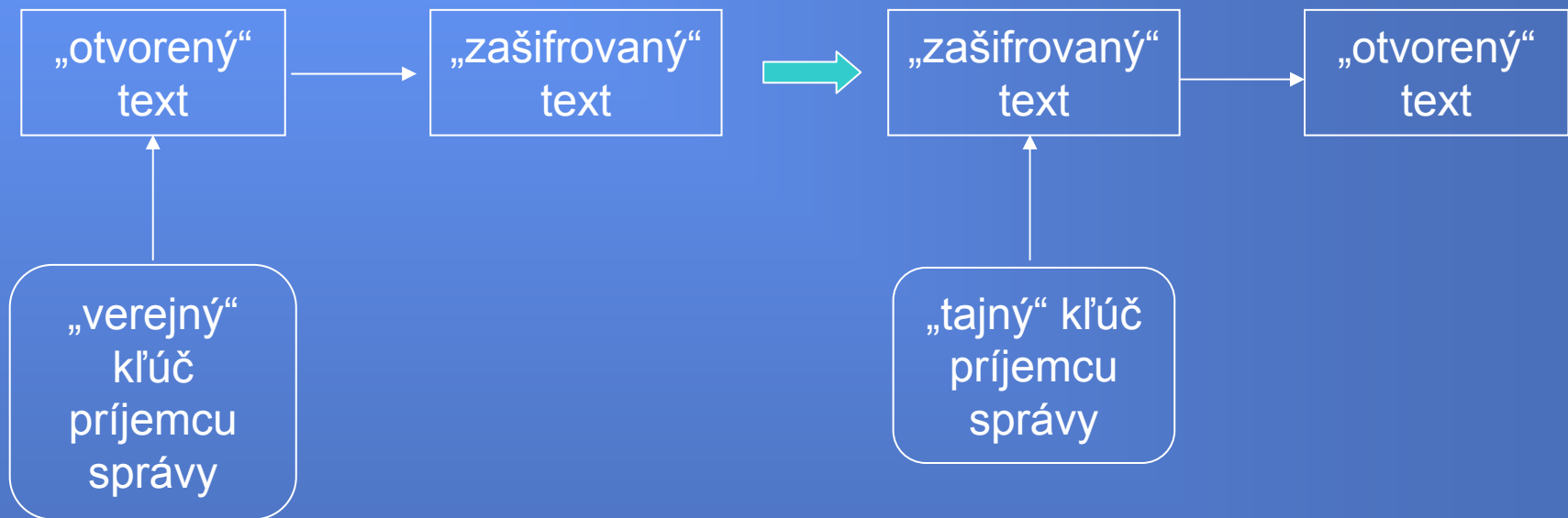
- **podpisovanie pomocou asymetrického šifrovania**

- v prípade podpisovania sa hash dokumentu zašifruje tajným kľúčom podpisovateľa a odšifruje verejným kľúčom podpisovateľa
- podpis môže vytvoriť len podpisovateľ, pretože len on pozná svoj tajný kľúč
- keďže verejný kľúč podpisovateľa je známy všetkým overovateľom tak si všetci môžu overiť pravosť podpisu
- hash dokumentu zašifrovaný tajným kľúčom už nemožno odšifrovať tým istým tajným kľúčom

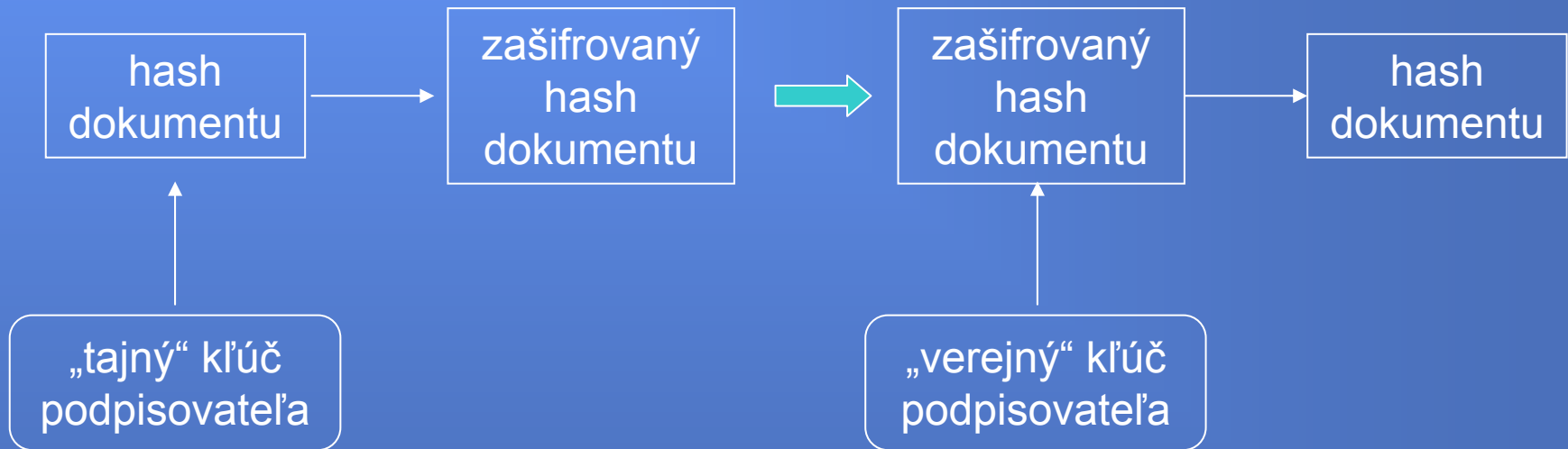
Symetrické šifrovanie:

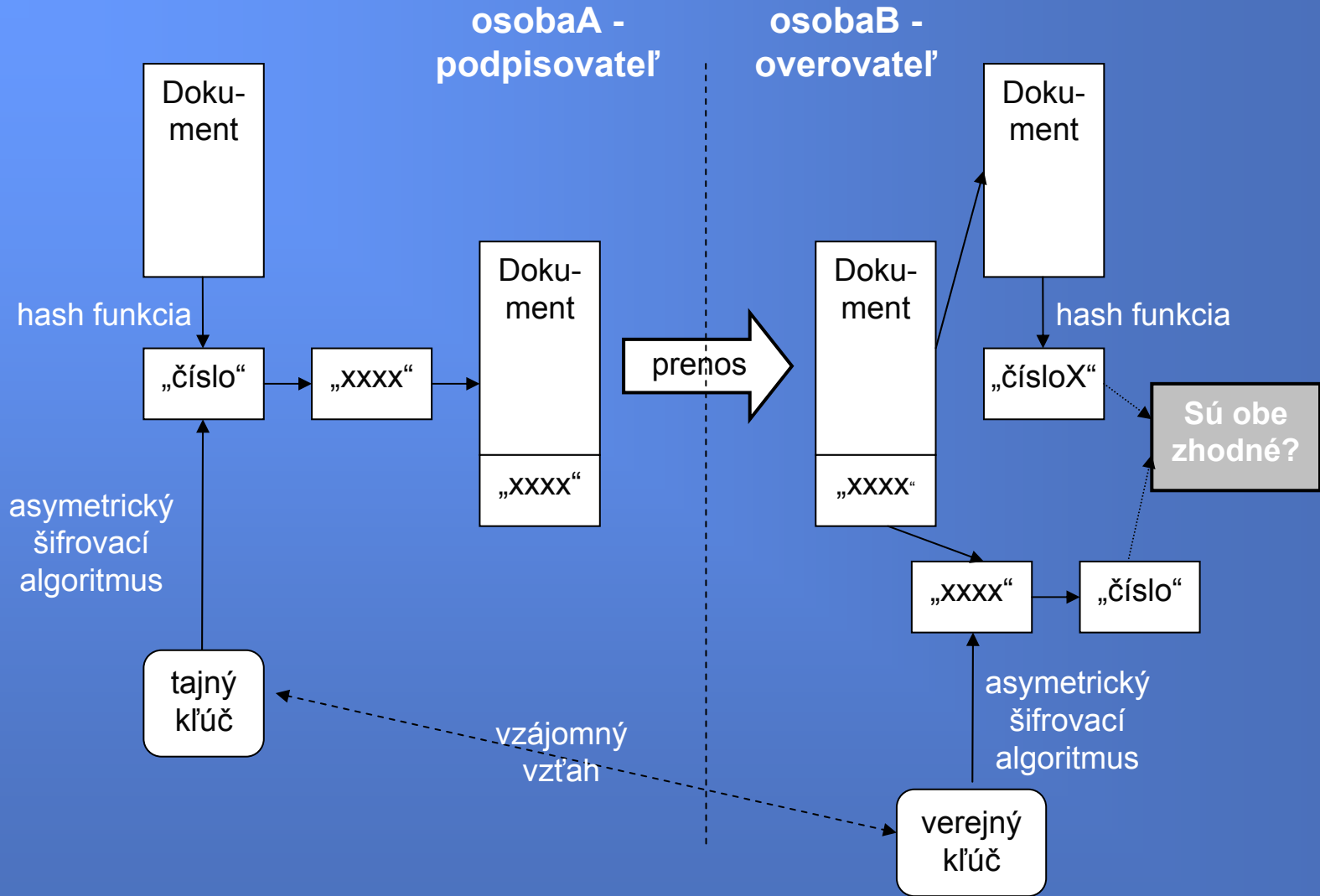


Asymetrické šifrovanie:



Podpisovanie pomocou asymetrického šifrovania:





Obr. 1.: Princíp elektronického podpisu



RSA algoritmus:

N – modul

$\Phi(N)$ – Eulerova funkcia

p, q – prvočísla

e – šifrovací (verejný) exponent

d – dešifrovací (súkromný) exponent

N, e – verejný kľúč

N, d – súkromný kľúč

p, q, d, Φ - znalosť jedného z týchto čísiel vedie k nájdeniu zbývajúcich troch
a znalosť d dáva algoritmus pre faktorizáciu čísla N

NSD – najväčší spoločný deliteľ

NSN – najmenší spoločný násobok

M – zasielaná správa

m – číselne vyjadrená správa

c – zašifrovaná správa

$$N = p * q$$

$$\Phi(N) = (p-1)*(q-1)$$

náhodne zvolené

zvolí sa podľa $e*d = 1 \text{ mod } \Phi(N)$

$$d = e^{-1} \text{ mod } ((p-1)*(q-1))$$

$$m_i = c_i^d \text{ mod } N$$

$$c_i = m_i^e \text{ mod } N$$

Postup vytvorenia kľúčového páru:

1. náhodne vygenerujeme dve veľké prvočísla (p) a (q)
2. vypočítame číslo N a číslo $\Phi(N)$
3. zvolíme náhodné číslo e podľa $1 < e < \Phi(n)$, tak že $\text{NSD}(e, \Phi(N))=1$, t.j. e a $\Phi(N)$ sú nesúdeliteľné
4. použitím Euklidovho algoritmu vypočítame číslo d také, že $1 < d < \Phi(N)$ a $e*d=1 \text{ mod } \Phi(N)$

Šifrovanie:

$$c_i = m_i^e \text{ mod } N$$

Dešifrovanie:

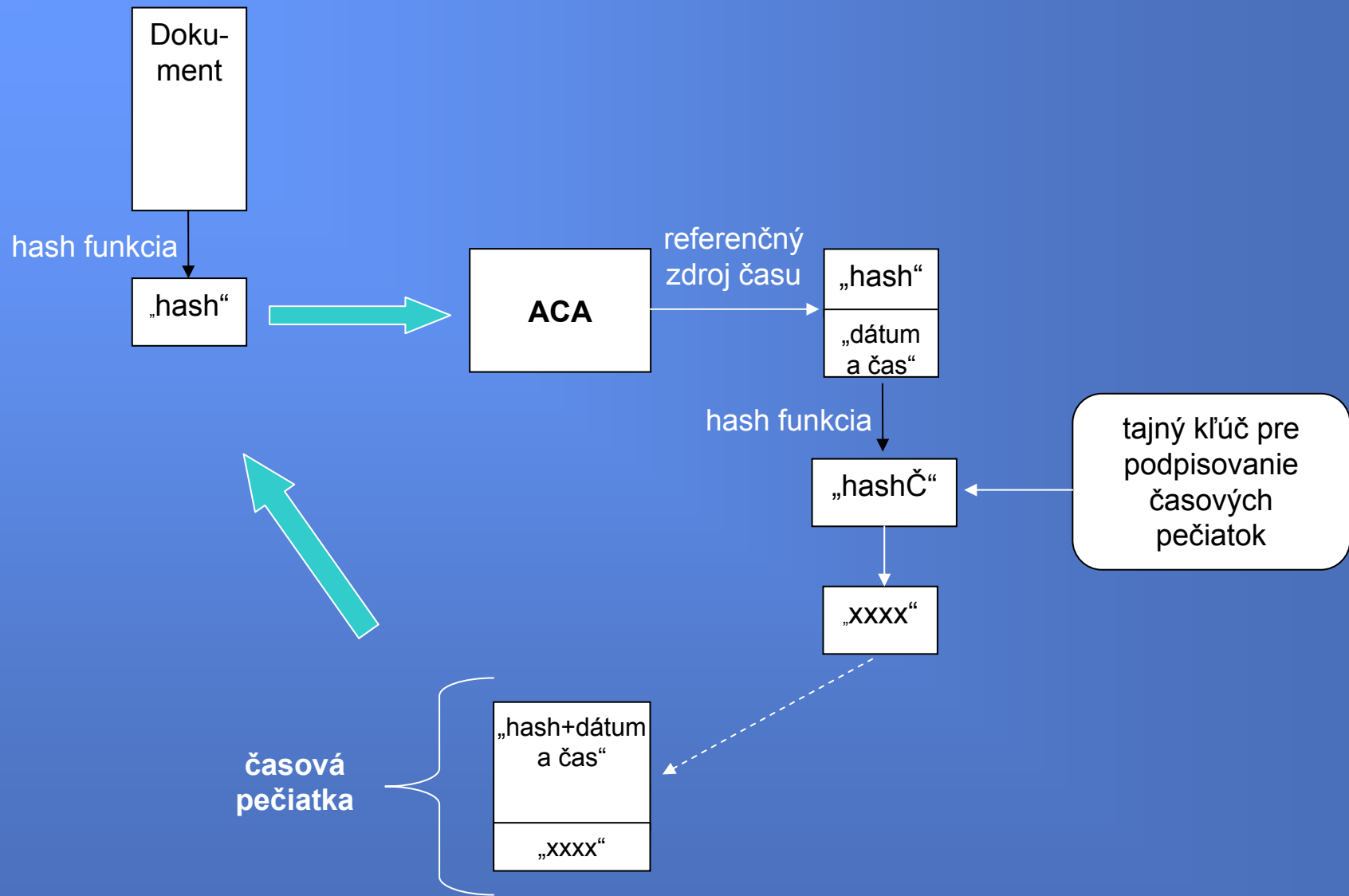
$$m_i = c_i^d \text{ mod } N$$

Časová pečiatka

- je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:
 - vyhotovila ju akreditovaná CA použitím súkromného kľúča určeného na tento účel
 - na verejný kľúč patriaci k uvedenému súkromnému kľúču bol vydaný kvalifikovaný certifikát
 - bola vyhotovená len použitím bezpečného zariadenia na vyhotovovanie časovej pečiatky
 - umožňuje jednoznačne identifikovať dátum a čas kedy bola vyhotovená

(§ 9 ods. 1 zákona NR SR č. 215/2002 Z.z. o elektronickom podpise)

- **vyhotovuje sa na hash (odtlačok) dokumentu**
 - hash hodnota dokumentu sa doplní o požadovaný časový údaj (dátum a čas) z referenčného, zaručeného zdroja času akreditovanej CA
 - takto upravený, doplnený hash sa podpíše zaručeným EP pomocou súkromného kľúča na tento účel určeného
- **podobne ako EP aj časová pečiatka sa pripája k dokumentu, pre ktorý bola vyhotovená**



Obr. 2.: Princíp časovej pečiatky

Elektronický podpis

časť II. - PKI

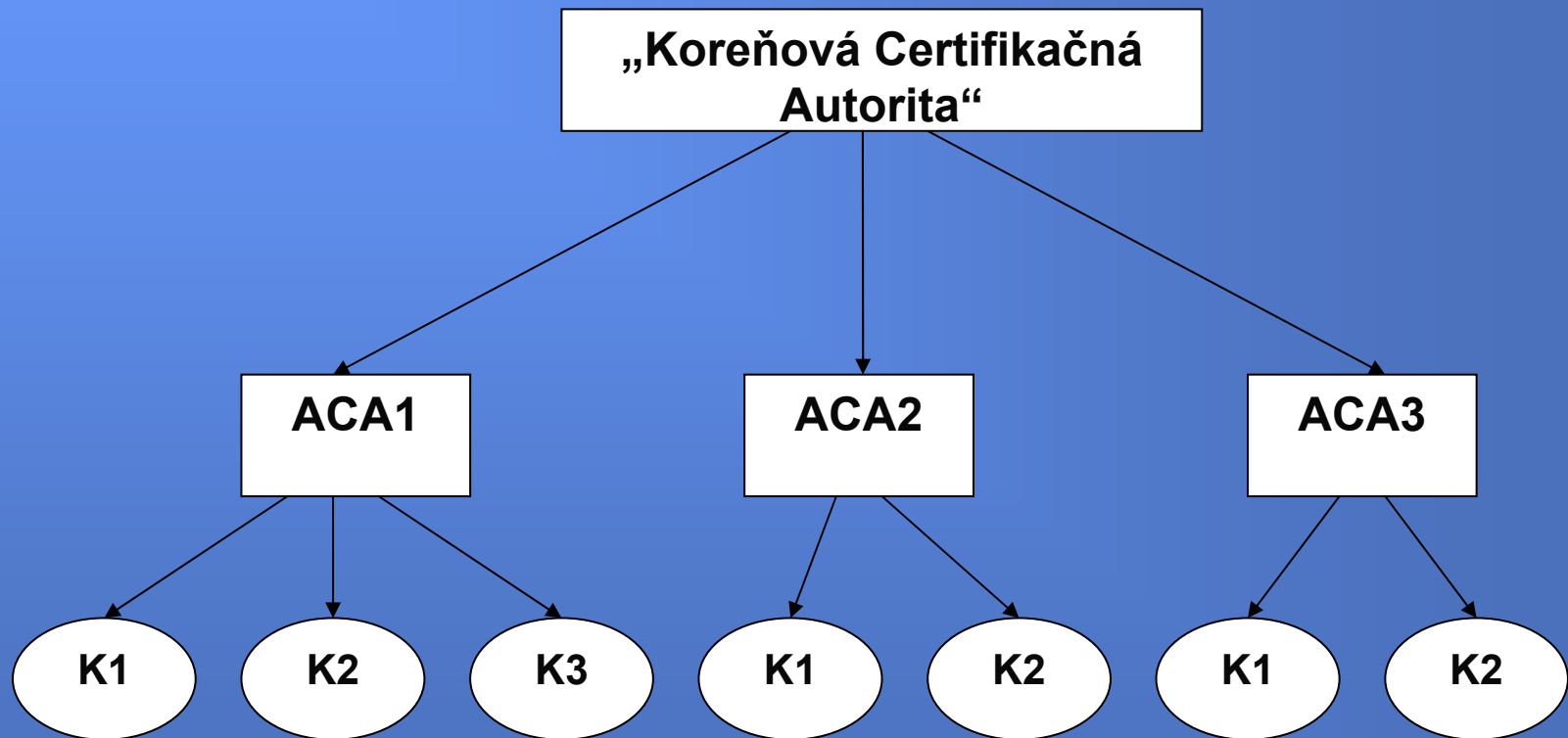
Infraštruktúra verejného kľúča – PKI

- PKI je sústava technických a organizačných opatrení spojených s vydávaním, správou, používaním a revokovaním certifikátov verejných kľúčov

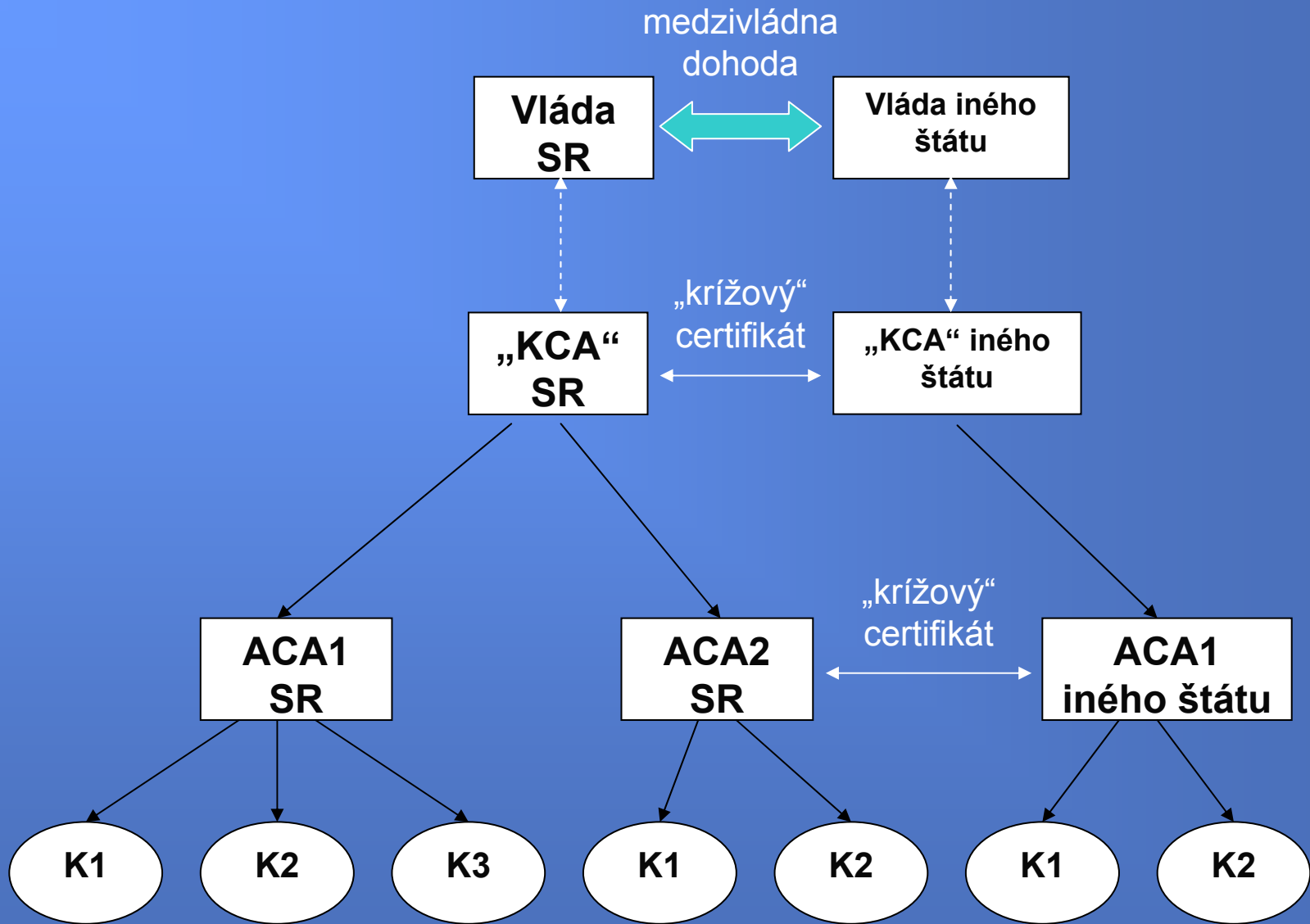
PKI:

- jednoznačné spojenie verejného kľúča a príslušnej osoby vlastniacej prislúchajúci tajný kľúč pomocou certifikátu verejného kľúča
- pyramída dôvery (dôvera v tretiu stranu)
- posilnenie dôvery ak je súčasťou PKI štát
- odpadá nutnosť výmeny kľúčov medzi všetkými osobami navzájom
- bezpečnostné mechanizmy (napr. vydávanie CRL najmä pre prípad straty „tajného“ kľúča)

Príklady PKI:



Obr. 3.: Príklad PKI



Obr. 4.: Príklad PKI

Certifikačná autorita (CA)

- je poskytovateľ certifikačných služieb, ktorý najmä vydáva, spravuje a revokuje certifikáty a vykonáva certifikačnú činnosť
- CA si pre styk s klientmi zriaduje jednu alebo viacej registračných autorít (RA)

Registračná autorita najmä:

- prijíma žiadosti o vydanie certifikátu
- kontroluje súlad údajov v žiadosti o certifikát s údajmi v predložennom preukaze totožnosti žiadateľa o vydanie certifikátu
- odosiela žiadosti o vydanie certifikátu certifikačnej autorite
- odovzdáva certifikáty žiadateľom o vydanie certifikátu

Certifikát verejného kľúča:

- je elektronický dokument, ktorým vydavateľ certifikátu potvrdzuje, že v certifikáte uvedený verejný kľúč patrí osobe, ktorej je certifikát vydaný

(§ 6 zákona NR SR č. 215/2002 Z.z. o elektronickom podpise)

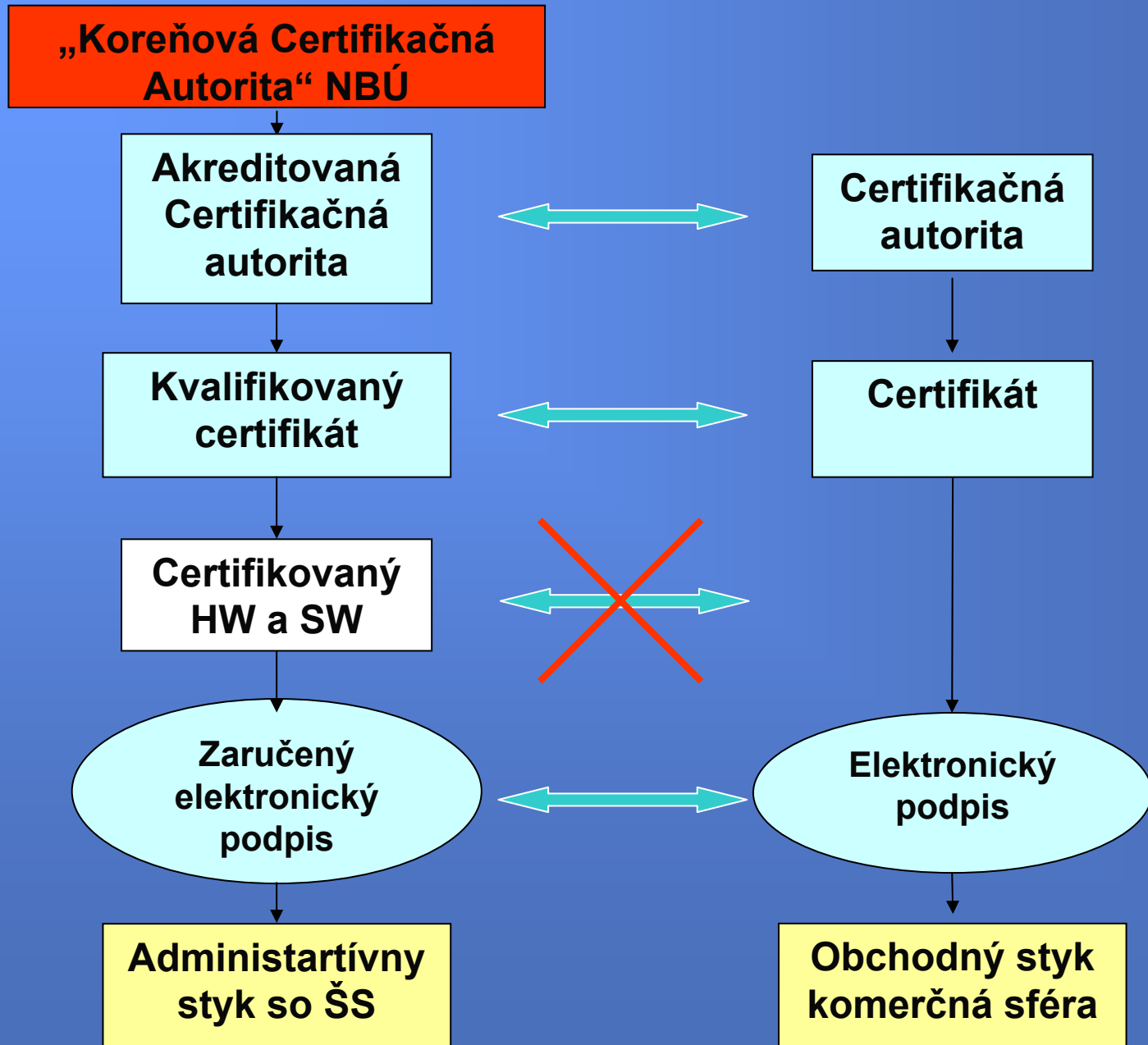
- skladá sa z tela certifikátu a z elektronického podpisu tela certifikátu

- telo certifikátu obsahuje najmä:
 - identifikačné údaje držiteľa certifikátu
 - verejný kľúč držiteľa certifikátu
 - identifikačné údaje vydavateľa certifikátu
 - identifikačné číslo certifikátu
 - dátum a čas začiatku a konca platnosti certifikátu
 - identifikáciu algoritmov, pre ktoré je uvedený verejný kľúč určený
 - identifikáciu algoritmov použitých pri vyhotovení elektronického podpisu tela certifikátu

- **elektronický podpis tela certifikátu**
vyhotovuje vydavateľ certifikátu použitím „tajného“ (súkromného) kľúča, ktorý je na to určený
- **pravosť certifikátu je možné zistiť overením el. podpisu tela certifikátu** (použitím verejného kľúča vydavateľa certifikátu, prislúchajúceho k súkromnému kľúču, ktorým je certifikát podpísaný)

Zoznam zneplatnených certifikátov (CRL):

- je to bezpečnostný mechanizmus, ktorý zabraňuje zneužitiu el. podpisu, napr. v prípade straty osobného tokenu, ktorý obsahuje „tajný“ kľúč podpisovateľa
- je zoznam sériových čísiel certifikátov, ktoré boli zneplatnené pred ukončením platnosti certifikátu, čiže pred dátumom konca platnosti certifikátu uvedeného v certifikáte
- tento zoznam je samozrejme podpísaný „tajným“ kľúčom vydavateľa certifikátov



Elektronický podpis

časť III. – EP prakticky

Čo je potrebné k praktickému použitiu elektronického podpisu?

- k praktickému použitiu elektronického podpisu je potrebné PC pripojené do siete Internet s aplikáciami MS Explorer a MS Outlook alebo podobnými, znalosti o ich používaní a základné znalosti o elektronickom podpise
- k použitiu zaručeného elektronického podpisu, t. j. podpisu ktorý podľa zákona o elektronickom podpise môže byť použitý v administratívnom styku so štátnou správou musí byť v prvom rade zabezpečená podmienka „podpisuj to čo vidíš“
- k tomu je potrebná úradom certifikovaná aplikácia (SCVA), ktorá umožňuje podpísanie dokumentu a aj overenie podpisu a úradom certifikované bezpečné zariadenie na vyhotovovanie elektronického podpisu (SSCD)
- bezpečným zariadením môže byť napríklad certifikovaná kryptografická karta (obdoba platobnej karty) so zariadením, ktoré umožňuje komunikovať počítaču s touto kartou, tzv. čítačka kariet alebo USB token
- v takomto prípade bezpečné zariadenie pre vyhotovovanie elektronického podpisu plní aj funkciu bezpečného uchovávanía tajného kľúča majiteľa

- ďalšou dôležitou podmienkou je vystavenie kvalifikovaného certifikátu konkrétnej osobe, túto úlohu by mala zabezpečovať akreditovaná CA NBÚ alebo úradom akreditovaná CA
- samotný proces elektronického podpisovania dokumentu je pre podpisovateľa obmedzený len na zasunutie kryptografickej karty do čítačky, zadanie PIN kódu a v aplikácii určenej na podpisovanie „odkliknutie“, že uvedený dokument sa má podpísať, takto upravený, podpísaný dokument je potom možné distribuovať
- na strane overovateľa prebieha overenie podobným spôsobom, nie je potrebné vkladať kryptografickú kartu a zadávať PIN kód, stačí len v príslušnej aplikácii kliknúť na voľbu overiť elektronický podpis
- bezpečné aplikácie by však aj pri overovaní ZEP mali vyžadovať vloženie tokenu (nie však zadanie PIN), pretože certifikát ACA alebo NBÚ by sa mal načítať z tohto tokenu, čiže z bezpečného úložiska, kde nie je možné jednoduchým spôsobom tieto certifikáty zameniť za falošné
- po overení sa na monitore objaví správa o úspešnom overení alebo správa o nemožnosti overenie, a ak je to možné tak aj príslušný dôvod

Praktická ukážka rôznych aplikácií pre EP a pre ZEP

Elektronický podpis

časť IV. - Legislatíva

Platná legislatíva

- **Zákon NR SR č. 215/2002 Z.z. o elektronickom podpise**
- **Vyhláška NBÚ č. 537/2002 Z. z., o formáte a spôsobe vyhotovenia zaručeného elektronického podpisu, spôsobe zverejňovania verejného kľúča úradu, postupe pri overovaní a podmienkach overovania zaručeného elektronického podpisu, formáte časovej pečiatky a spôsobe jej vyhotovenia, požiadavkách na zdroj časových údajov a požiadavkách na vedenie dokumentácie časových pečiatok (o vyhotovení a overovaní elektronického podpisu a časovej pečiatky)**
- **Vyhláška NBÚ č. 538/2002 Z. z., o formáte a obsahu kvalifikovaného certifikátu, o správe kvalifikovaných certifikátov a o formáte, periodicite a spôsobe vydávania zoznamu zrušených kvalifikovaných certifikátov (o kvalifikovaných certifikátoch)**
- **Vyhláška NBÚ č. 539/2002 Z. z., ktorou sa ustanovujú podrobnosti o požiadavkách na bezpečné zariadenia na vyhotovovanie časovej pečiatky a požiadavky na produkty pre elektronický podpis (o produktoch elektronického podpisu)**
- **Vyhláška NBÚ č. 540/2002 Z. z., o podmienkach na poskytovanie akreditovaných certifikačných služieb a o požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov**
- **Vyhláška NBÚ č. 541/2002 Z. z., o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách a pravidlách na výkon certifikačných činností**
- **Vyhláška NBÚ č. 542/2002 Z. z., o spôsobe a postupe používania elektronického podpisu v obchodnom a administratívnom styku**

Zákon NR SR č. 215/2002 Z.z. o elektronickom podpise

§3 - Elektronický podpis

- **Elektronický podpis je informácia pripojená alebo logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:**
 - nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča a elektronického dokumentu,
 - na základe znalosti tejto informácie a verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení možno overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, je zhodný s elektronickým dokumentom použitým na jej vyhotovenie.

(§ 3 ods. 1 zákona NR SR č. 215/2002 Z.z. o elektronickom podpise)

§4 – Zaručený elektronický podpis

- **zaručený elektronický podpis spĺňa požiadavky uvedené v §3 a navyiac:**
 - je vyhotovený pomocou súkromného kľúča, ktorý je určený na vyhotovenie zaručeného EP
 - možno ho vyhotoviť len s použitím bezpečného zariadenia na vyhotovovanie zaručeného EP
 - na verejný kľúč patriaci k súkromnému kľúču použitému na vyhotovenie zaručeného EP je vydaný kvalifikovaný certifikát

§6 - Certifikát verejného kľúča

- je elektronický dokument, ktorým vydavateľ certifikátu potvrdzuje, že v certifikáte uvedený verejný kľúč patrí osobe, ktorej je certifikát vydaný

(§ 6 zákona NR SR č. 215/2002 Z.z. o elektronickom podpise)

- skladá sa z tela certifikátu a z elektronického podpisu tela certifikátu

- telo certifikátu obsahuje najmä:
 - identifikačné údaje držiteľa certifikátu
 - verejný kľúč držiteľa certifikátu
 - identifikačné údaje vydavateľa certifikátu
 - identifikačné číslo certifikátu
 - dátum a čas začiatku a konca platnosti certifikátu
 - identifikáciu algoritmov, pre ktoré je uvedený verejný kľúč určený
 - identifikáciu algoritmov použitých pri vyhotovení elektronického podpisu tela certifikátu

§7 - Kvalifikovaný certifikát

- je certifikát verejného kľúča podľa predchádzajúcej definície a navyše:
 - je v ňom uvedené, že je kvalifikovaný
 - má v sebe uvedené obmedzenia na jeho použitie, ak tretia strana takéto obmedzenia rozlišuje
 - je v ňom uvedený účel, na ktorý je určený
 - má telo certifikátu podpísané zaručeným EP
 - vydala ho akreditovaná CA alebo NBÚ

Typy kvalifikovaných certifikátov (KC):

- KC fyzickej osoby – vydáva ho akreditovaná CA fyzickej osobe
- KC akreditovanej CA – vydáva ho NBÚ akreditovanej certifikačnej autorite
- kvalifikovaný krížový certifikát – vydáva ho akreditovaná CA akreditovanej CA-te
- kvalifikovaný certifikát NBÚ – vydáva ho NBÚ na vlastný verejný kľúč (tzv. self signed certificate)

§9 - Časová pečiatka

- je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:
 - vyhotovila ju akreditovaná CA použitím súkromného kľúča určeného na tento účel
 - na verejný kľúč patriaci k uvedenému súkromnému kľúču bol vydaný kvalifikovaný certifikát
 - bola vyhotovená len použitím bezpečného zariadenia na vyhotovovanie časovej pečiatky
 - umožňuje jednoznačne identifikovať dátum a čas kedy bola vyhotovená

(§ 9 ods. 1 zákona NR SR č. 215/2002 Z.z. o elektronickom podpise)

§12 – Certifikačná autorita

- CA je poskytovateľ certifikačných služieb, ktorý spravuje certifikáty a vykonáva certifikačnú činnosť
- poskytovanie certifikačných služieb je podnikaním
- na vykonávanie certifikačných činností a poskytovanie certifikačných služieb sa povolenie nevyžaduje

Povinnosti CA

- **pred začatím poskytovania služieb je CA povinná zverejniť:**
 - certifikačný poriadok
 - používané technické špecifikácie, formáty, normy a štandardy
 - cenník platených služieb a zoznam bezplatne poskytovaných služieb
 - obmedzenia pri poskytovaní služieb, ak existujú
 - informácie o svojej akreditácii
- **zverejňovať svoje identifikačné údaje a informácie o svojich certifikátoch**
- **oznámiť NBÚ začiatok svojej činnosti min. 30 dní vopred**

- **CA je ďalej povinná:**
 - mať vypracované bezpečnostné pravidlá a pravidlá na výkon certifikačných činností
 - dodržiavať uvedené pravidlá počas celej doby poskytovania certifikačných služieb
 - vykonávať certifikačné činnosti tak, aby nebolo možné vytvárať kópie súkromných kľúčov
 - certifikáty vydávať na základe zmluvy
 - pred uzavretím zmluvy informovať žiadateľa o svojej bezpečnostnej politike a pravidlách poskytovania certifikačných služieb
 - poskytnúť žiadateľom informácie o produktoch pre EP
 - informovať žiadateľa o možných právnych dôsledkoch
 - zabezpečovať vydávanie certifikátov
 - zabezpečovať službu zrušenia certifikátov
 - zverejňovať zoznam zrušených certifikátov
 - viesť prevádzkovú dokumentáciu
 - archivovať súvisiacu dokumentáciu

§13 - Akreditácia

- certifikačná autorita môže NBÚ požiadať o akreditáciu
- akreditovanou CA môže byť právnická alebo fyzická osoba, ktorá má vytvorené materiálne, priestorové, technické, personálne, organizačné a právne podmienky na poskytovanie akreditovaných certifikačných služieb
- podrobnosti o podmienkach na poskytovanie akreditovaných certifikačných služieb stanovuje vyhláška NBÚ č. 540/2002 Z.z. o podmienkach na poskytovanie akreditovaných certifikačných služieb a o požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov
- ak žiadateľ o akreditáciu splnil podmienky na udelenie akreditácie, NBÚ do 90 dní od prijatia žiadosti rozhodne o akreditácii a certifikačnej autorite vystaví certifikát

Povinnosti akreditovanej CA

- všetky povinnosti CA sa vzťahujú aj na akreditovanú CA
- bezpečnostné pravidlá a pravidlá na výkon certifikačných činností musia byť v súlade s vyhláškou NBÚ č. 541/2002 Z.z., o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách a pravidlách na výkon certifikačných činností
- akreditovaná CA je povinná preukázať spoľahlivosť nevyhnutnú na poskytovanie certifikačných služieb

§21 Registračná autorita

- RA koná v mene certifikačnej autority alebo na základe zmluvy uzatvorenej s certifikačnou autoritou
- RA je vo svojej činnosti viazaná certifikačným poriadkom CA, v ktorej mene koná alebo s ktorou má uzatvorenú zmluvu
- RA najmä:
 - prijíma žiadosti o vydanie certifikátu
 - kontroluje súlad údajov v žiadosti o certifikát s údajmi v predloženom preukaze totožnosti žiadateľa o vydanie certifikátu
 - odosiela žiadosti o vydanie certifikátu certifikačnej autorite
 - odovzdáva certifikáty žiadateľom o vydanie certifikátu

§15 - Zrušovanie certifikátov

- **CA je povinná zrušiť certifikát, ktorý spravuje, ak:**
 - zistí, že pri vydaní certifikátu neboli splnené podmienky podľa zákona
 - zistí, že certifikát bol vydaný na základe nepravdivých údajov
 - o zrušenie certifikátu požiada držiteľ
 - to nariadi súd
 - zistí, že držiteľ zomrel alebo právnická osoba zanikla
 - zistí, že súkromný kľúč patriaci k verejnému kľúču uvedenému v certifikáte pozná iná osoba
- **certifikát sa považuje za zrušený od okamihu vydania prvého zoznamu zrušených certifikátov, ktorý tento certifikát obsahuje**
- **platnosť zrušeného certifikátu nemožno obnoviť**

§8 - Zoznam zrušených certifikátov

- je elektronický dokument, ktorým vydavateľ certifikátov oznamuje predčasné ukončenie ich platnosti
- skladá sa z tela zoznamu zrušených certifikátov a elektronického podpisu tela zoznamu zrušených certifikátov
- telo zoznamu zrušených certifikátov obsahuje najmä:
 - identifikačné údaje vydavateľa certifikátov
 - dátum a čas vydania zoznamu zrušených certifikátov
 - dátum a čas vydania ďalšieho zoznamu zrušených certifikátov
 - zoznam identifikačných čísiel certifikátov, ktoré boli zrušené spolu s dátumom a časom ich zrušenia

§10 – Úrad (NBÚ)

- **Ústredným orgánom štátnej správy pre EP je NBÚ**
- **Požiadavky na správu kvalifikovaných certifikátov akreditovanou CA sa vzťahujú aj na NBÚ**
- **NBÚ plní tieto úlohy:**
 - vykonáva kontrolu dodržiavania zákona
 - posudzuje žiadosti CA-ít pôsobiacich v SR o akreditáciu, udeľuje a odníma akreditáciu
 - vydáva kvalifikované certifikáty verejných kľúčov akreditovaným certifikačným autoritám
 - zverejňuje vlastný verejný kľúč
 - vydáva kvalifikované certifikáty verejných kľúčov zahraničným certifikačným autoritám
 - eviduje CA pôsobiace v SR
 - vedie a zverejňuje zoznam akreditovaných CA a CA s odňatou akreditáciou
 - zrušuje vydané kvalifikované certifikáty
 - vedie register zahraničných CA, ktorých certifikáty boli uznané na použitie v SR
 - certifikuje produkty pre elektronický podpis
 - plní ďalšie úlohy vyplývajúce zo zákona

§ 11 - Kontrola

- **NBÚ môže kontrolovať CA odo dňa oznámenia začiatku svojej činnosti**
- **CA je povinná umožniť výkon kontroly**
- **ak CA porušuje povinnosti vyplývajúce zo zákona (napr. nie je dostatočne bezpečnostne spoľahlivá) môže NBÚ najmä:**
 - **obmedziť (max. na 3 mesiace) alebo zakázať poskytovanie certifikačných činností**
 - **nariadiť zrušenie kvalifikovaných certifikátov**

§5 - Používanie elektronického podpisu

- ak možno v styku s verejnou mocou používať elektronický podpis, tento EP musí byť zaručeným elektronickým podpisom
- pri overovaní zaručeného EP overovateľ na základe kvalifikovaného certifikátu verejného kľúča overí, či verejný kľúč na overenie zaručeného EP patrí podpisovateľovi

§22 - Povinnosti držiteľa certifikátu

- **držiteľ certifikátu je povinný:**
 - zaobchádzať so svojím súkromným kľúčom s náležitou starostlivosťou, tak aby nedošlo k zneužitiu súkromného kľúča
 - uvádzať presné, pravdivé a úplné informácie vo vzťahu k certifikátu svojho verejného kľúča
 - neodkladne požiadať CA, ktorá spravuje jeho certifikát o zrušenie certifikátu, ak zistí, že došlo alebo hrozí zneužitie jeho súkromného kľúča
- **za škodu spôsobenú porušením povinností zodpovedá držiteľ**

§24 – Požiadavky na produkty pre elektronický podpis

- na uchovávanie súkromných kľúčov a na vyhotovovanie zaručených elektronických podpisov sa musia používať bezpečné zariadenia, ktoré spoľahlivo chránia v nich uložený súkromný kľúč
- súlad bezpečných zariadení s bezpečnostnými požiadavkami overuje a potvrdzuje NBÚ
- bezpečné zariadenia musia najmä:
 - zabezpečiť, že podpisovaný elektronický dokument sa pri podpise nezmení
 - umožniť zobrazenie podpisovaného dokumentu ešte pred podpísaním

§17 – Uznávanie zahraničných certifikátov

- **certifikát alebo kvalifikovaný certifikát, ktorý vydala CA so sídlom v zahraničí možno uznať v SR ak:**
 - medzinárodná dohoda podpísaná Slovenskou republikou ustanovuje, že zahraničný kvalifikovaný certifikát je uznávaný ako kvalifikovaný certifikát alebo zahraničná CA je uznaná za akreditovanú CA v SR

§25 - Audit

- akreditovaná CA je povinná opakovane sa podrobiť externému auditu bezpečnosti poskytovania certifikačných činností (raz za 12 mesiacov)
- záverečná správa o výsledkoch auditu sa musí predložiť NBÚ do 30 dní od ukončenia auditu
- podrobnosti a audite sú vo vyhláške NBÚ č.540/2002 Z.z. o podmienkach na poskytovanie akreditovaných certifikačných služieb a o požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov

§26 - Sankcie

- **za porušenie povinnosti podľa zákona môže NBÚ uložiť pokutu napr.:**
 - do 10.000.000,- Sk právnickej alebo fyzickej osobe, ktorá poskytuje akreditované certifikačné služby bez akreditácie
 - do 500.000,- Sk certifikačnej autorite, ktorá si nespĺní oznamovaciu povinnosť
 - do 100.000,- Sk fyzickej osobe, ktorá predložila nepravdivé údaje pri podávaní žiadosti o vydanie certifikátu

§23 – Ochrana osobných údajov

- na informačný systém poskytovateľa certifikačných služieb sa vzťahuje zákon NR SR č. 428/2002 Z.z. o ochrane osobných údajov v informačných systémoch



Ďakujem za pozornosť!