# Elektronický podpis

*Šifrovanie a Elektronický podpis*

*Certifikačná autorita*

*Elektronické podpisovanie pdf dokumentov*

*Elektronická podateľňa*

*Praktické ukážky*

Katedra aplikovanej matematiky a hospodárskej informatiky

**Ekonomická fakulta Technickej univerzity**

**2018**

# Elektronický podpis – motivácia

## Elektronická výmena dokumentov - výhody

- zrýchlenie prístupu k informáciám obsiahnutých v dokumentoch a k realizácií určitých transakcií
- väčší komfort – možnosť získavať informácie, resp. realizovať určité transakcie z domu alebo pracovne v zamestnaní
- menšia prácnosť a chybovosť – získanú informáciu je možné ďalej spracovávať, bez nutnosti prepisovania, čím sa znižuje riziko chybovosti
- úspora nákladov – veľmi aktuálne

# Šifrovanie

- Zabezpečuje dôvernosť a ochranu prenášaných údajov voči tretej strane
- Štandardné protokoly SSL (Internet banking), WTSL (Wap banking), šifrovanie v rámci GSM siete (SMS banking)
- Vlastné implementované šifrovanie – DES, TriplDES a pod.
- Pasívny e-mail banking – PGP alebo ZIP, ARJ a pod.

# ÍNAVORFIŠ O ADEV-AIFARGOTPYRK

Niečo náročnejšie ☺

H - S R G S L V

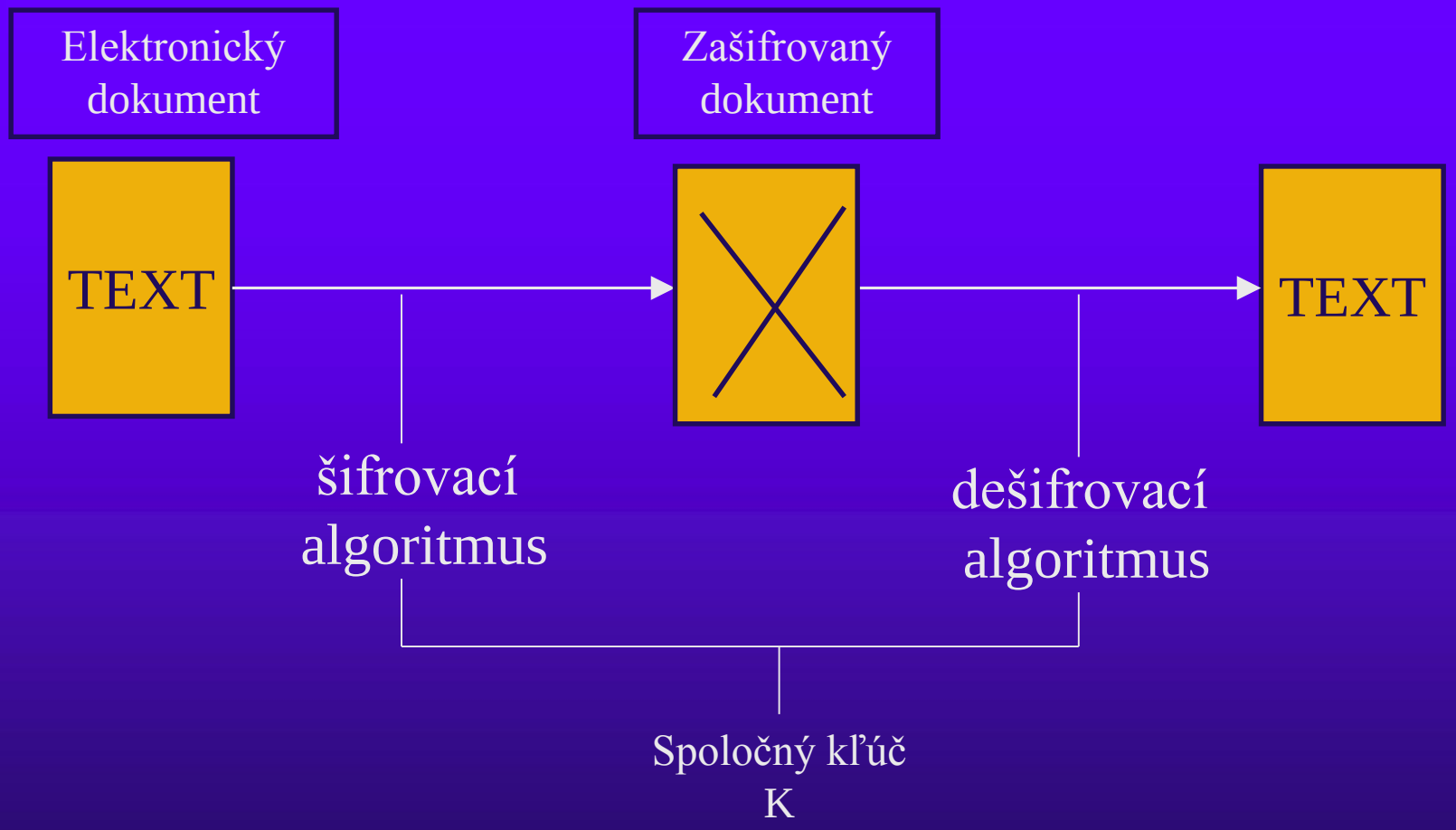
Riešenie : E – P O D P I S

Pomôcka:

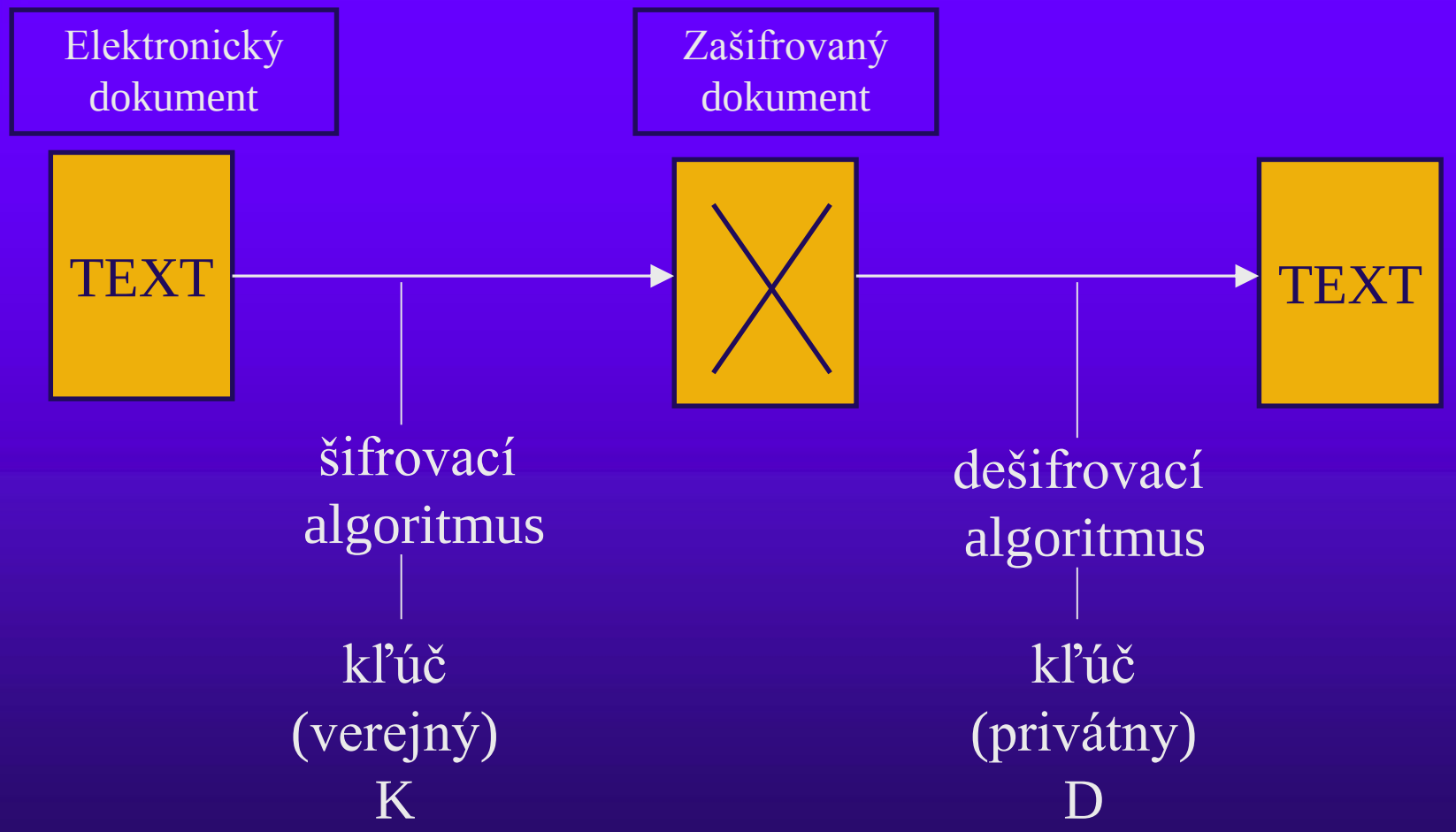
1. Číslo: 3
2.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |

# Symetrické šifrovanie



# Asymetrické šifrovanie

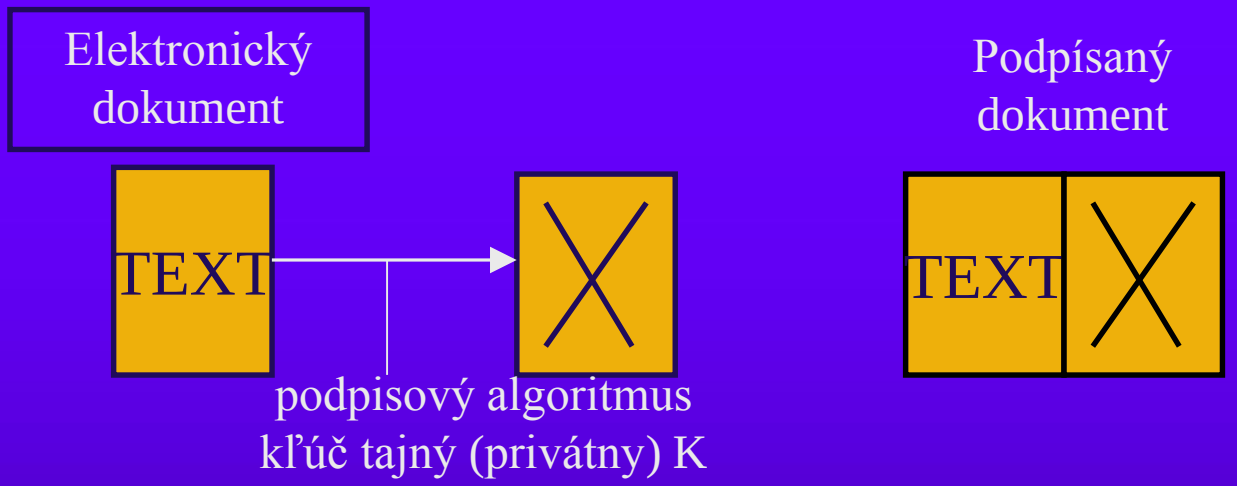


Aký je súvis medzi šifrovaním (utajovaním) a podpisovaním ?

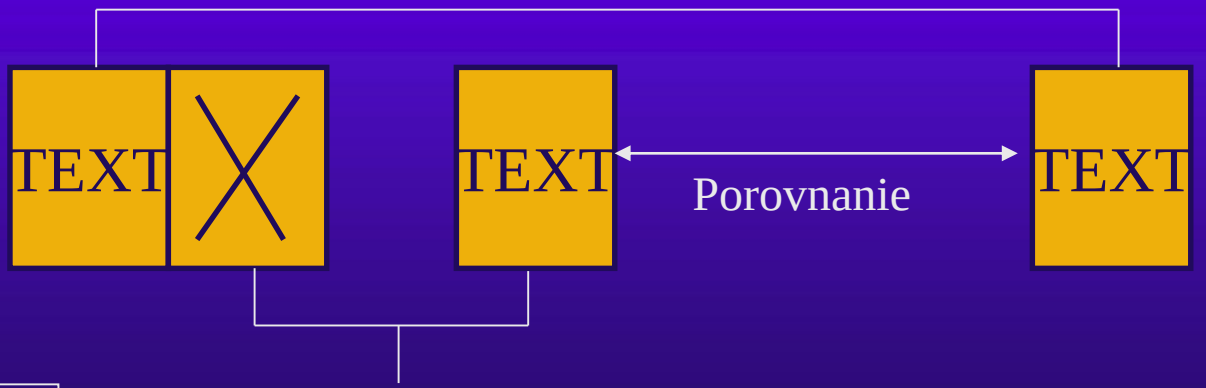
Klasickým podpisom na papieri nič neutajujeme...

# Digitálny podpis na báze RSA

- vytvorenie podpisu




- overenie podpisu




Pozn. kľúče K,D sa generujú ako dvojica

# Elektronický podpis

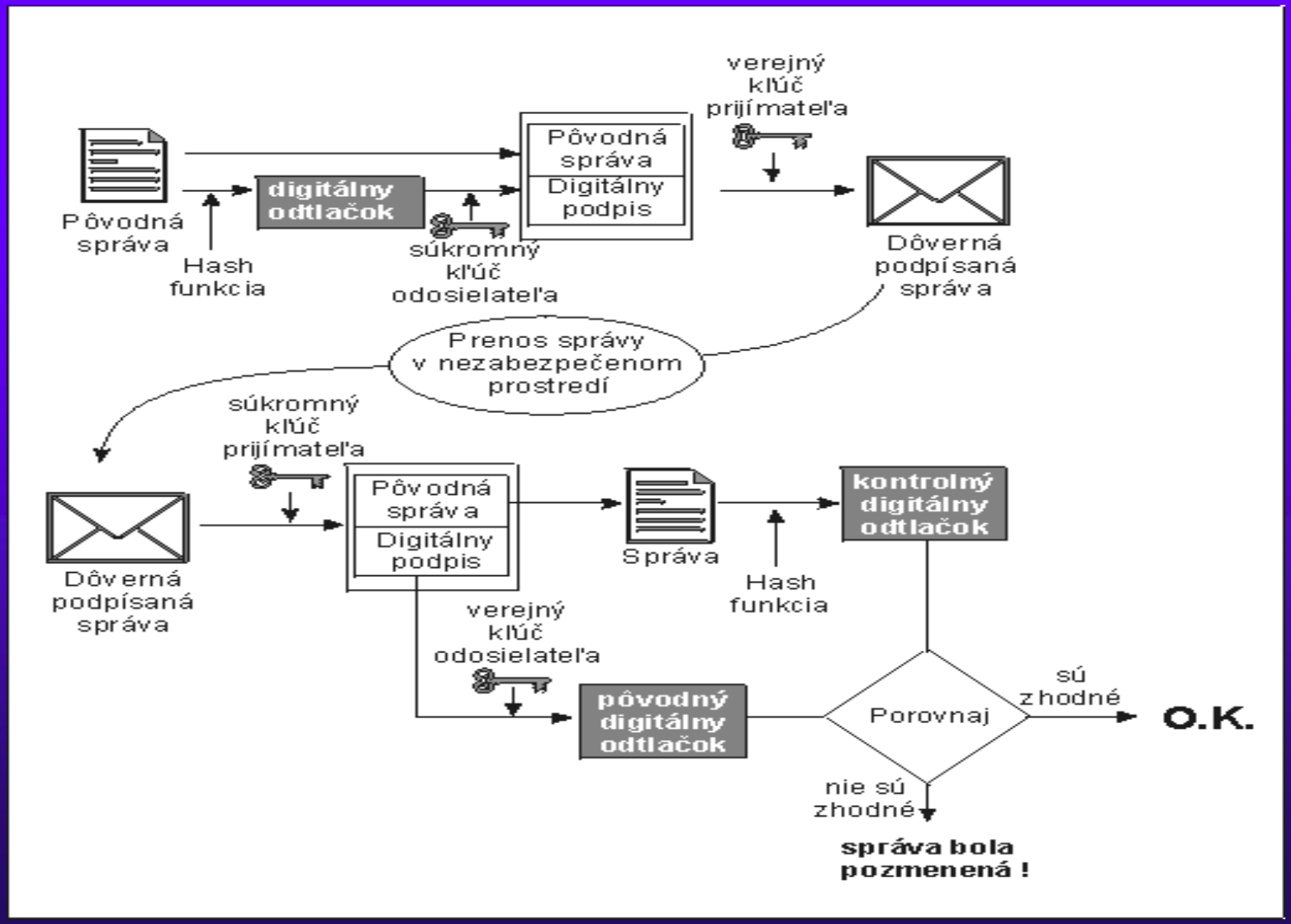
- Digitálny podpis v zmysle **návrhu zákona o elektronickom podpise pre SR** sa definuje ako informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá spĺňa nasledujúce požiadavky:

1. *nie je (efektívne) možné ju vytvoriť bez znalosti súkromného kľúča,*
2. *na základe znalosti tejto informácie a verejného kľúča prislúchajúceho k súkromnému kľúču použitému pri jej vytvorení je možné overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, nebol po jej vytvorení zmenený.*

# Elektronický podpis - funkcie

- identifikácia autora,
- autenticitu a integritu (t.j. že overovaný a podpisovaný dokument sú rovnaké),
- overiť čas vytvorenia podpisu (t.j. že čas uvedený v podpise nebol neskôr modifikovaný),
- nepopierateľnosť autorstva,
- nemožnosť podpísať prázdny dokument.

# Podpis a šifrovanie

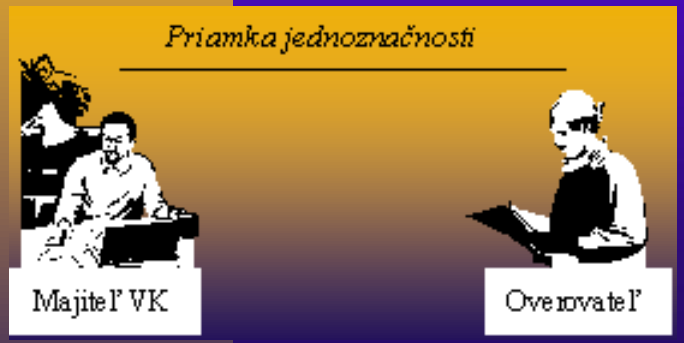


# Problém identifikácie osôb v elektronickom svete

- Ako si overiť, že komunikujeme skutočné s osobou, za ktorú sa druhá strana vydáva?
- Ako zistiť, že podpis, ktorý overujeme nie je podvrhnutý a bol vytvorený skutočne avizovanou osobou?

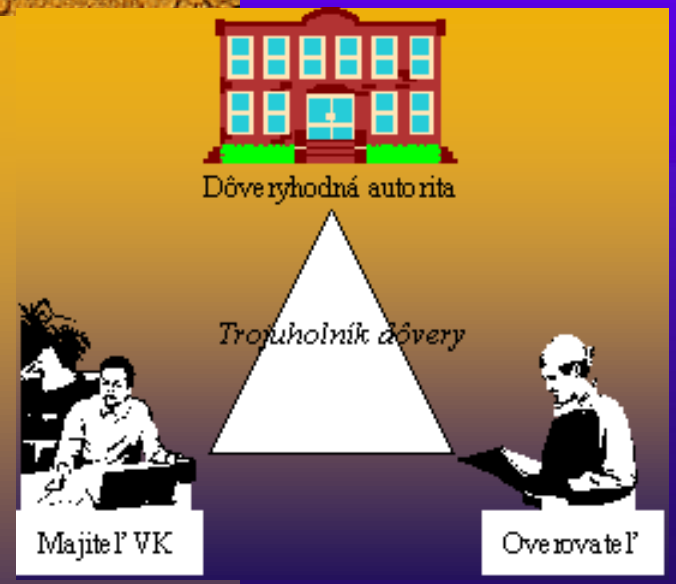
# Priradenie verejného kľúča ku konkrétnej osobe

- *priamka jednoznačnosti*
  - ide o zmluvu o verejnom kľúči medzi majiteľom kľúča a overovateľom podpisov. Takýto spôsob spojenia je z pohľadu obidvoch strán jednoznačný. Správne uzavretá dohoda chráni obidve strany a je jeden z dôkazových prostriedkov v prípade sporu.
    - Takéto nasadenie digitálneho podpisu je možné v t.z. uzavretých systémoch. V súčasnej dobe je táto metóda používaná u službách elektronického bankovníctva (VUB, SLSP,...).



# Priradenie verejného kľúča ku konkrétnej osobe

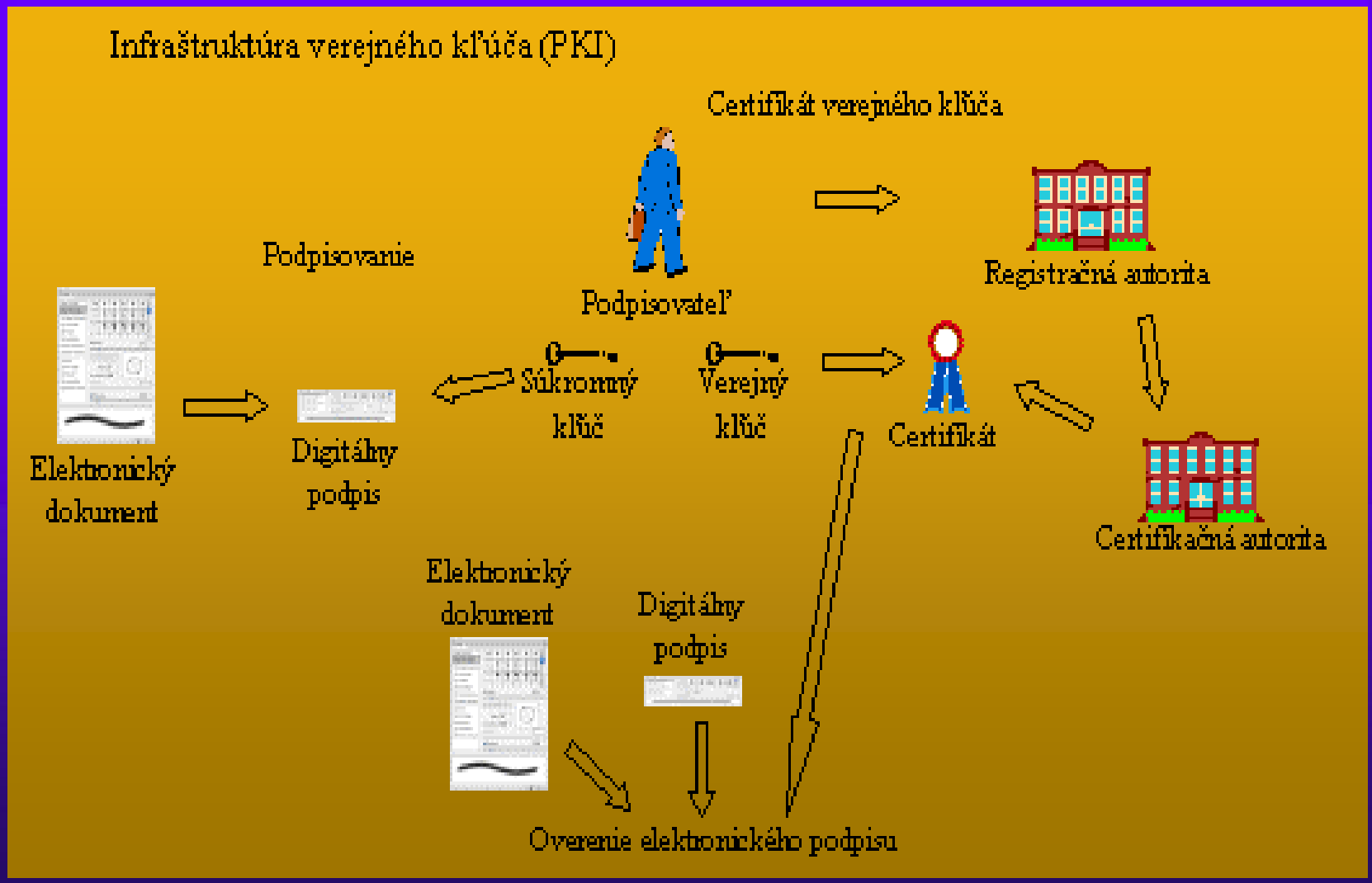
- *2.trojuholník dôvery*
  - v otvorených systémoch sa majiteľ kľúča často nemá možnosť stretnúť s overovateľom podpisov, aby spolu uzavreli zmluvu o príslušnom verejnom kľúči.
    - V takomto prípade je vhodné využiť dôveryhodnú tretiu stranu – ***certifikačnú autoritu (CA)***, ktorá by mala zabezpečiť jednoznačné spojenie verejného kľúča s konkrétnou osobou – jeho majiteľom a to na základe overenej žiadosti majiteľa, v ktorej sú uvedené jeho základné identifikačné údaje a príslušný verejný kľúč. údaj



# PKI (Public Key Infrastructure) Infraštruktúra verejného kľúča

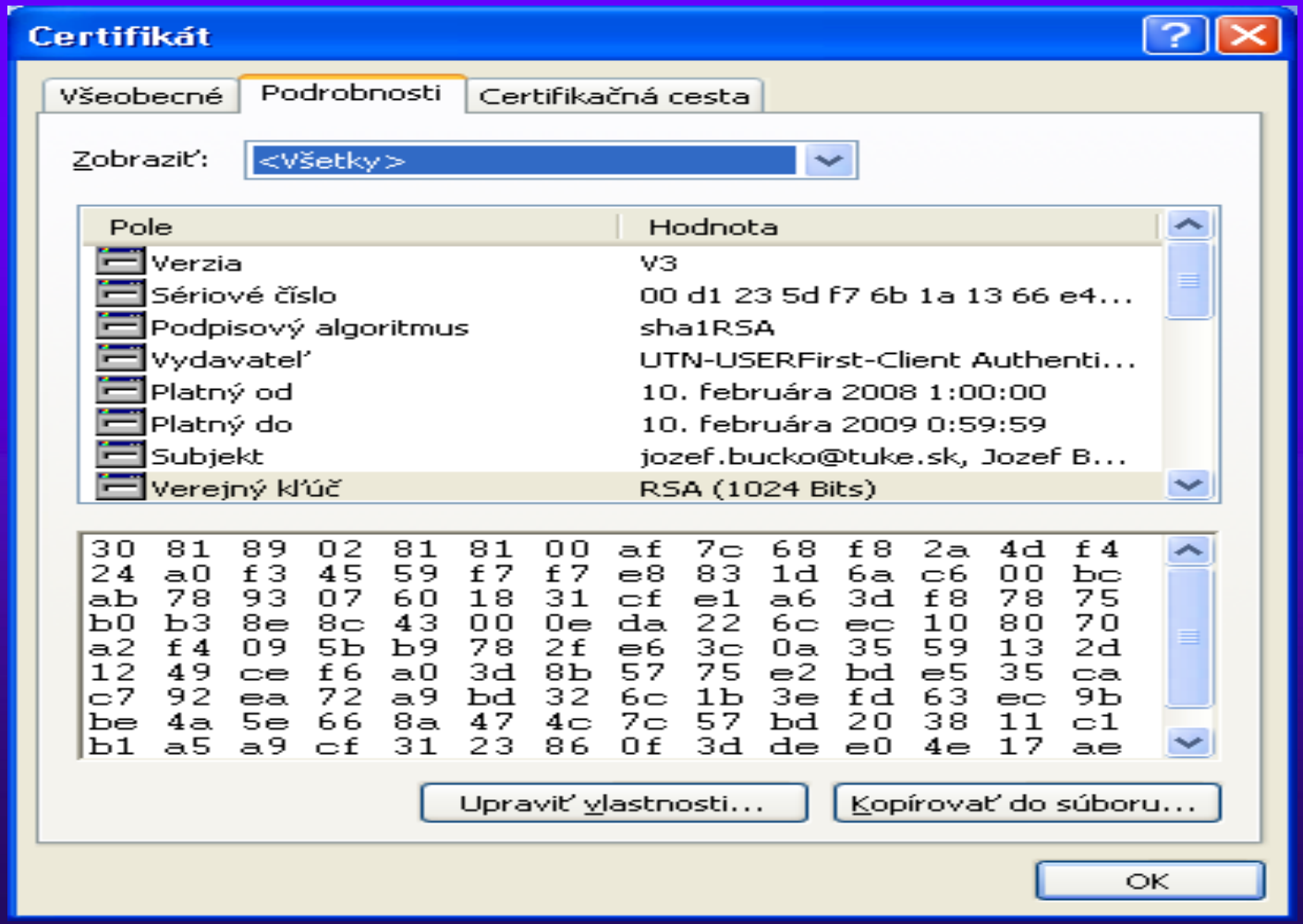
- spojenie verejného kľúča s konkrétnou osobou prostredníctvom tzv. certifikátu sa zabezpečuje prostredníctvom infraštruktúry verejného kľúča - PKI
- je sústava technických a organizačných opatrení spojených s vydávaním, správou, používaním a revokovaním certifikátov verejných kľúčov.

# PKI


Infraštruktúra verejného kľúča (PKI)
Certifikát verejného kľúča
Podpisovanie
Registračná autorita
Podpisovateľ
Súkromný kľúč
Verejný kľúč
Certifikát
Elektronický dokument
Digitálny podpis
Certifikačná autorita
Elektronický dokument
Digitálny podpis
Overenie elektronického podpisu

# Certifikát – podpísaný ver. kľúč

Certifikát: je el. dokument, podpísaný CA, ktorým sa potvrdzuje, že VK patrí určitej osobe (držiteľovi certifikátu)



Lister - [F:\Projekty\Tatrabanka\Openxkpki\kluc\bucko.asc]

Súbor Upraviť Možnosti Pomocník 59 %

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: PGP 8.1 - not licensed for commercial use: www.pgp.com

lQOgBEYLm+wBCADPPzR2lfNTcAgeZuEdzxclLXl1/JVqq27I0nsFHAWo+jxh6Dj4
RNVcSH0OeQghHZQIPO+EnwzCzFhW2vJeA8erdCPFVxYv7qFpwEU3LkSuiJDi4jHy
Il95++3ai34+gPvBuwPiaMWcvsVW+AErc32GuoNUjgGi+EqKaDeAmhSUTPaWN2UH
jbVqy27eRTtyn+t7M8bttsn/mqzzPPM7BiW4FH3ZEaN4R0waPlaWHCwmtbnprZWH
EVfoSnektHWe4r8TdQVs5XrzPh+WfOHj+JNgD7hFuAXcLcb3bZKZxNwfZAhzOJ5v
w8n2lZ58bQrF/Hym/5PEFEG7Xb2UfM6yXboRABEBAAEBzReh/rFDMbeaj+YjoM7b
pbb928GChS0+Cdl1KK13yQ9nfguAi5NDjf6iodYNKyPSOb5LdwoPw/V+kEVSk5q2
Hmkfn16pCF58nYLfduR/589bI2i71h5Ic7G+aix0WOMEWjLEwKglnkne1ZuoxJbP
KWpyNzFbvmrnyzxRTKvdwB+FtvFv0/rVTi1IFggDBO6xQbiLMOIrGLWQ45BEyM8O
A1KJ6eXuNnxiseMsVgymqBYsB2uYHXBAyteqFxvgMB/hPZ3qh4qEC68vMnOmkTIC
LNtIZ2mY5KZELQNg63GhiBJvfX17+xR1XS3qlisEzTbrxoXrvADkrlMgMZiBSG6h
W5X5rfsOhB0qDu7jk0AYFH3/lbIrnDfG9QgNryW0Q8WPTNuorzmi0Xrzt9HHuMP6
TrkUFktDZpPacomVQnTCX4P1DFPalO/09qjWHGKvIYY8bbmAkDKt2fJWQdxBCh5X
LYvY4e7Vi0sJLwO5DHYaEYxn51bS5nl3lqnD/Da3js6dOtWND+BlgYUJ11VAfF1A
nobG79p8vj0o8PWe+1Y6vfVyVBCd3ZRMibIGJ17kt7mIL8ZyjopK2XVaruedyIsU
3tm+HB6jmC56YhYr4gZTBoV1M28nNHpK7Uu6Vsp4l0XpFGe1hLJcJdNYrQP5/0C5
/pDmM/8MX/K1UM58Pot+hghwWUV0Cl07M4darbFrgn2f6bLEwo7gji5BLBKY+qyi
4NcAUEjV1WtdRq9N2vHrx75A5v1aOoW7r2T6Y19qaA4IpTCySjnKzm7d3lZFJZpv
4UnxCcWfd2zclp4fpuyLRM/xAE+6q16jK8euaU2yWTtJCHnz4QWRD7wJXNq7vVI8
hEfz4F/0GuSg/vXhfgkx979jMrQsVGhhd3RlIEZyZWVtYWlsIE1lbWJlciA8am96
ZWYuYnVja29AdHVrZS5zaz4=
=JLKF
-----END PGP PRIVATE KEY BLOCK-----
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.1 - not licensed for commercial use: www.pgp.com

mQENBEYLm+wBCADPPzR2lfNTcAgeZuEdzxclLXl1/JVqq27I0nsFHAWo+jxh6Dj4
RNVcSH0OeQghHZQIPO+EnwzCzFhW2vJeA8erdCPFVxYv7qFpwEU3LkSuiJDi4jHy
```

# EP a čas jeho vyhotovenia, resp. overenia

Možnosti zachytenia času:

1) Pomocou atribútu čas podpisu nachádzajúcom sa v samotnom EP

2) Pomocou časovej pečiatky – podpis nezávislej tretej strany k dodanému el. odtlačku, s presným údajom uvedeným v atribúte čas podpisu

# Praktické aspekty EP

1) Generovanie dvojice kľúčov

2) Certifikácia verejného kľúča

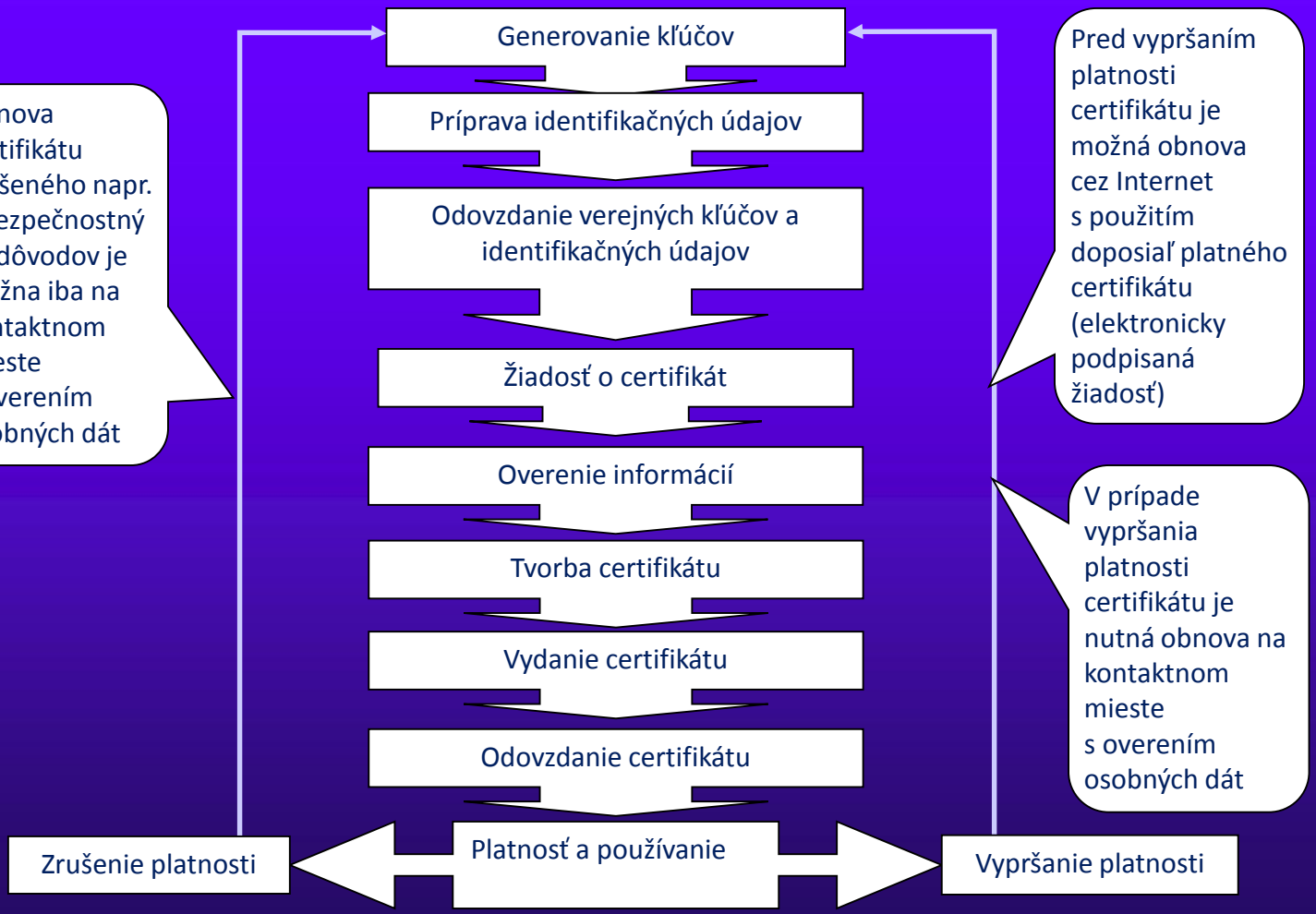
3) Samotné podpisovanie elektronických dokumentov

4) Podpisovanie a šifrovanie emailov

# Možnosť vytvoriť si digitálny podpis

- CAEKFTUKE - https://v2.ekf.tuke.sk
- Comodo - http://www.instantssl.com/ssl-certificate-products/free-email-certificate.html
- Thawte - http://www.thawte.com/secure-email/personal-email-certificates/
- PGP – www.pgp.com

# Postup pri tvorbe a používaní certifikátu



# Po vytvorení certifikátu

- Môžeme prakticky začať elektronický podpisovať
  - email (nutný emailový klient – softvér)
  - ľubovoľný elektronický dokument (nutný softvér na podpisovanie e-dokumentov – pgp, Kleopatra)
  - Pdf dokumenty (softvér, acrobat reader XI)

Praktické použitie e-podpisu