ELEKTRONICKÝ PODPIS

Prezentácia
PP 2019/2020
25. marca 2020

JUDr. Jozef Andraško, PhD.

CC-BY 2.0

PREHĽAD

- **ZÁKLADY ELEKTRONICKÉHO PODPISU (EP)**
  - Vlastnoručný podpis
  - Základy EP
  - Vytvorenie EP
  - Certifikát
  - Elektronická pečať
  - Elektronická časová pečiatka

- **PRÁVNA ÚPRAVA**
  - úroveň EÚ

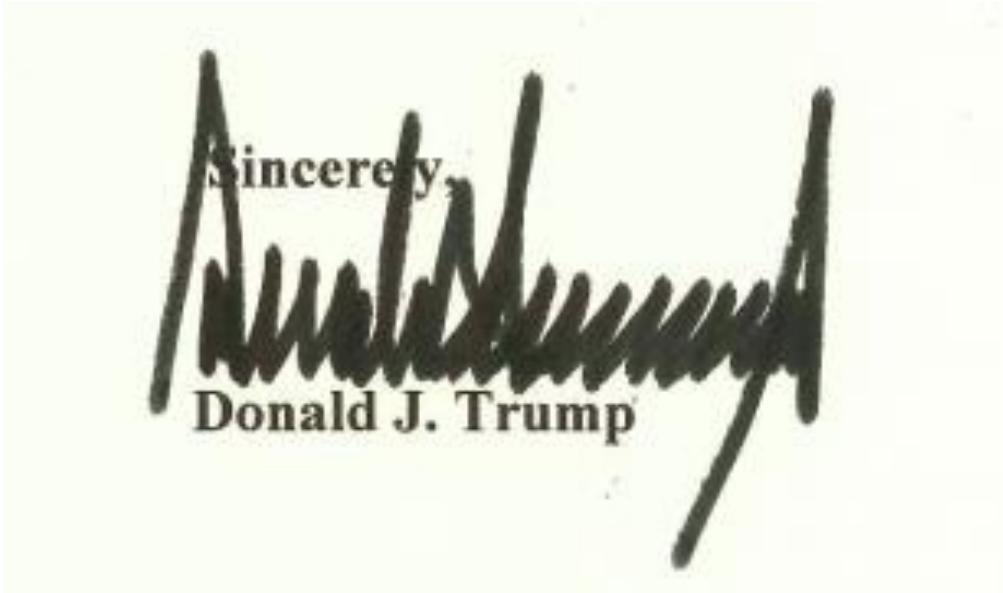
ÚVOD

- vznik **informačnej spoločnosti**
- **čo je vo fyzickom svete, malo by byť aj vo virtuálnom priestore**
- normy, ktoré sa aplikujú vo fyzickom svete, by sa mali aplikovať aj vo virtuálnom priestore
- **namiesto vlastnoručného podpisu (VP) začal používať EP**

vlastnoručný podpis

VP

Právne hľadisko?



VP

Právne hľadisko?

- prejav vôle
- vyjadrenie súhlasu s obsahom podpísaného dokumentu

VP

Bezpečnostné hľadisko?

VLASTNORUČNÝ PODPIS PLNÍ NASLEDUJÚCE BEZPEČNOSTNÉ POŽIADAVKY

identifikuje osobu, ktorá dokument podpísala

zaručuje autentickosť (originalitu) dokumentu, aby nedošlo k modifikácii dokumentu po podpise (integrita)

vyjadruje súhlas podpisovateľa s obsahom dokumentu

nemožno ho preniesť na iný dokument

je **nesfalšovateľný**, nakoľko vytvoriť ho vie len podpisovateľ a overiť ho dokáže každý

Ako zabezpečiť, **aby bezpečnostné požiadavky VP boli naplnené aj vo virtuálnom priestore** v situáciách, kedy sa vyžaduje podpísanie elektronického dokumentu?

elektronický podpis vs. digitálny podpis

EP/DP

- synonymá?
- EP – viacero foriem?

PRÍKLADY:

- napísanie mena do elektronického dokumentu
- naskenovanie vlastnoručného podpisu a vložením ho do elektronického dokumentu
- EP vytvorený na podpisový tablet
- **Digitálny podpis**

digitálny podpis

DIGITÁLNY PODPIS - ZÁKLADY

HASHING

ŠIFROVANIE (ASYMETRICKÉ)

DIGITÁLNY PODPIS

DIGITÁLNY PODPIS - ZÁKLADY

HASHING

ŠIFROVANIE (ASYMETRICKÉ)

DIGITÁLNY PODPIS

HASHING

- **jednosmerný proces**
  - nemôžete znovu obnoviť mrkvu
- rovnaký vstup bude mať rovnaký výstup
  - odtlačok prsta
- dokonca aj veľké množstvo vstupov vedie k výstupu **rovnakej veľkosti**
  - vždy malú misku

HASHING

SPRÁVA

- **jednosmerný proces**
  - nemôžete znovu obnoviť mrkvu
- rovnaký vstup bude mať rovnaký výstup
  - odtlačok prsta
- dokonca aj veľké množstvo vstupov vedie k výstupu **rovnakej veľkosti**
  - vždy malú misku

hašovací algoritmus (napr. SHA256, MD5...)

Hašovacia hodnota (odtlačok elektronického dokumentu)

0388657483F93CF73137

SHA256 HASH GENERATOR

zahešuj mrkvu

0388657483F93CF73137E843C6D40EBD2B3B6FEF3CA662AE8CE105D6601EDA4D

zahešuj mrkvu!

80AF85F04BA78B54E21EFC46B2FA5D3E2F67C14444F105A6105E2302F019D667

DIGITÁLNY PODPIS - ZÁKLADY

HASHING

ŠIFROVANIE (ASYMETRICKÉ)

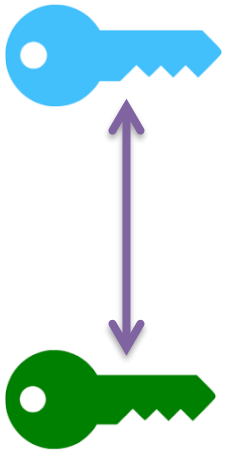
DIGITÁLNY PODPIS

ASYMETRICKÉ ŠIFROVANIE

- chcem poslať elektronický dokument (ED)
- pomocou hašovacieho algoritmu vypočítam **hašovaciu hodnotu** ED (vypočítaná hašovacia hodnota)
- túto hodnotu **zašifrujem mojim súkromným kľúčom** (podpisový kľúč)
  - nikomu ho nedám!
  - je len môj!

- **Táto hodnota tvorí elektronický podpis dokumentu!**

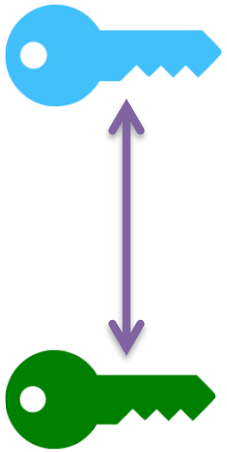
- **adresát pomocou verejného kľúča rozšifruje EP**
  - slúži na overenie správnosti EP – overovací kľúč



ASYMETRICKÉ ŠIFROVANIE

Súkromný kľúč – verejný kľúč

- SK - jedno (veľmi) veľké číslo, ktoré je väčšinou prenášané vo forme textového súboru
- keď ho otvoríte, uvidíte niekoľko riadkov na pohľad nezmyselného textu
- dvojica kľúčov
- VK môže mať hocikto
- zistenie SK z VK matematicky ťažko zvládnuteľné
- **čo zašifrujem jedným kľúčom – odšifrujem druhým**



DIGITÁLNY PODPIS - ZÁKLADY

HASHING

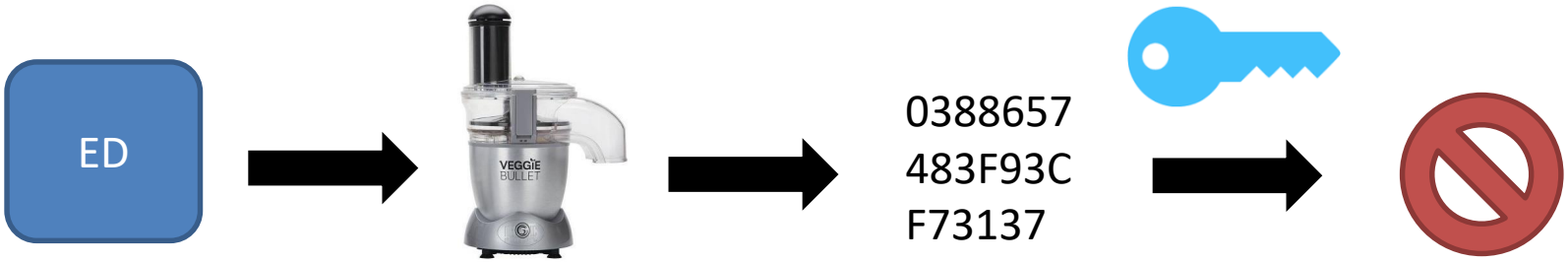
+

ŠIFROVANIE (ASYMETRICKÉ)

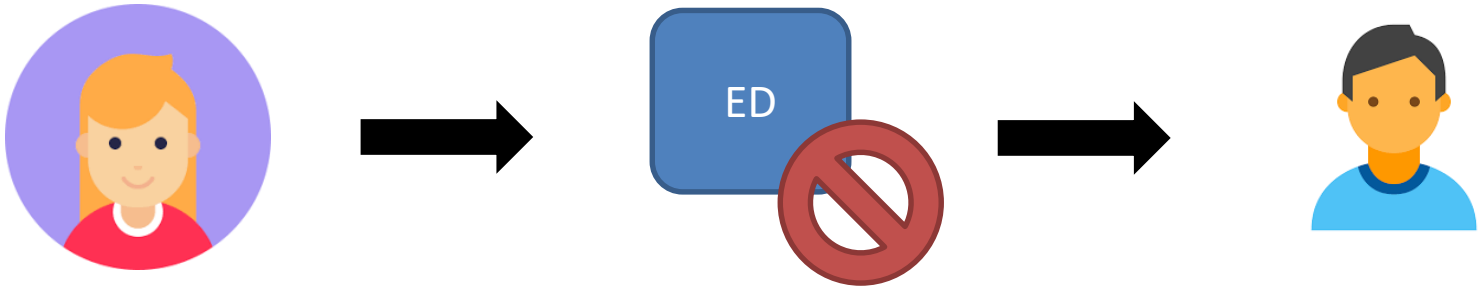
=

DIGITÁLNY PODPIS

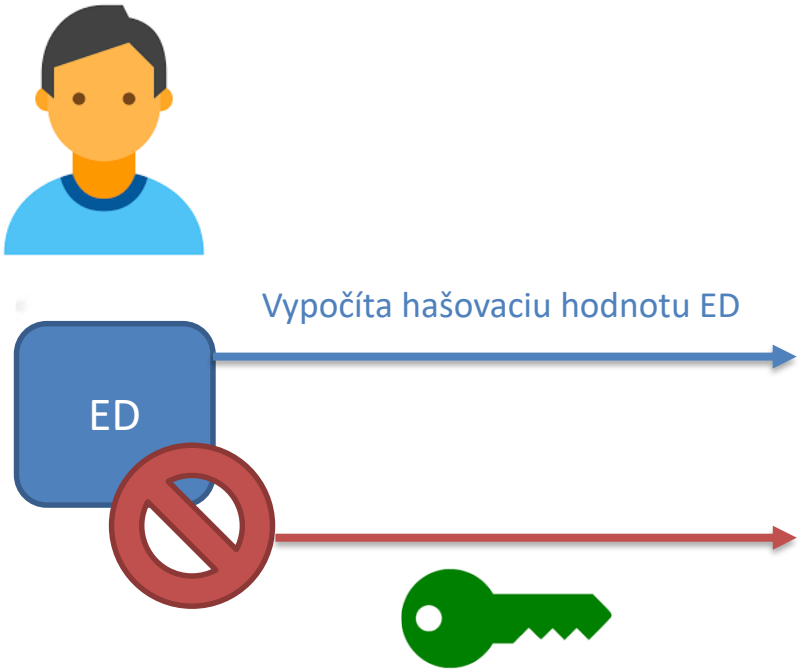
ASYMETRICKÉ ŠIFROVANIE



ASYMETRICKÉ ŠIFROVANIE



ASYMETRICKÉ ŠIFROVANIE



0388657
483F93C
F73137

0388657
483F93C
F73137

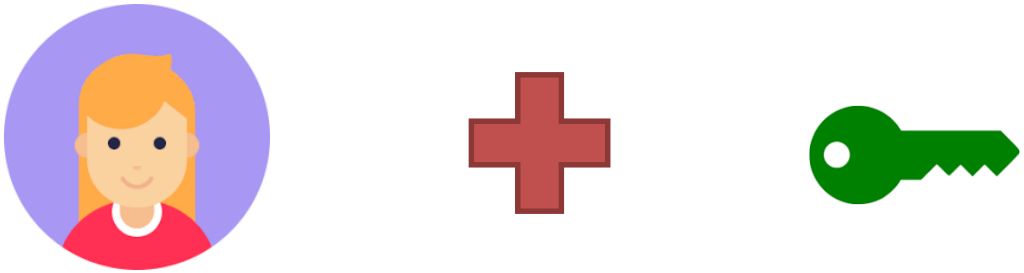
ZHODUJÚ SA?

Ako viem, že  vytvorila EP?

CERTIFIKÁT VK

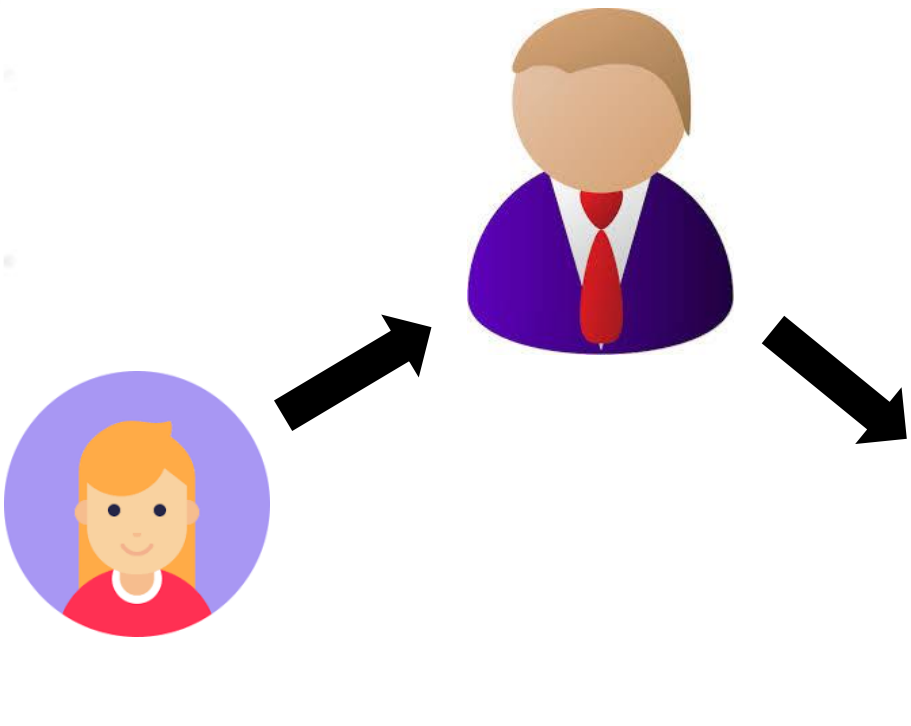
- certifikát verejného kľúča (CVK)
- certifikačnou autoritou (CA)

Spojenie identity a verejného kľúča



CERTIFIKÁT VK

CA



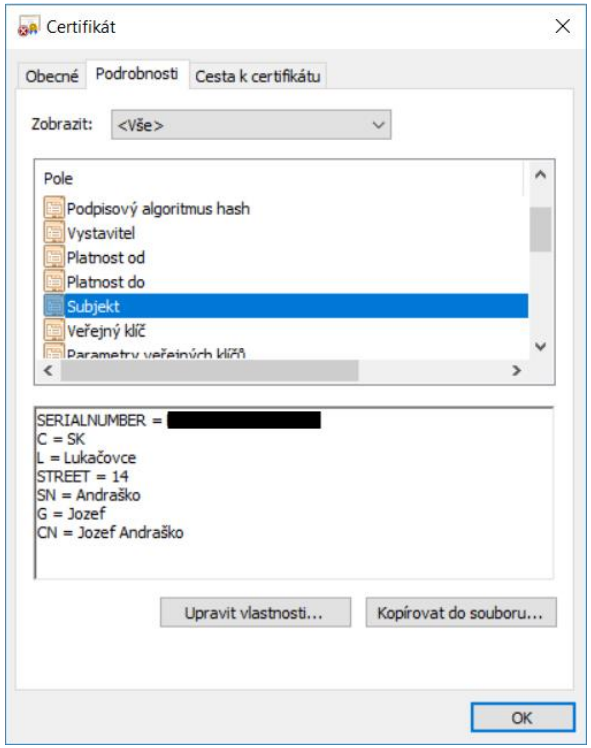
- meno
- priezvisko
- verejný kľúč
- doba platnosti
- **podpíše svojim SK - CA**

CVK

- preukaz elektronickej identity, ktorý **zakladá identitu osoby** (žiadateľa o certifikát) vo virtuálnom priestore

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

- **formát - X.509**

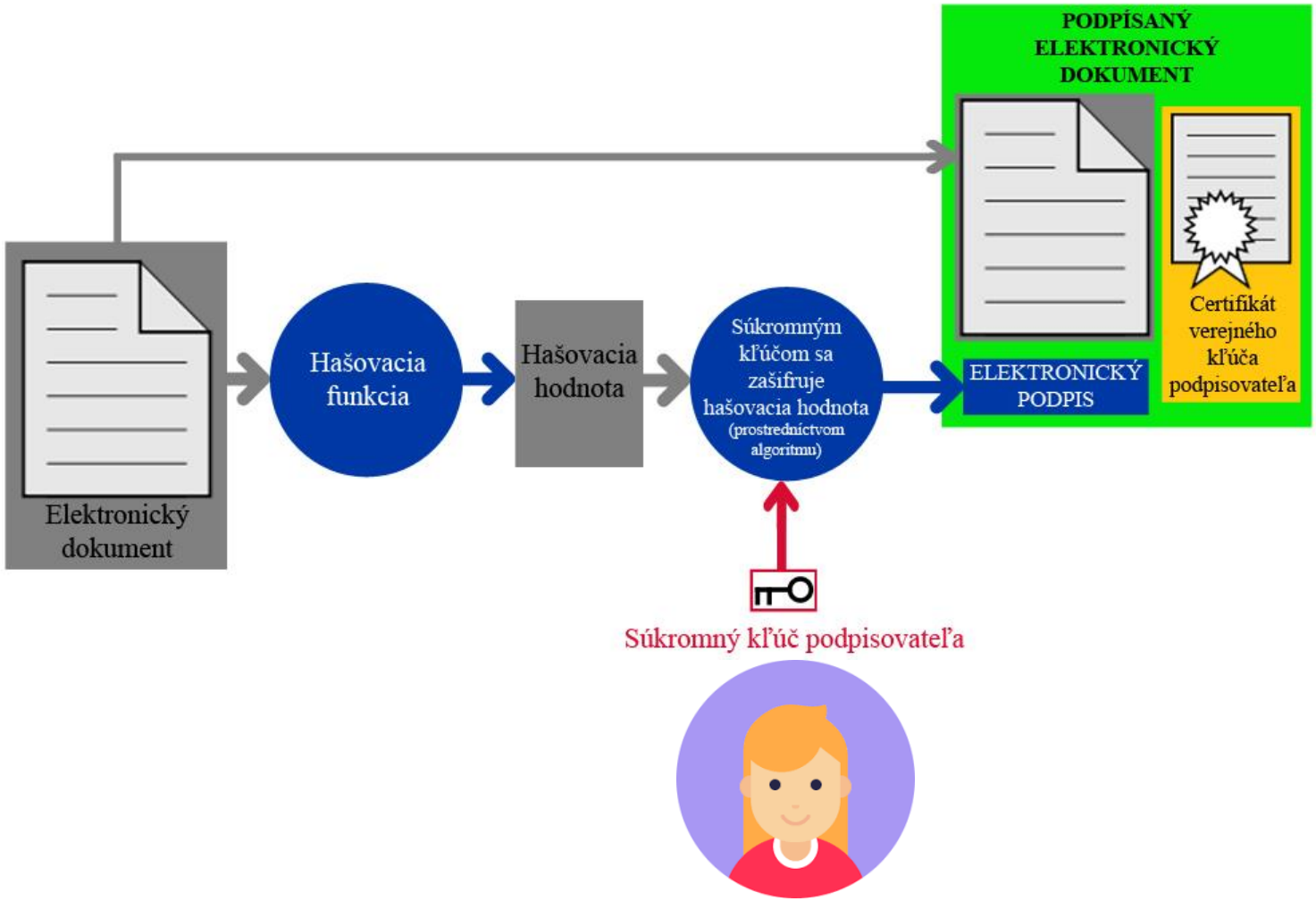


X.509

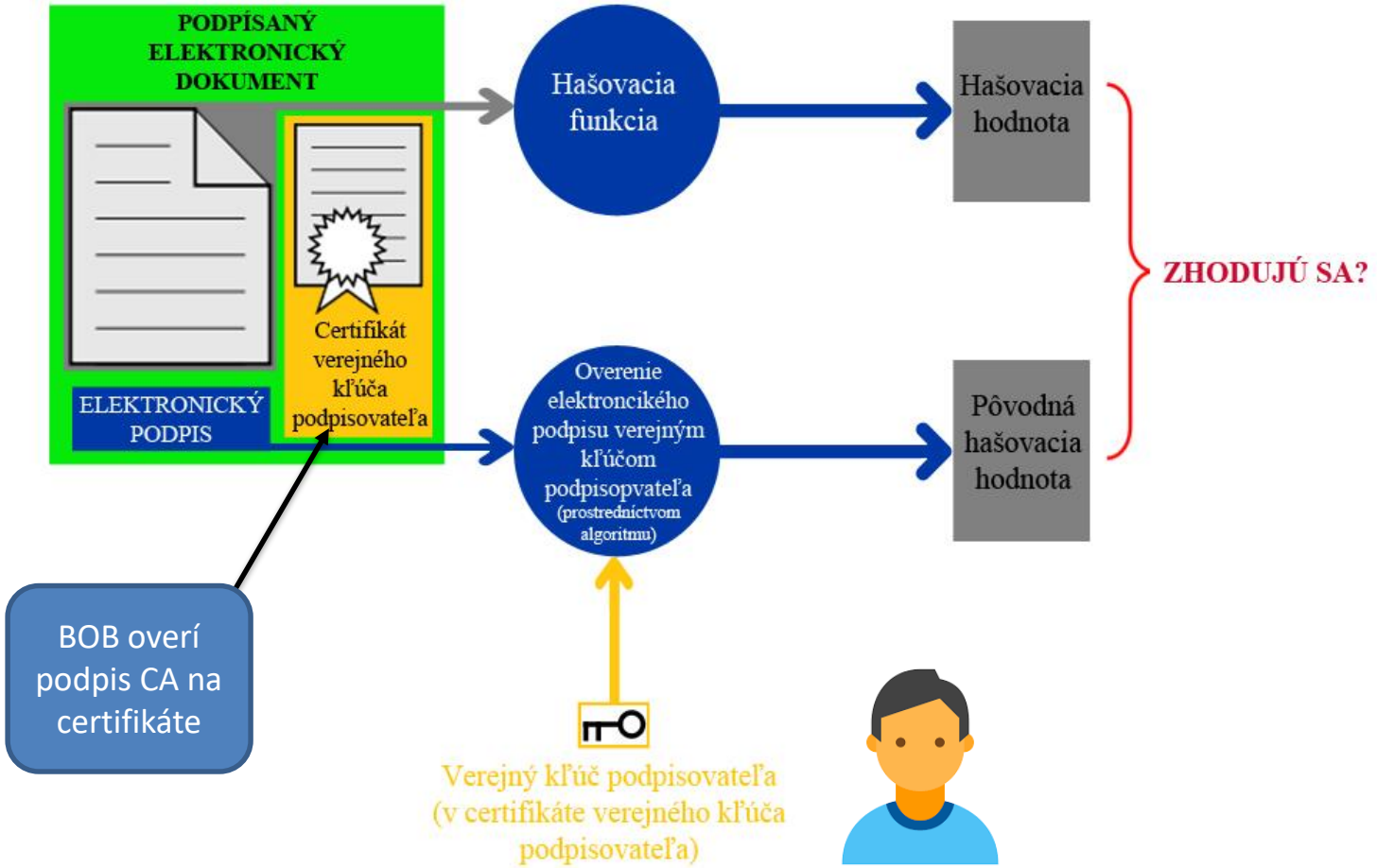
- CVK – **atribútový certifikát** (Štandard X.509)

- **CVK – AC**: cestovný pas – víza potrebné na vstup do krajiny
- **CVK:** sa používa na **autentifikáciu** a viaže **meno držiteľa na verejný kľúč**
- **AC:** sa používa na účely **autorizácie**, nakoľko viaže **konkrétne oprávnenie s menom jeho držiteľa**
  - napr. správca systému by bol držiteľom AC pre vstup do daného systému.

VYTVORENIE EP



OVERENIE EP


PODPÍSANÝ ELEKTRONICKÝ DOKUMENT
ELEKTRONICKÝ PODPIS
Certifikát verejného kľúča podpisovateľa
Hašovacia funkcia
Hašovacia hodnota
ZHODUJÚ SA?
Overenie elektroncikého podpisu verejným kľúčom podpisopvateľa (prostredníctvom algoritmu)
Pôvodná hašovacia hodnota
BOB overí podpis CA na certifikáte
Verejný kľúč podpisovateľa (v certifikáte verejného kľúča podpisovateľa)

elektronická pečať

ePEČAŤ

- z technického hľadiska predstavuje DP
- **iný účel**
- nie podpisovateľ – pôvodca pečate (PO)
- PO – súkromný kľúč
  - problém s uznávaním EP – PO
  - hromadné podpisovanie dokumentov

elektronická časová pečiatka

e-ČASOVÁ PEČIATKA

- dokázanie existencie konkrétneho elektronického dokumentu v konkrétnom čase

- **dokazuje existenciu ED v čase vytvorenia časovej pečiatky**

Právna úprava

ÚROVEŇ EÚ

NARIADENIE eIDAS

- Nariadenia EP a Rady 910/2014 z 23. júla 2014 **o elektronickej identifikácii a dôveryhodných službách** pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES

- Smernica o EP + projekty

- pôsobnosť
  - pozitívna
  - negatívna

NARIADENIE eIDAS

- Nariadenia EP a Rady 910/2014 z 23. júla 2014 **o elektronickej identifikácii a dôveryhodných službách** pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES

- trust service = **služba dôvery!**

NARIADENIE eIDAS

Por.	Oblasti upravené Nariadením eIDAS
1.	elektronická identifikácia
2.	pravidlá pre služby dôvery
3.	elektronické podpisy
4.	elektronické pečate
5.	elektronické časové pečiatky
6.	elektronické dokumenty
7.	elektronické doručovacie služby pre registrované zásielky
8.	certifikačné služby pre autentifikáciu webových sídiel

- uznávanie elektronických podpisov, elektronických pečatí a elektronických časových pečiatok
- vzájomné uznávanie prostriedkov elektronickej identifikácie a úrovne záruky

- uznávanie elektronických podpisov, elektronických pečatí a elektronických časových pečiatok
- vzájomné uznávanie prostriedkov elektronickej identifikácie a úrovne záruky

NARIADENIE eIDAS – služby dôvery

Služby dôvery

- **elektronické služby**, ktoré sa spravidla poskytujú **za odplatu** a spočívajú:

*a) vo **vyhotovovaní, overovaní a validácii elektronických podpisov, elektronických pečatí alebo elektronických časových pečiatok**, elektronických doručovacích služieb pre registrované zásielky a certifikátov, ktoré s týmito službami súvisia, alebo*

*b) vo vyhotovovaní, overovaní a validácii **certifikátov pre autentifikáciu webových sídiel**, alebo*

*c) v **uchovávaní** elektronických podpisov, pečatí alebo certifikátov, ktoré s týmito službami súvisia.*

Elektronický podpis

ELEKTRONICKÝ PODPIS - OBYČAJNÝ

- **údaje v elektronickej forme**, ktoré **sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme** a ktoré podpisovateľ používa na podpisovanie

- čokoľvek, čo vieme **zdigitalizovať** a pripojiť k dokumentu

- heslo, PIN, obrázok, podpisový tablet...

ELEKTRONICKÝ PODPIS - ZDOKONALENÝ

- obyčajný EP + ďalšie podmienky
- **jedinečnosť spojenia ZEP** s **fyzickou osobou**, ktorá vyhotovuje elektronický podpis, čiže podpisovateľom
- **určenie totožnosti podpisovateľa**
- vyhotovený pomocou **údajov na vyhotovenie elektronického podpisu**, ktoré môže podpisovateľ s vysokou mierou dôveryhodnosti **používať pod svojou výlučnou kontrolou**
- **prepojený s údajmi**, ktoré sa ním podpisujú, takým spôsobom, že **každú dodatočnú zmenu údajov možno zistiť**

autentifikácia

identifikácia

súkromný kľúč

integrita

ELEKTRONICKÝ PODPIS - KVALIFIKOVANÝ

- **zdokonalený EP + ďalšie podmienky**

- vyhotovený s použitím **kvalifikovaného zariadenia na vyhotovenie elektronického podpisu**
  - čipová karta, USB token
  - **zabezpečuje bezpečnosť** KEPu

- založený na **kvalifikovanom certifikáte pre elektronické podpisy**, ktorý vydáva kvalifikovaný poskytovateľ služieb dôvery

NAJVYŠŠIA MIERA ZÁRUKY V AUTENTICKOSŤ ELEKTRONICKÉHO PODPISU

bol vytvorený **osobou, ktorej bol vydaný kvalifikovaný certifikát pre elektronický podpis**

Právne účinky EP

PRÁVNE ÚČINKY EP

- nesmú byť odopierané **právne účinky**
- nesmie byť **odmietaný ako dôkaz** v súdnom konaní
- **iba z toho dôvodu, že má elektronickú podobu**, alebo že nespĺňa požiadavky na kvalifikované elektronické podpisy

LEN KEP MÁ PRÁVNY ÚČINOK ROVNOCENNÝ S VLASTNORUČNÝM PODPISOM!!!

Elektronická pečať

ELEKTRONICKÁ PEČAŤ

- **obyčajná, zdokonalená a kvalifikovaná**

- údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom (eDokument) v elektronickej forme s cieľom **zabezpečiť pôvod a integritu týchto pridružených údajov**

- okrem autentifikácie dokumentu, ktorý vydala, aj na autentifikáciu **akéhokoľvek jej digitálneho majetku**, napríklad softvérového kódu alebo serverov

ANI VO FORME KVALIFIKOVANEJ ELEKTRONICKEJ PEČATE NEMÁ PRÁVNE ÚČINKY VLASTNORUČNÉHO PODPISU!

Elektronická časová pečiatka

ELEKTRONICKÁ ČASOVÁ PEČIATKA

- **údaje v elektronickej forme**, ktoré viažu **iné údaje v elektronickej forme** s konkrétnym časom, čím tvoria dôkaz o existencii týchto iných údajov v danom čase
  - iné údaje v elektronickej forme – dokument

- spojenie elektronickej časovej pečiatky s inými údajmi dokazujú, že tieto iné údaje **existovali v konkrétnom momente**

- dôveryhodným spôsobom určuje čas existencie konkrétnych údajov

- **obyčajná**
- **kvalifikovaná - domnienka:**
  - **správnosti dátumu a času**, ktorý uvádza
  - **integrity údajov**, s ktorými je dátum a čas spojený

EP, EPeč vo verejných službách

VEREJNÉ SLUŽBY

- ak členský štát EÚ vyžaduje v prípade **použitia online služby, ktorú poskytuje subjekt verejného sektora** alebo v jeho mene, použitie EP alebo EPeč. **konkrétnej úrovne,** tento členský štát má povinnosť **uznať** EP alebo EPeč. z iných členských štátov, ak sú **rovnakej alebo vyššej úrovne**

- **zakazuje sa**, aby členský štát EÚ pre online službu vyžadoval elektronický podpis alebo elektronickú pečať **vyššej úrovne bezpečnosti ako kvalifikovanú úroveň**

ĎAKUJEM

ZA POZORNOSŤ!

jozef.andrasko@flaw.uniba.sk