Elektronický podpis

10.04.2025

Operační systémy
IV. ročník

Bc. Lukáš Pospíšil

MěSOŠ
Klobouky u Brna

Cíl tématu

- **Znám** pojmy:
  - elektronický podpis, hash funkce, digitální certifikát, cert. autorita
- **Popíšu** a **vyjmenuju:**
  - princip fungování elektronického podpisu
  - metody ověřování pravosti elektronického podpisu
  - využití el. podpisu v praxi (dat. schránky, smlouvy, …)
- **Umím:**
  - metody ověřování pravosti elektronického podpisu
  - určit, jaký typ el. podpisu je potřebný pro konkrétní situaci
  - popsat úlohu CA a způsob vydávání digitálních certifikátů

Elektronický podpis

- **Digitální alternativa klasického vlastnoručního podpisu**
- Slouží k
  - **ověření totožnosti podepisující osoby**
  - **garanci neměnnosti podepisovaného dokumentu**
    - pouhá úprava jednoho písmena v dokumentu podpis zneplatní
- V určitých úrovních je **právně závazný**

Elektronický podpis

- Naskenovaný obrázek podpisu **NENÍ ELEKTRONICKÝ PODPIS**
  - lze ho snadno zkopírovat nebo podvrhnout
- Elektronický podpis musí být
  - **kryptograficky zabezpečený**
  - **neoddělitelně spojený s podepsaným dokumentem**

Elektronický podpis

Princip vytvoření

- **Matematicky odvozený kód**
  - váže se ke konkrétnímu dokumentu
- Založený na **asymetrické kryptografii**
- Vytvořen pomocí **dvojice klíčů**
  - soukromý a veřejný

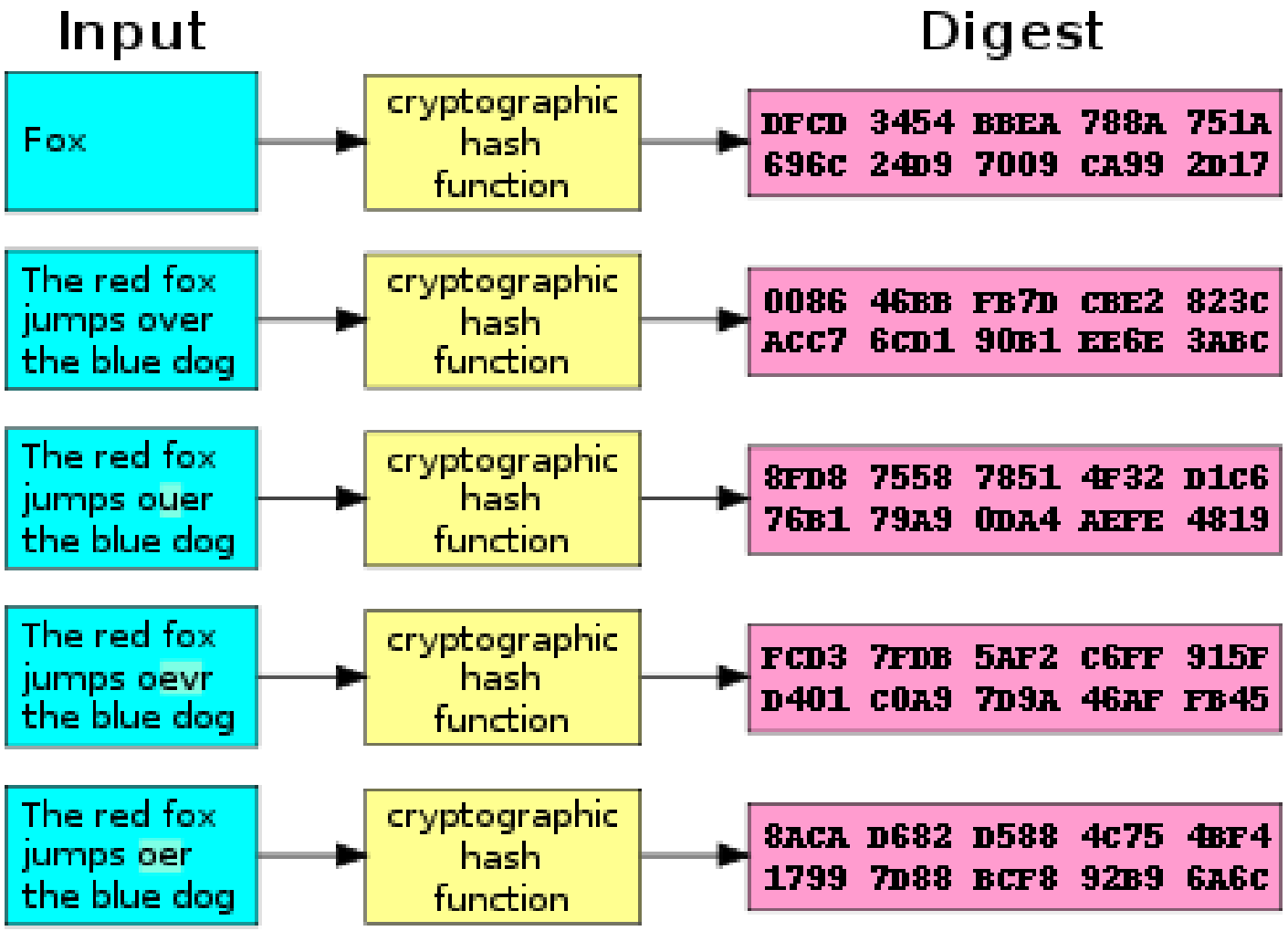
Princip vytvoření

- Z dokumentu se **vypočítá jeho otisk (hash)**
- Otisk dokumentu se **zašifruje soukromým klíčem** podepisujícího
- Výsledek – **elektronický podpis připojený k dokumentu**
- Příjemce si může podpis ověřit
  - **pomocí veřejného klíče** podepisujícího

Hash funkce

- **Krátký unikátní řetězec znaků**
  - vypočítá se z dokumentu pomocí hashovací funkce
- Každý dokument má svůj **jedinečný hash**
  - **malá změna dokumentu způsobí jiný hash**
- **Jednosměrný proces**
  - nelze z hash rekonstruovat původní dokument
- Jakákoliv **úprava dokumentu po podpisu bude odhalena**

Hash funkce


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

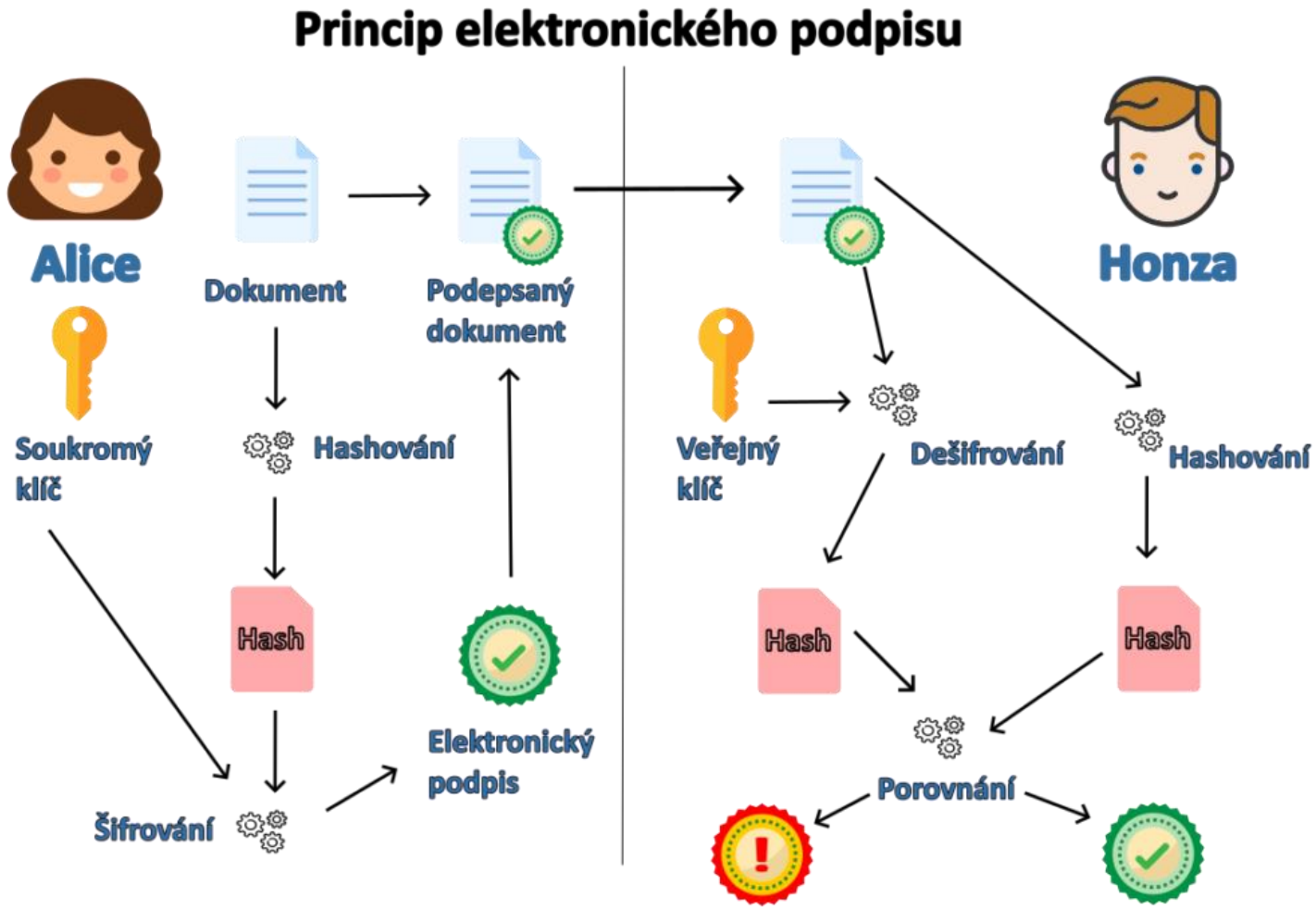
Použití hash při tvorbě

- Při podepisování souboru se nepodepisuje celý soubor
  - **podepisuje se pouze hash souboru**
- Je to **rychlejší** (hash je krátký, soubor může být veliký)
- Dokument zůstává čitelný
  - podpis nezasahuje do obsahu dokumentu
- Zajišťuje neměnnost

Použití hash při tvorbě

- Při podepisování
  - **vypočítáme hash dokumentu**
  - hash **zašifrujeme soukromým klíčem** podepisujícího
  - výsledek připojíme jako elektronický podpis
- Při ověřování
  - příjemce **spočítá hash**
  - **odemkne podpis veřejným klíčem** podepisujícího
  - **získá originální hash**
  - **porovná oba hashe**
    - pokud je shoda – dokument je pravý, nepozměněný

Použití hash při tvorbě



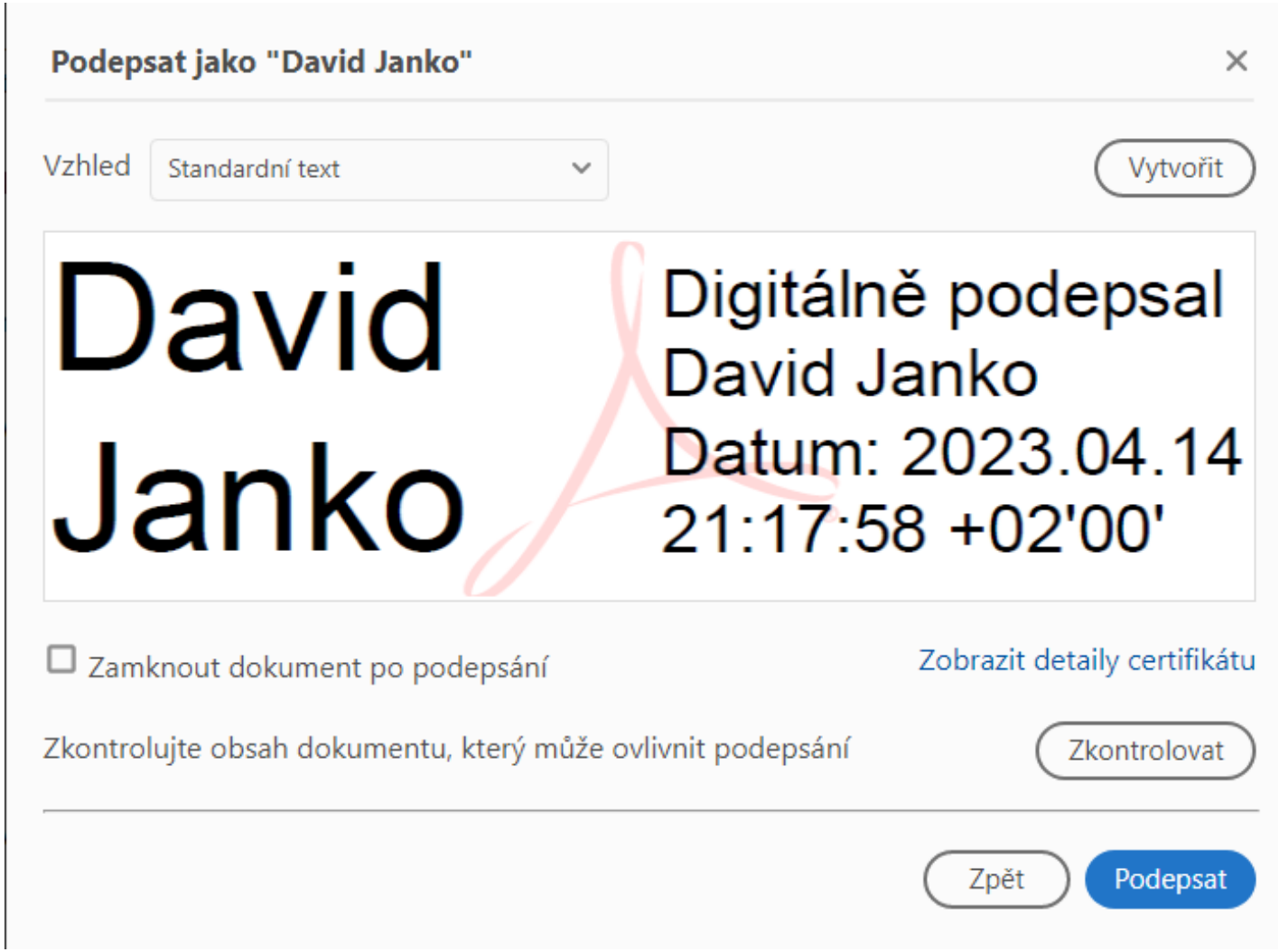
MěSOŠ Klobouky u Brna

VYUŽITÍ ELEKTRONICKÉHO PODPISU V PRAXI

Podpis smluv, dokumentů

- **Rychlé a bezpečné podepsání dokumentu odkudkoliv**
  - bez nutnosti tisku a fyzického podpisu
- Po podpisu – **právně závazný dokument**
  - s užitím kvalifikovaného podpisu
- **Zabrání jakýmkoliv úpravám ve smlouvě**
- Příklad – pracovní smlouva, objednávka, žádost o dotace…

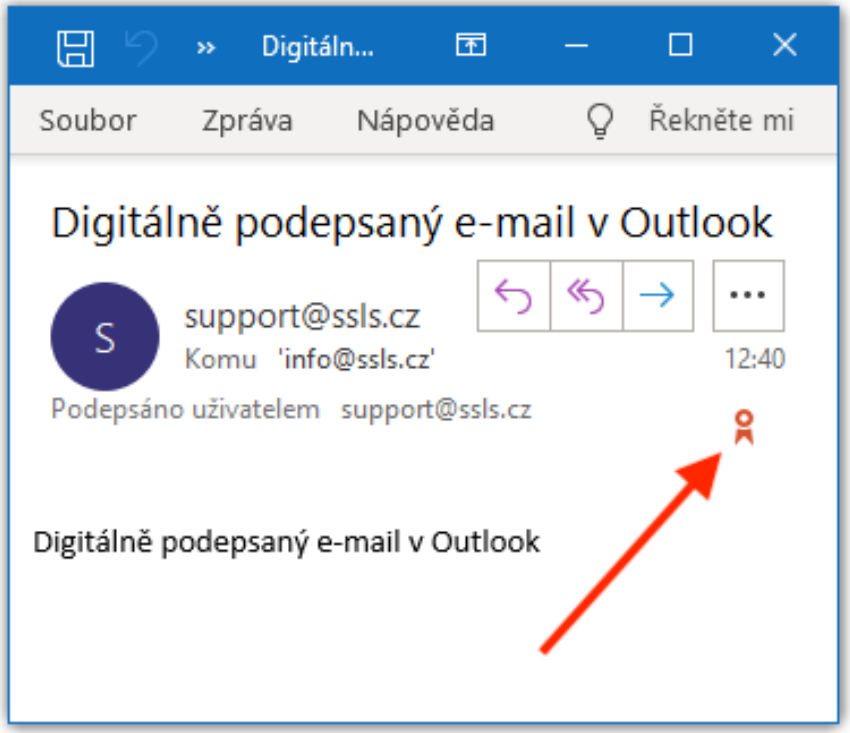
Podpis v PDF



MěSOŠ Klobouky u Brna

Podpis e-mailů

- **Ověření odesílatele e-mailu**
- **Zabránění podvrženým zprávám**
- Chrání před phishinovými útoky
- Zajišťuje neměnnost zprávy po cestě
- Ikonka důvěryhodnosti odesílatele

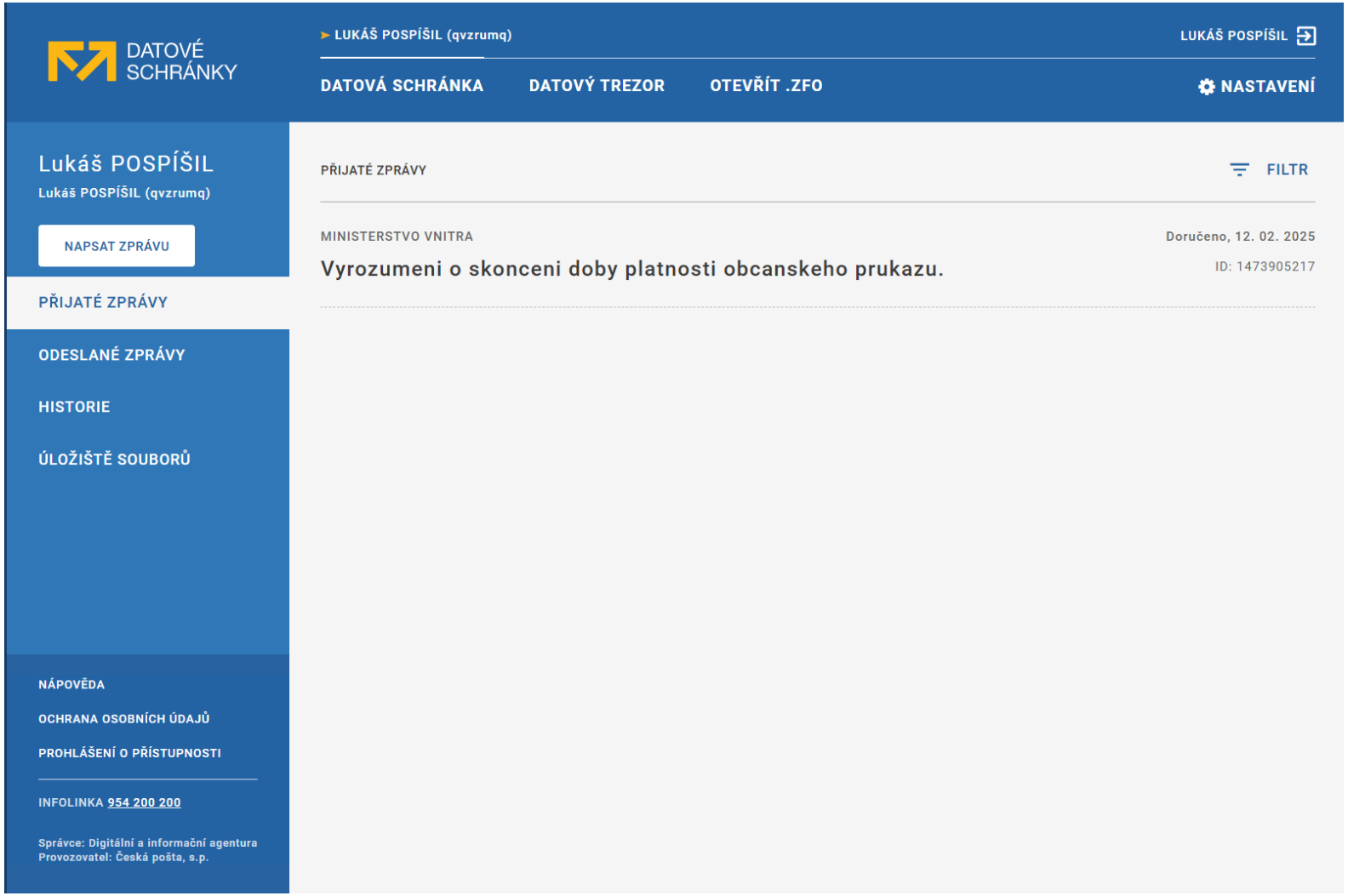


MěSOŠ Klobouky u Brna

Komunikace se státem

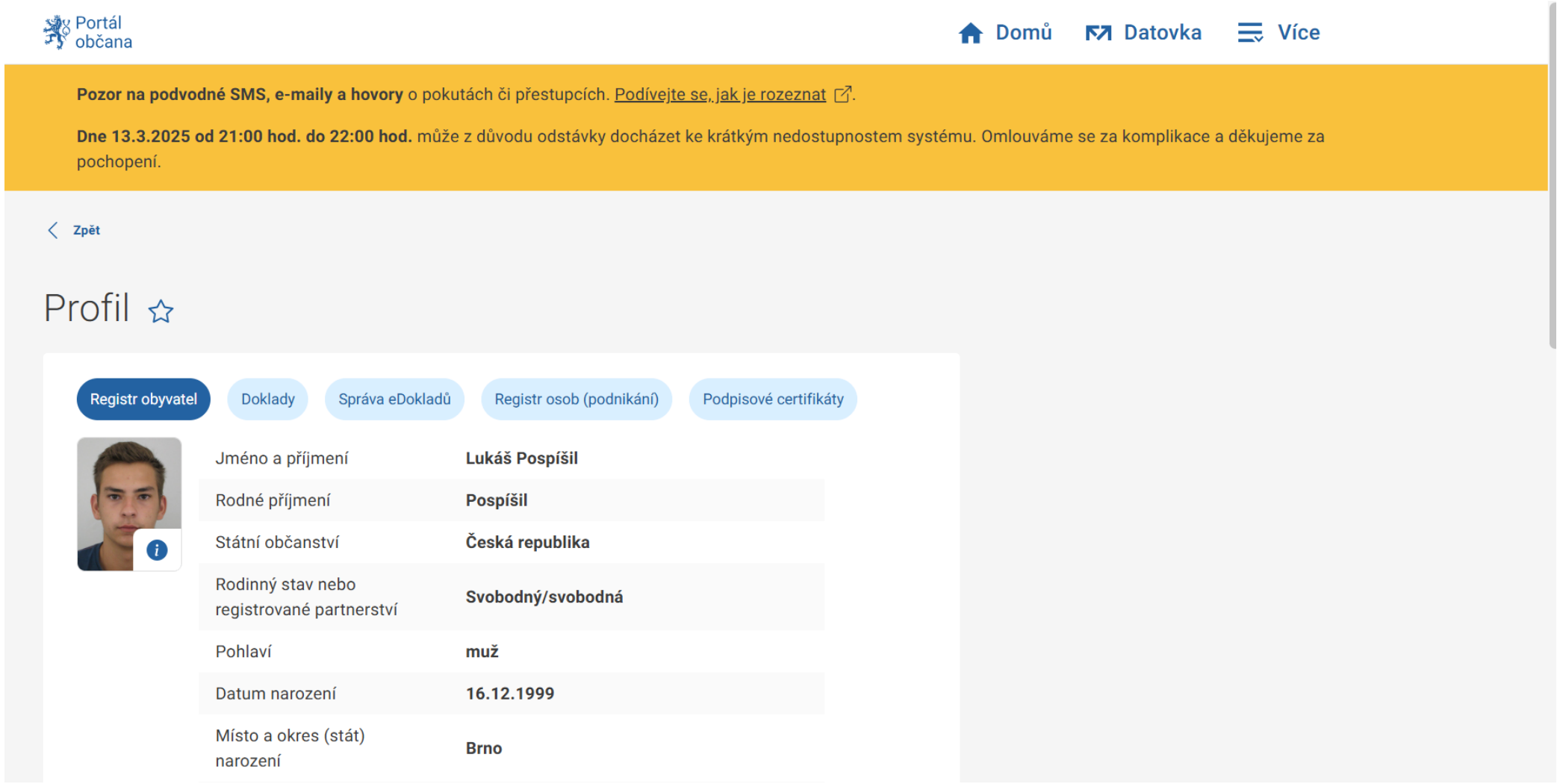
- **Datová schránka**
  - každá odeslaná zpráva přes DS je podepsána elektronicky
    - automaticky
  - není potřeba dokument opatřovat elektronickým podpisem
  - například pro zasílání daňového přiznání, komunikace s úřady veřejné správy…
- **eObčanka**
  - občanský průkaz s čipem
  - obsahuje kvalifikovaný elektronický podpis

Datová schránka

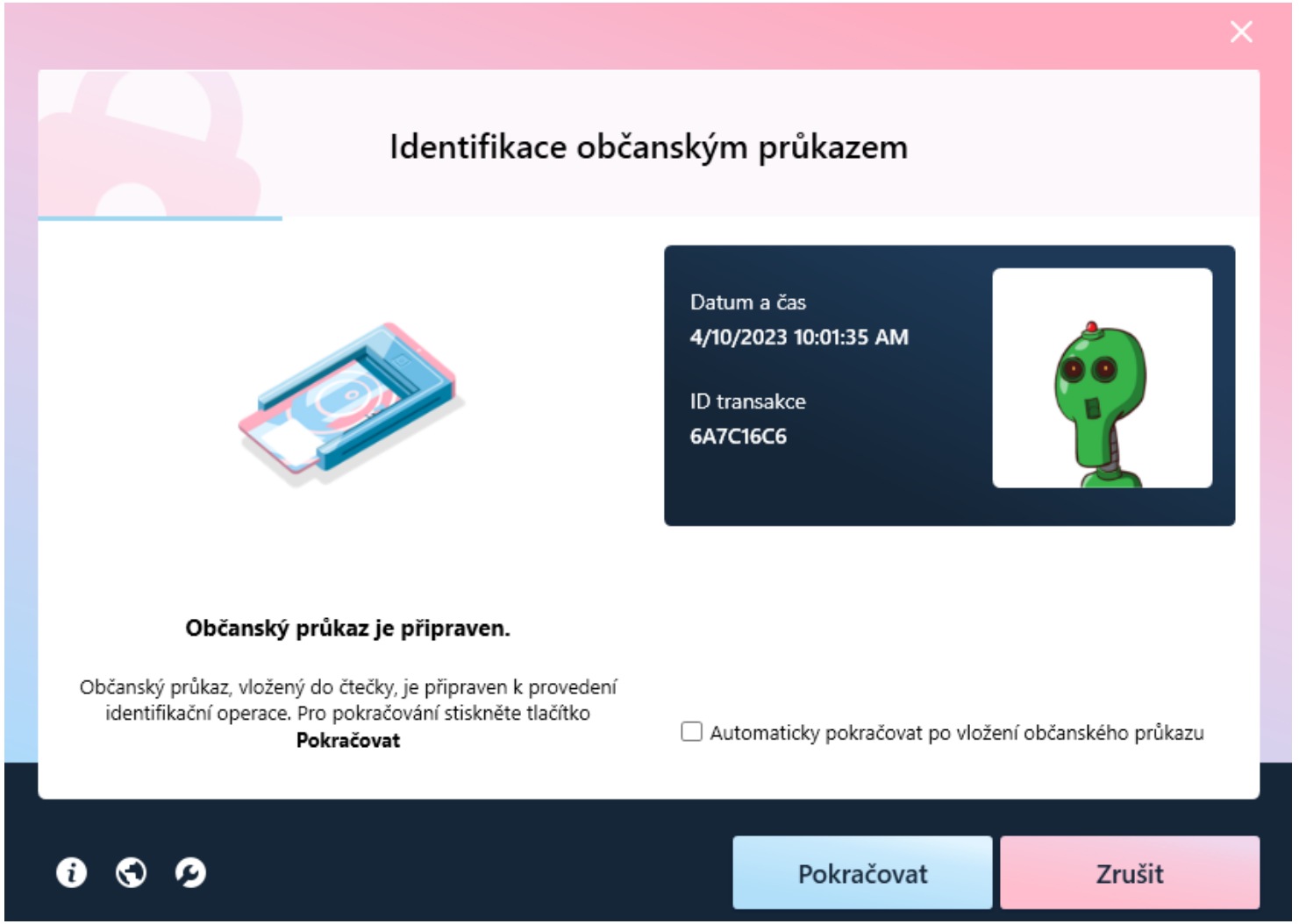


MěSOŠ Klobouky u Brna

Portál občana



eObčanka



MěSOŠ Klobouky u Brna

Online bankovnictví

- **Potvrzení plateb, smluv, přihlašování**
- **Bankovní identita**
  - podpis dokumentů v různých službách
  - přihlášení do systému státní správy, Portál občana, Datová schránka…
  - e-shopy s ověřením věku…

METODY OVĚŘENÍ PRAVOSTI

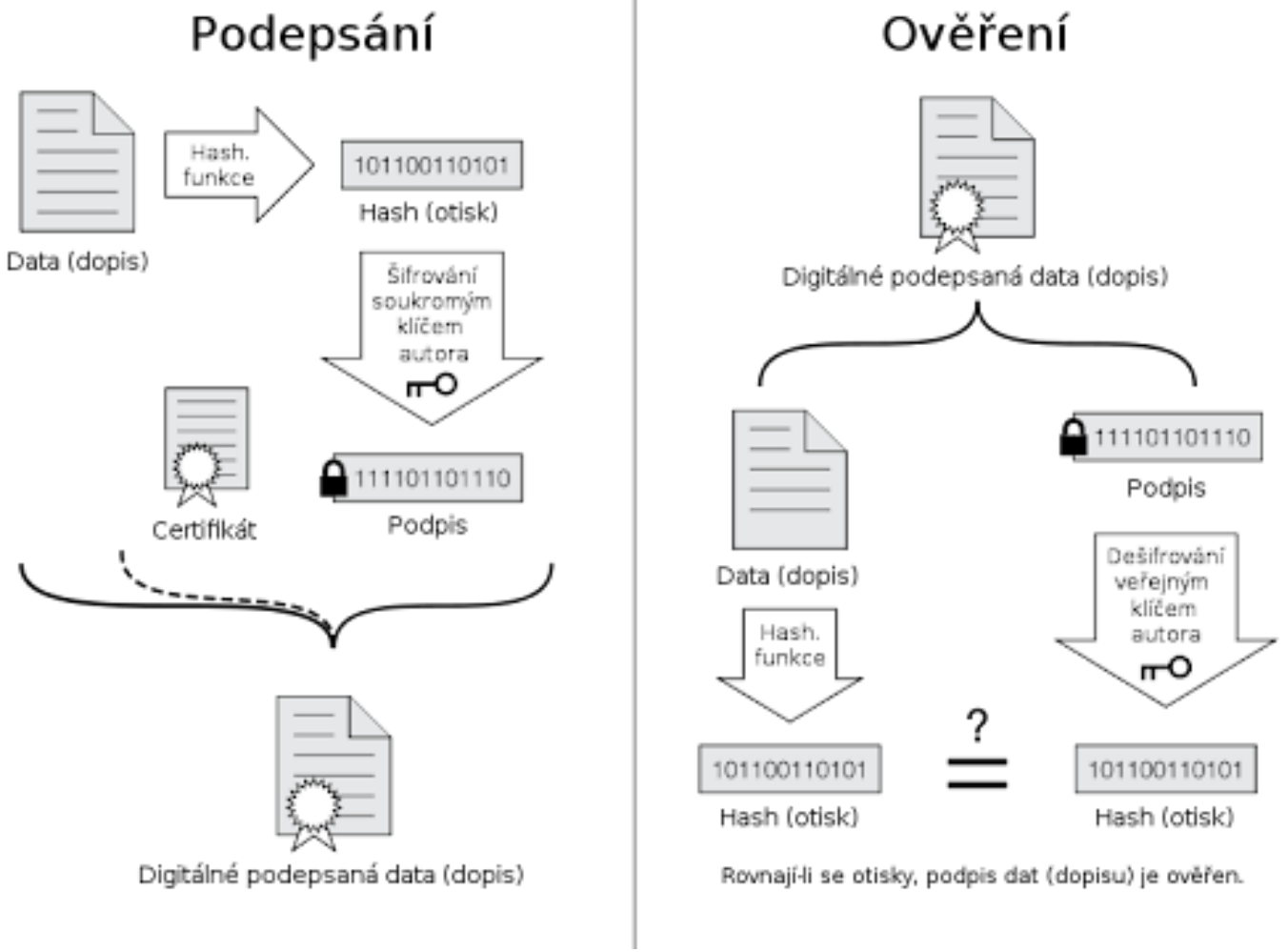
Metody ověření pravosti

- Podpis bez možnosti ověření pravosti je k ničemu
- Ověření musí zajistit
  - **autenticitu**
    - podpis byl vytvořen konkrétní osobou
  - **integritu**
    - dokument nebyl po podpisu změněn
  - **validaci certifikátu**
    - podpis je platný, nebyl zneplatněn

Hash a veřejný klíč

- Při ověření – **veřejný klíč podepisujícího k ověření hash hodnoty dokumentu**
- Ověřující strana **získá veřejný klíč podepisujícího**
  - z dokumentu **vypočítá hash**
  - pomocí **veřejného klíče dešifruje hash**
    - jsou stejné – dokument je pravý, nebyl změněn
    - různé – dokument byl změněn, podpis není platný
- Například Acrobat ukáže
  - jestli je podpis platný
  - jestli nebyl změněn

Hash a veřejný klíč



MěSOŠ Klobouky u Brna

PKI

- Infrastruktura pro distribuci a správu veřejných klíčů a digitálních certifikátů
- Pomocí přenosu důvěry umožňuje
  - **používat cizí veřejné klíče a důvěřovat tak původu zpráv**
  - **bez nutnosti individuální kontroly klíčů**

PKI

- Pro ověření, jestli je veřejný klíč skutečně dané osoby
  - **certifikáty vydané certifikační autoritou**
- Certifikát obsahuje veřejný klíč podepisujícího
  - je **podepsán certifikační autoritou**
- Webový prohlížeč nebo PDF čtečka ověří, jestli byl dokument vydán důvěryhodnou CA
  - **podepsaný důvěryhodnou CA – platný**
  - **nepodepsaný důvěryhodnou CA – varování**

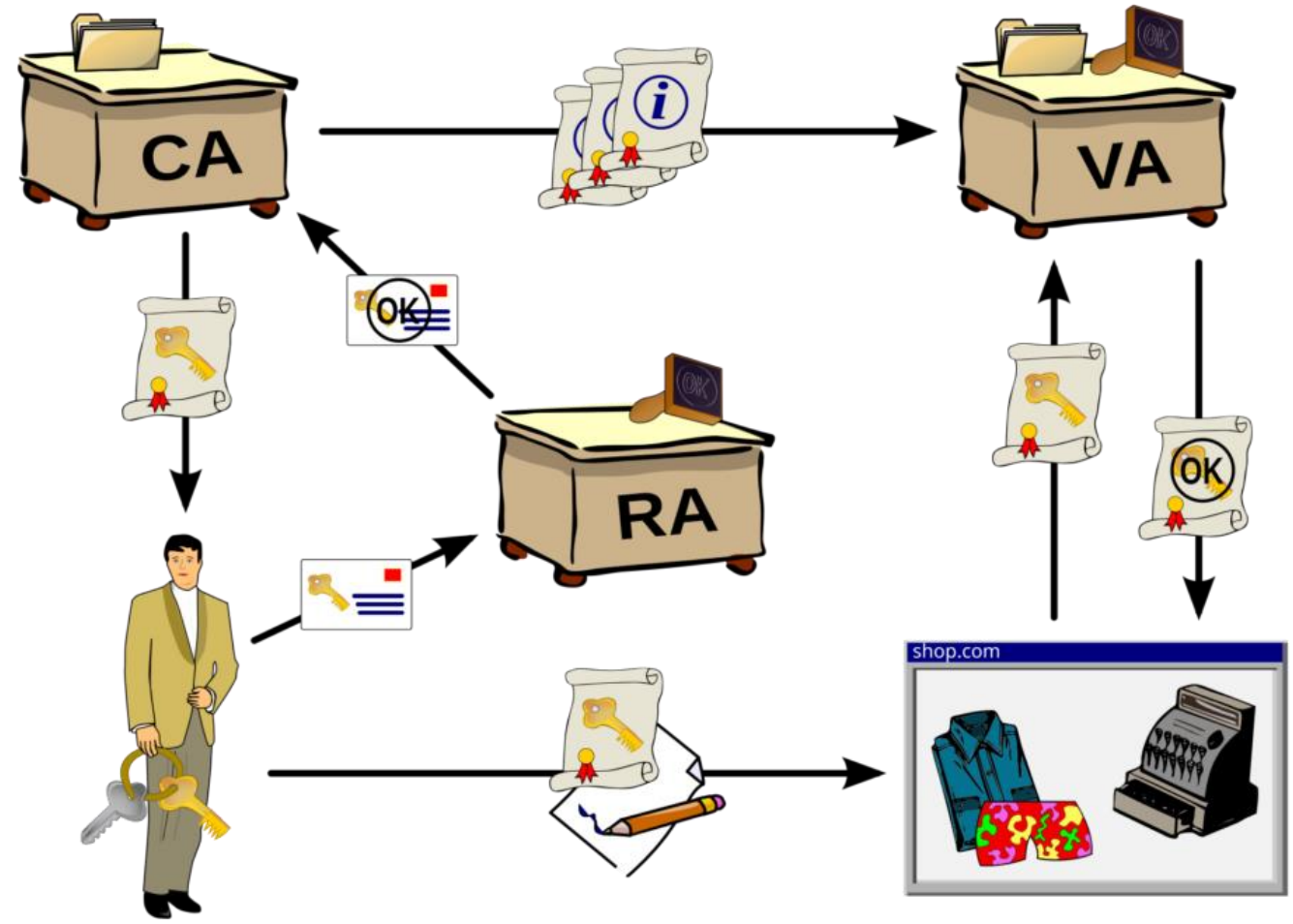
PKI - součásti

- **Certifikační autorita (CA)**
  - ukládá, vydává a podepisuje certifikáty,
- **Registrační autorita (RA)**
  - ověřuje identitu žadatelů,
- **Centrální adresář**
  - bezpečné místo pro ukládání a indexaci klíčů.

PKI

- PKI zajišťuje:
  - **integritu zpráv**
    - zpráva nebyla změněna (od vytvoření podpisu, zašifrování)
  - **nepopíratelnost**
    - doložení původce zprávy (např. pomocí elektronického podpisu)
  - **důvěrnost**
    - nemožnost odposlechu při přenosu zpráv (pomocí šifrování)

Schéma principu výměny klíčů CA



MěSOŠ Klobouky u Brna

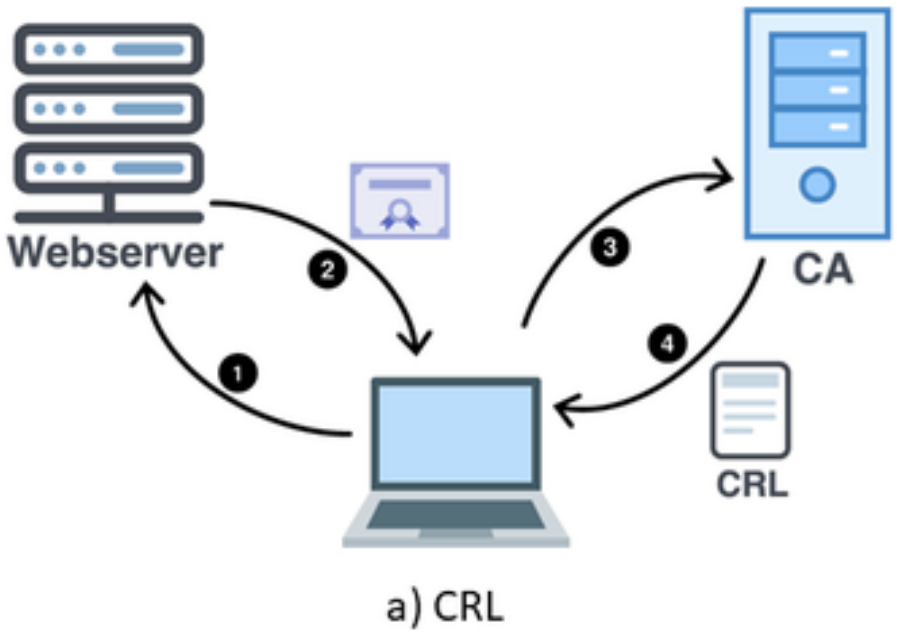
Platnost

- Certifikát má **omezenou dobu platnosti**
  - zpravidla 1 rok
- Může být zneplatněn i před ukončením doby platnosti
- Například – firma odvolá cert. svého zaměstnance
  podpis se stane neplatným

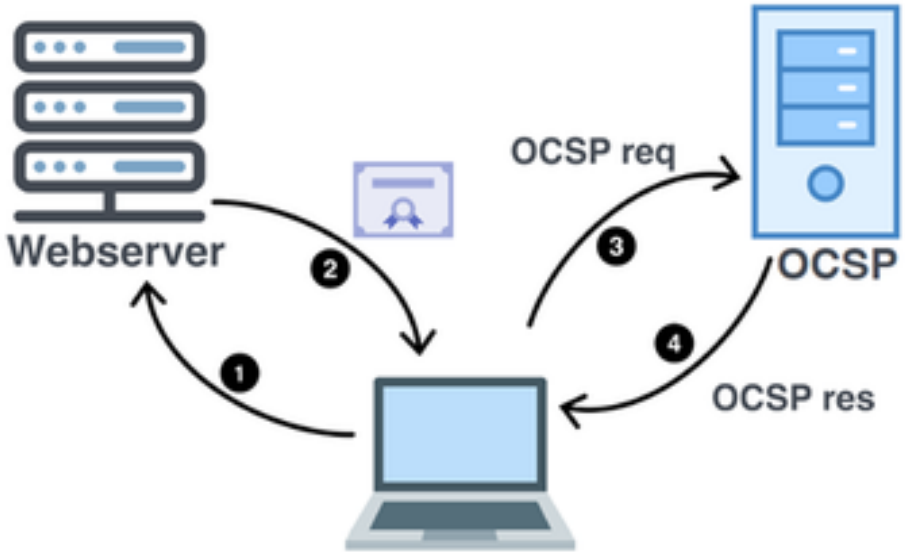
Platnost

- Existují dva základní způsoby pro ověření platnosti:
  - **CRL (Certificate Revocation List)**
    - **seznam zneplatněných certifikátů**
    - pravidelně zveřejňuje CA
    - potřeba neustále aktualizovat a stahovat.
  - **OCSP (Online Certificate Status Protocol)**
    - **online dotaz na server autority**
    - okamžitě ověří stav certifikátu
    - rychlejší a používanější způsob
      - PDF čtečka, e-mailový klient

Mechanismus CRL a OCSP



a) CRL



b) OCSP

MěSOŠ Klobouky u Brna

Způsob ověřování důvěry

- Pro zajištění důvěryhodnosti podpisu
  - nutnost ověřit **pravost veřejného klíče podepisující osoby**
- Využívají se dva hlavní způsoby
  - pomocí CA – tzv. **hierarchická struktura**
  - pomocí sítě důvěry – tzv. **distribuovaný systém**

Certifikační autorita – hierarchická struktura

- Spoléhá na **důvěryhodnou třetí stranu – CA**
- Uživatelé věří, že CA vydává certifikáty po řádném ověření
- CA podepisuje certifikáty svým **soukromým klíčem**
  - důvěřujeme CA -> důvěřujeme klíčům, které vydala
- Může využívat registrační autoritu (RA)
  - ověřuje totožnost žadatelů
- **Tento model tvoří základ PKI**

Síť důvěry – distribuovaný systém

- **Síť důvěry (Web of Trust)**
- Nevyužívá jednu autoritu
  - umožňuje uživatelům **vzájemné podepisování veřejných klíčů**
- Každý uživatel nastaví vlastní podmínky důvěry
  - např. „Budu důvěřovat klíčům, které podepsali alespoň dva lidé, kterým důvěřuji.“
- Každý si může vystavit certifikát a sám si ho podepsat
  - **self-signed certificate**
  - PGP/GPG – nástroje pro šifrování a podpis e-mailů

Distribuce klíčů

- Pro ověření podpisu – nutnost získat **správný veřejný klíč podepisujícího**
- CA vydávají digitální certifikáty obsahující veřejné klíče
- Distribuovat můžeme
  - **přímým sdílením**
  - **certifikátem podepsaným CA**
  - **hiearchickou PKI infrastrukturou**

ÚROVNĚ ELEKTRONICKÉHO PODPISU

Legislativa

- EU a ČR
  - nařízení **eIDAS (EU 910/2014)**
- Tři úrovně zabezpečení
  - prostý – (jednoduchý)
  - uznávaný
  - zaručený
  - kvalifikovaný

Jednoduchý elektronický podpis

- Nejzákladnější forma
- **Nejnižší úroveň zabezpečení**
- Naskenovaný podpis, zaškrtávací políčko na webu „Souhlasím“, napsání jména do e-mailu
- Může být zfalšován, **není platný pro smlouvy**

Zaručený elektronický podpis

- **Vyšší úroveň zabezpečení**
- **Vázaný na identitu**
- Založen na certifikátu bez dalších podmínek
- Lze uložit na HW prostředek (token, čip)
- K podepisování smluv mezi firmou/zaměstnancem
- Firemní komunikace
- **Není ekvivalentní vlastnoručnímu podpisu podle zákona**

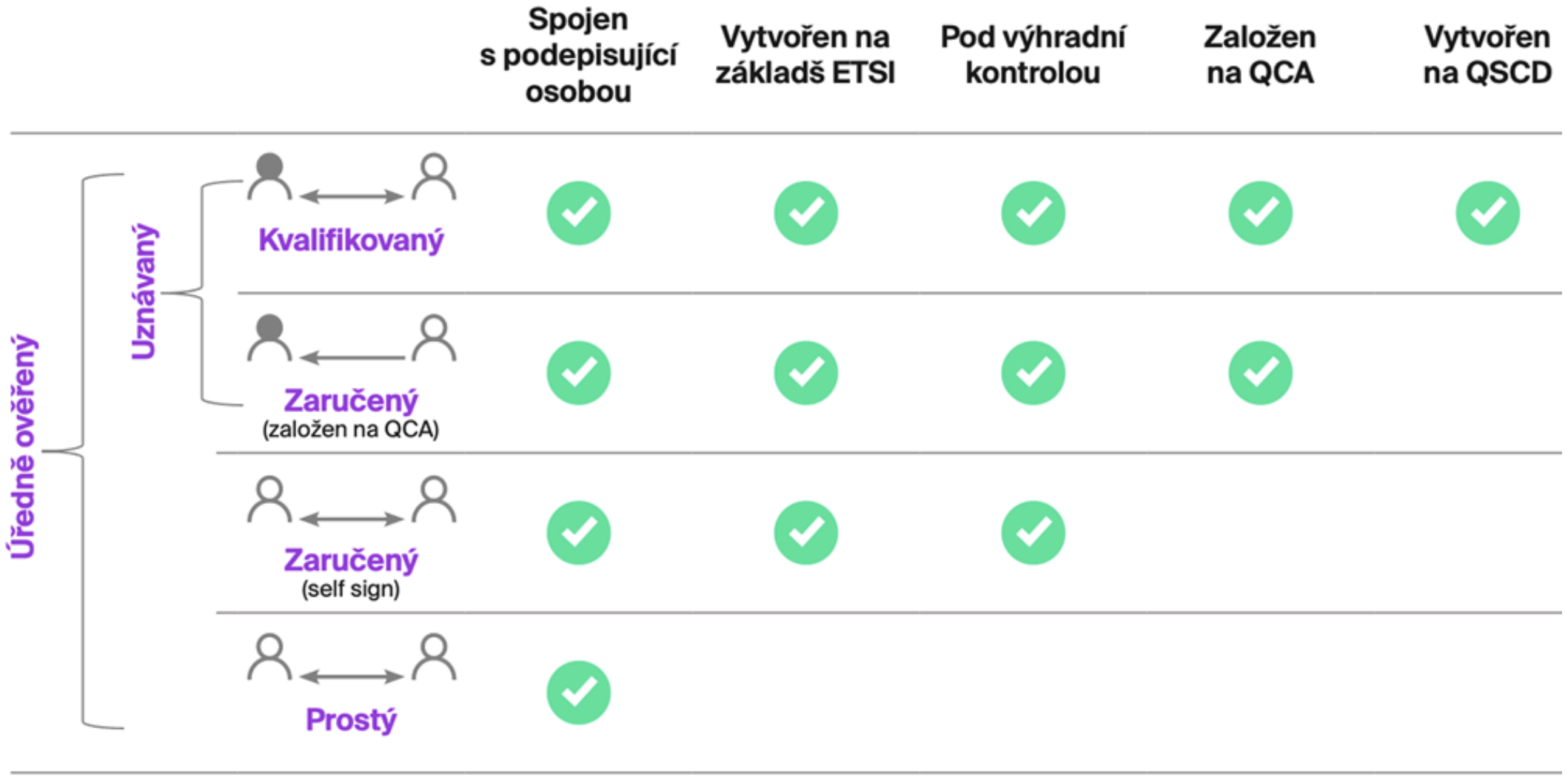
Uznávaný elektronický podpis

- Též označován jako zaručený, založený na kvalif. certifikátu
- **Vyšší úroveň zabezpečení**
- **Vázaný na identitu podepisující osoby**
- Založen na **kvalifikovaném certifikátu**
  - **vydává důvěryhodná CA** (PostSignum)
- Lze uložit na HW prostředek (token, čip)
- K podepisování smluv mezi firmou/zaměstnancem
- Firemní komunikace
- **Není ekvivalentní vlastnoručnímu podpisu podle zákona**

Kvalifikovaný elektronický podpis

- **Nejvyšší úroveň zabezpečení**
- **Vázaný na identitu**
- **Právně závazný**, nahrazuje vlastnoruční podpis
- Založen na **kvalifikovaném certifikátu**
  - **vydává důvěryhodná CA** (PostSignum)
- **Musí** být uložen na HW prostředek (token, eOběanka…)
  - zajištění, že klíč neopustí fyzické médium (token)
- **Jediná plně uznávaná varianta podle české legislativy**

Úrovně podpisů



MěSOŠ Klobouky u Brna

CERTIFIKÁTY

Certifikáty

- Ověřují identitu podepisujícího
- Zajišťují pravost podpisu
- V rámci EU a ČR se rozlišují dva typy:
  - **osobní**
  - **komerční**

Osobní certifikát

- **Ke generování kvalifikovaného elektronického podpisu**
- **Právně rovnocenný vlastnoručnímu podpisu**
- Žadatel
  - **osobně doloží svou totožnost** (pomocí OP)
  - certifikát se vydá na **bezpečné zařízení**
    - USB token, čip…

Komerční certifikát

- **Vydáván právnickým osobám**
  - firmy, úřady, organizace
- K elektronickému podepisování firemních dokumentů, přihlášení do vnitřních systémů státní správy…
- Žadatel
  - **statutární zástupce firmy**
  - certifikát se vydá na **bezpečné zařízení**
    - USB token, čip…
  - **podpis musí být vytvářen kvalifikovaným prostředkem** (QSCD)

Certifikační autority

- organizace, která **ověřuje totožnost žadatelů**
  - vydává jim elektronické certifikáty
- Zajišťuje **správu, revokaci a obnovu certifikátů**
- Certifikační autority v ČR:
  - PostSignum (Česká pošta) – nejrozšířenější v ČR
  - I. CA (První certifikační autorita)
  - eIdentity
  - Bankovní identita
    - nový způsob ověřování

HARDWAROVÉ PROSTŘEDKY

Hardwarový prostředek

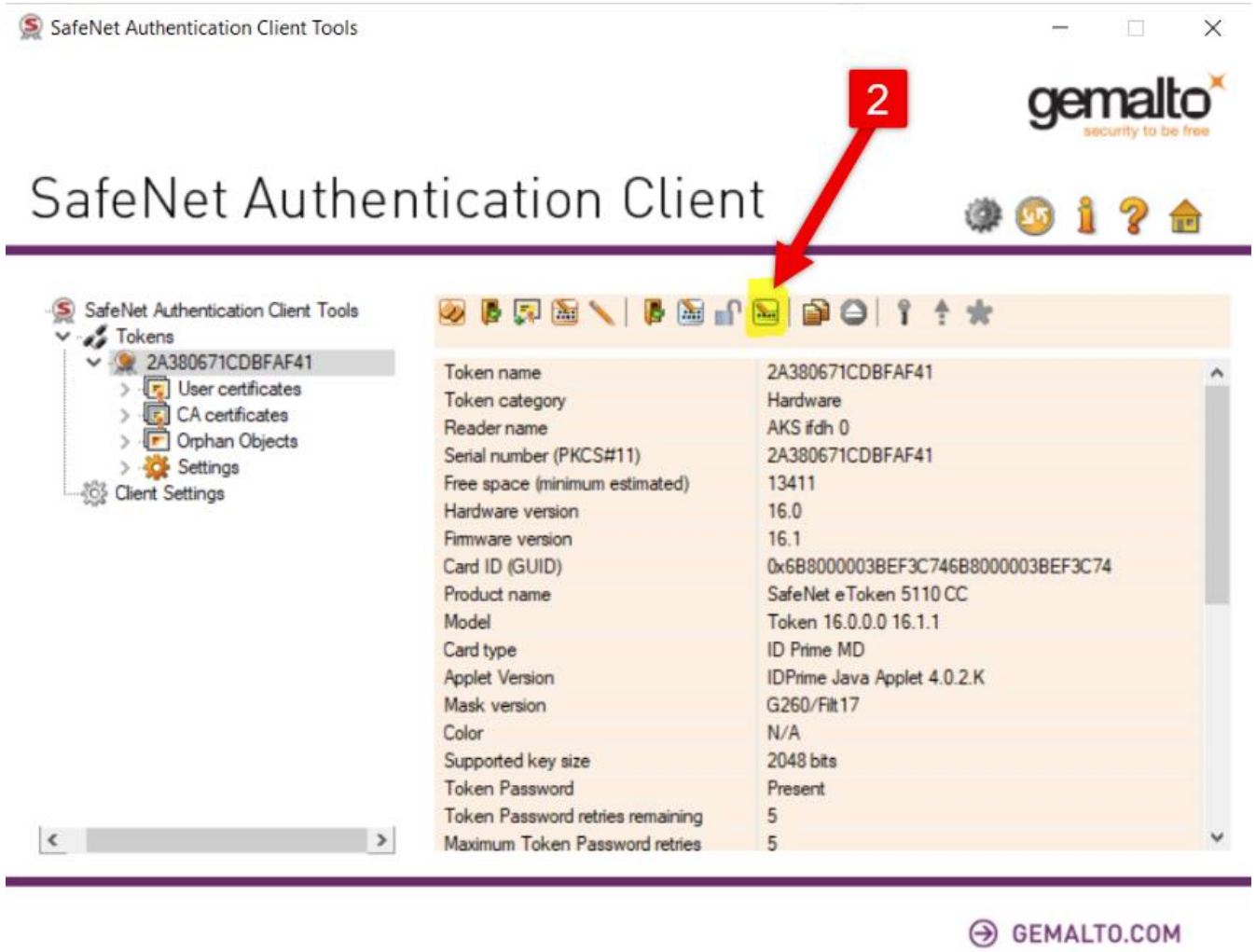
- Elektronický podpis lze uložit
  - softwarově (souborový certifikát)
  - hardwarově
- Hardwarové řešení
  - vyšší bezpečnost
  - **soukromý klíč nikdy neopustí zařízení**
- Pro kvalifikované certifikáty nutnost

Token

- USB zařízení
- **Uchovává soukromý klíč**
- Podepisování dokumentů **bez kopírování klíče do PC**
- Ochrana proti zcizení – nutnost zadat PIN
  - většinou omezeno na 5 pokusů, jinak je zablokován
- Využíván zaměstnanci st. správy, právníky, účetními…

Token

Software pro správu tokenu



MěSOŠ Klobouky u Brna

Čipové karty

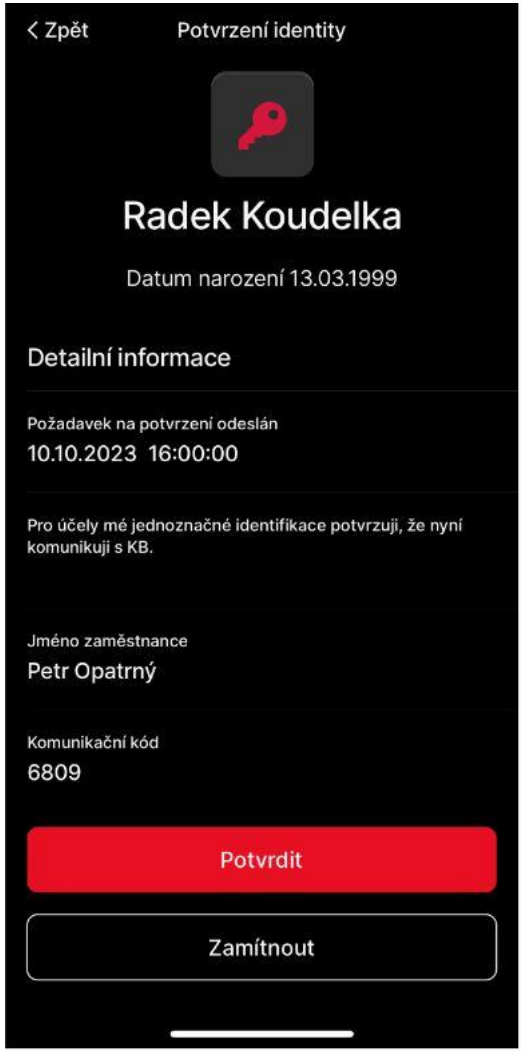
- Plastová karta s **integrovaným čipem**
- Obsahuje **elektronický certifikát**
- Ke čtení potřeba **čtečka čipových karet**
- Ochrana – PIN kód

MěSOŠ Klobouky u Brna

Mobilní telefon

- Mobilní aplikace
  - **Mobilní klíč eGovernmentu**
- **Identifikace pomocí biometriky**
  - otisk prstu, Face ID
- Nebo pomocí **2FA**
  - sms kód, KB klíč…
- Není nutnost vlastnit token nebo čipovou kartu

KB Klíč



MěSOŠ Klobouky u Brna

Mobilní klíč eGovernmentu

MěSOŠ Klobouky u Brna

Anotace

Tato prezentace slouží k seznámení se s principy elektronického podpisu a jeho využitím v digitálním světě. Zaměřuje se na základní pojmy, jako je hashovací funkce, asymetrická kryptografie, digitální certifikát a certifikační autorita. Žáci se naučí, jak elektronický podpis zajišťuje autenticitu a integritu dokumentů a jak se liší jeho úrovně podle legislativy ČR. Dále pochopí, jaké jsou metody ověřování pravosti elektronického podpisu a jaké hardwarové prostředky lze k podpisování využít.

Hlavním cílem je, aby žáci porozuměli principům digitálního podepisování, uměli určit vhodný typ podpisu pro různé situace a byli schopni rozpoznat bezpečnostní rizika spojená s elektronickou autentizací.

Užité zdroje

- https://vyuka.mesosdev.cz/kb/operacni-systemy/kryptografie/elektronicky-podpis/

Autor: Bc. Lukáš Pospíšil

Předmět: Operační systémy

Ročník: 4.

Rok vytvoření: 2025

Poslední aktualizace: 2025

MěSOŠ Klobouky u Brna