

M U N I
M E D

Institut
biostatistiky
a analýz

Uživatel počítačové sítě

Daniel Klimeš, Jan Krejčí, Roman Šmíd



Osnova

1. Pojmy, termíny
2. Připojení k počítačové síti
 - Možnosti připojení, co je zapotřebí, srovnání
3. Síťové služby
 - DHCP, DNS, HTTP, Email, vzdálený přístup
4. Bezpečnost na síti
 - Hesla, viry, firewall, email, spyware, phishing
5. **Šifrování, elektronický podpis, elektronická identita a její prokazování**
6. **Český E-government**
7. Elektronické zdravotnictví ČR



M U N I
M E D

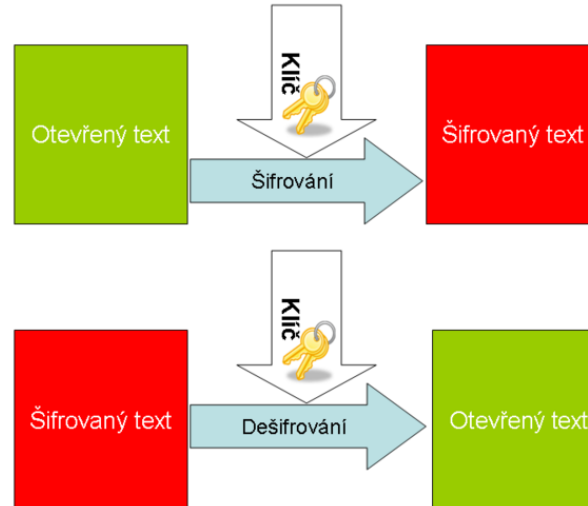
Institut
biostatistiky
a analýz

Šifrování a elektronický podpis



Šifrování

- Změna podoby (zakódování) textu a dat do formy, která je bez znalosti dešifrovacího klíče (hesla) nečitelná



- Lze šifrovat např.
 - Dokumenty (7zip, winrar - symetricky)
 - Emaily (podpora emailových klientů, veřejný klíč adresáta)
 - Síťovou komunikaci (https, sftp, imaps, ssh)
 - Disky (truecrypt, realcrypt, bitlocker)
- Utajení obsahu komunikace a dokumentů



Typy šifrování

Symetrické šifrování

- Jednodušší podoba, pro šifrování i dešifrování je použit jediný klíč - heslo

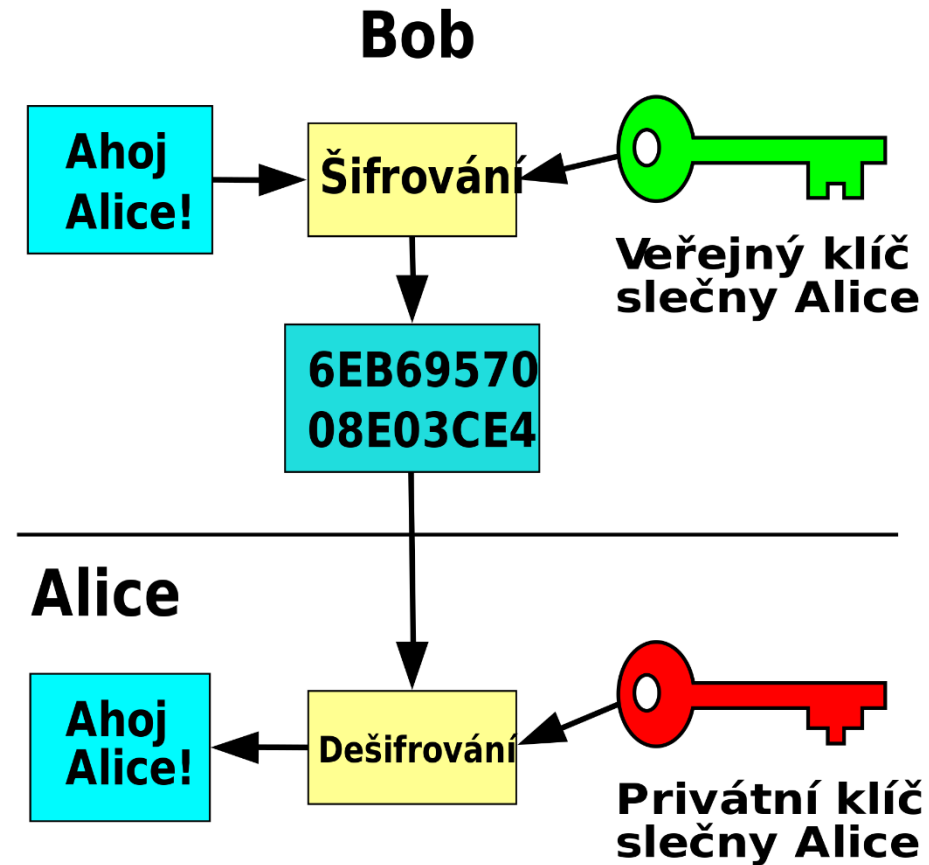
Asymetrické šifrování

- Klíč má dvě části, **soukromou a veřejnou**

Pokud mi chce někdo zaslat **šifrované** informace, zašifruje je pomocí **veřejné části klíče příjemce**.
Jediný, kdo dokáže tato data dešifrovat je vlastník privátní části klíče, tedy já



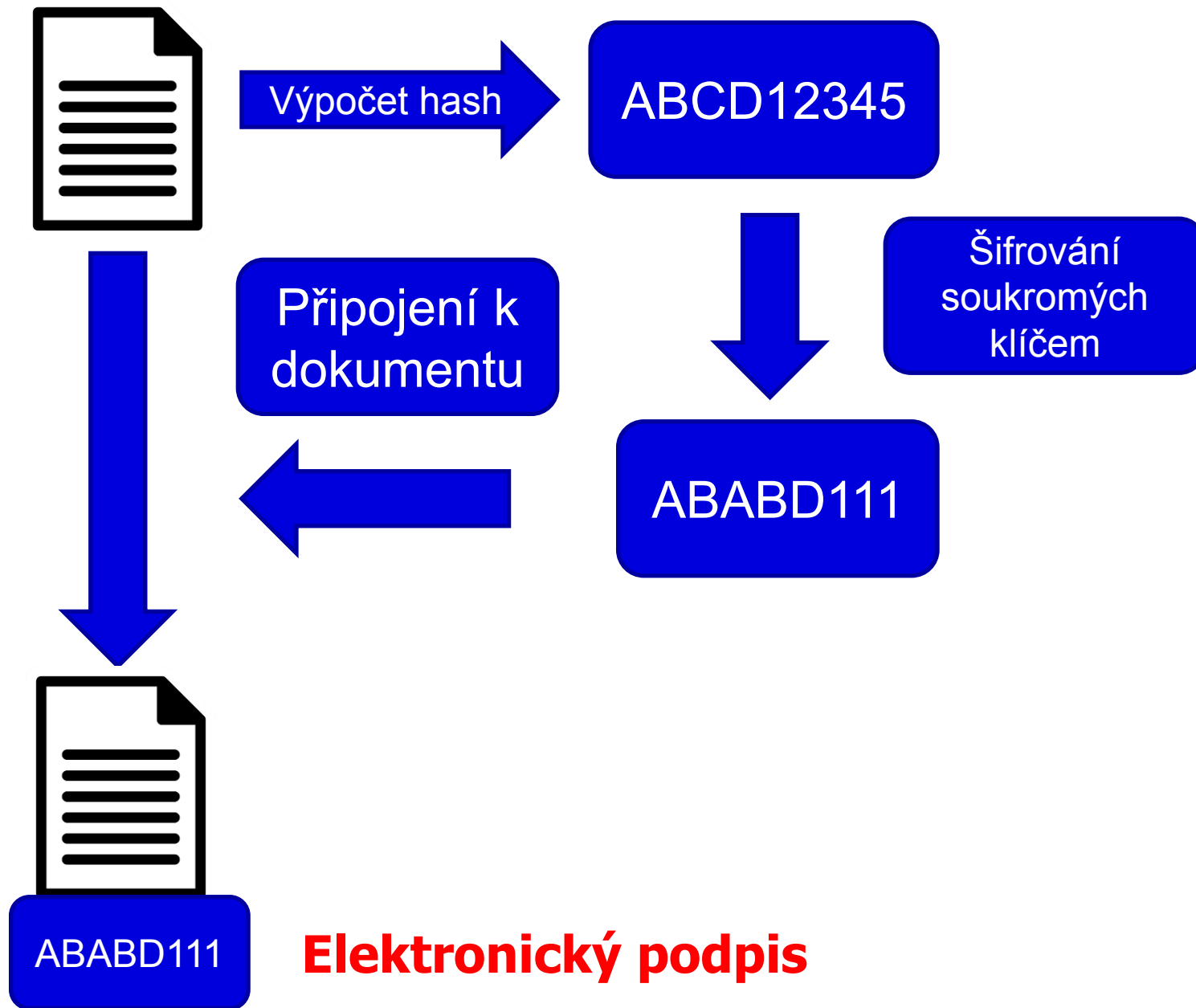
Asymetrické šifrování



Elektronický podpis

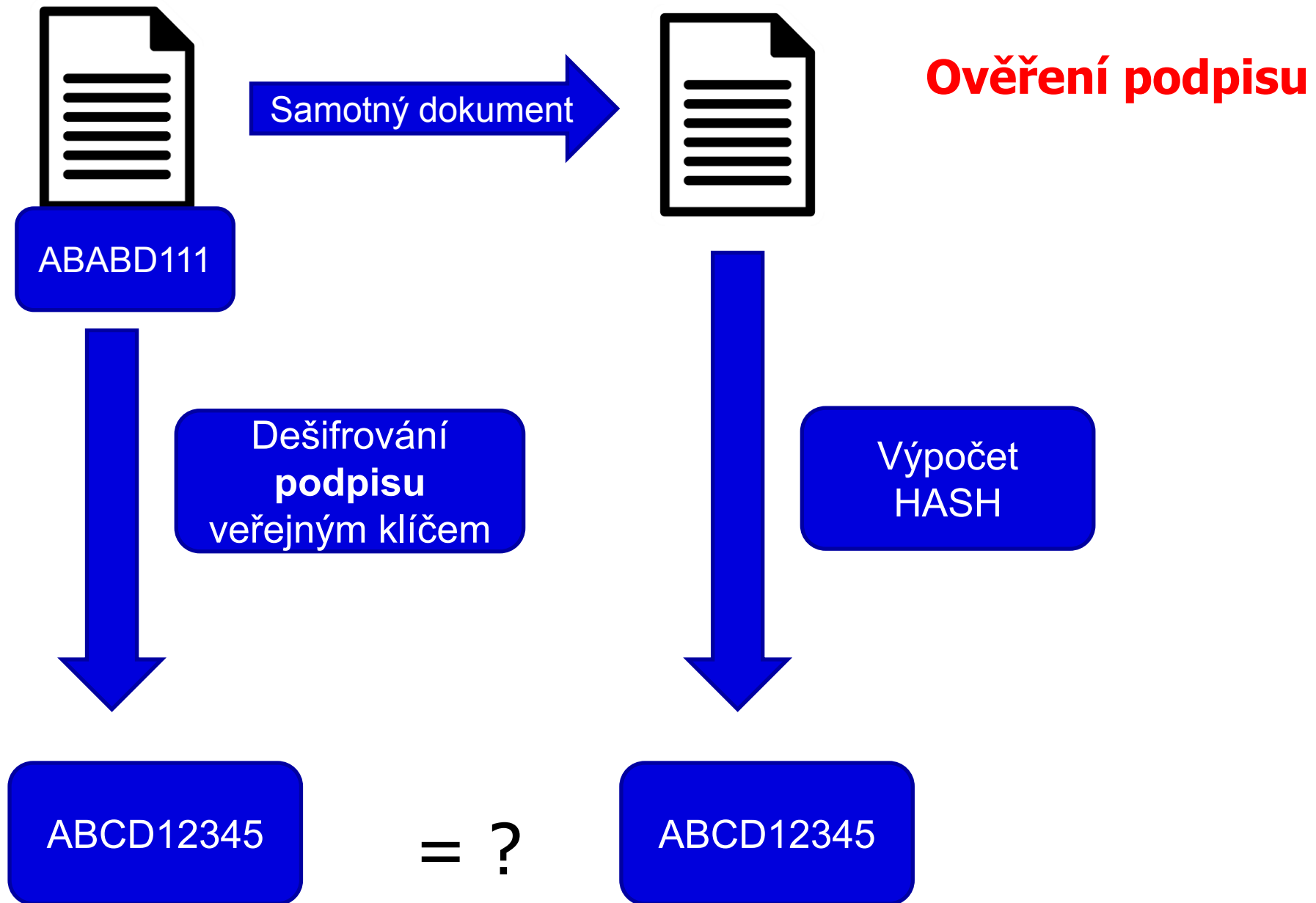
- **Využívá prvky asymetrického šifrování**
- Pokud chci nějaký text digitálně **podepsat**, stačí pro podepsání použít **soukromou** část klíče (provede emailový klient, PDF editor)
- Každý, kdo zná veřejnou část mého klíče (je odesílána automaticky s podepsaným emailem) pak může mnou digitálně podepsaný text
 - Přečíst
 - **Ověřit, zda jsem autorem/odesílatelem**
 - **Ověřit, zda nebyl text někým neoprávněně pozměněn**
- Podepsaný email/dokument **není šifrovaný!!**
 - Nemusíte nic „počítat“ nebo si pamatovat, provede emailový klient nebo jiná aplikace (pdf reader)





Elektronický podpis





Digitální certifikát

- Fyzicky = počítačový soubor od certifikační autority
 - Vydává certifikační autorita
 - Omezená platnost certifikátu (obvykle 1 rok)
- Obsahuje
 - Údaje o subjektu** (uživatel, server)
 - Jméno
 - E-mailová adresa
 - Další identifikační údaje
 - Veřejný klíč subjektu**
 - Oddělenou komponentou je příslušný soukromý klíč**
 - Lze odvolat (revokovat) v případě vyzrazení soukromého klíče
 - Kvalifikovaný** x komerční certifikát



shutterstock · 211348171



Kvalifikovaný x komerční certifikát

□ **Zákon č. 297/2016 Sb. Zákon o službách vytvářejících důvěru pro elektronické transakce**

□ **Kvalifikovaný certifikát**

□ **Vydává kvalifikovaný poskytovatel** služeb vytvářejících důvěru

□ <https://www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru.aspx>

- Česká pošta (PostSignum)
- První certifikační autorita, a. s.
- elidentity a. s.
- Software602 a. s.,
- SEFIRA spol. s r.o.,



Digitální certifikát – jak získat prakticky

- Vydávají akreditované společnosti (např. Česká pošta)
 1. Přihlášení do webové (případně stažení off-line) aplikace
 2. Vlastnoruční vygenerování a uložení páru klíčů s heslem
 3. Vyplnění žádosti
 4. Návštěva pobočky s žádostí, ověření údajů
 5. Zařazení veřejné části klíče certifikační autoritou do seznamu ověřených klíčů
 6. Obdržení podepsaného certifikátu s veřejným klíčem a identifikací

- Na MU lze získat osobní digitální certifikát pro uživatele zdarma na adrese <http://pki.cesnet.cz/cs/tcs-personal.html>
- osobní certifikáty použitelné k zabezpečení elektronické pošty.



Elektronický podpis a eIDAS

- elektronický podpis (FO)

- elektronická pečeť (PO)

a. kvalifikovaný elektronický podpis (QES, Qualified Electronic Signature):

- Musí být založen na kvalifikovaném certifikátu pro elektronický podpis
- Musí být vytvořen pomocí kvalifikovaného (bezpečného) prostředku pro vytváření elektronických podpisů (čipová karta a USB token = **QSCD** (od: Qualified Signature Creation Device)).

b. zaručený elektronický podpis, založený na kvalifikovaném certifikátu

- Musí být založený na kvalifikovaném certifikátu
- Není nutný kvalifikovaný prostředek (certifikovaná čipová karta/token).

c. zaručený elektronický podpis (AdES, Advanced Electronic Signature)

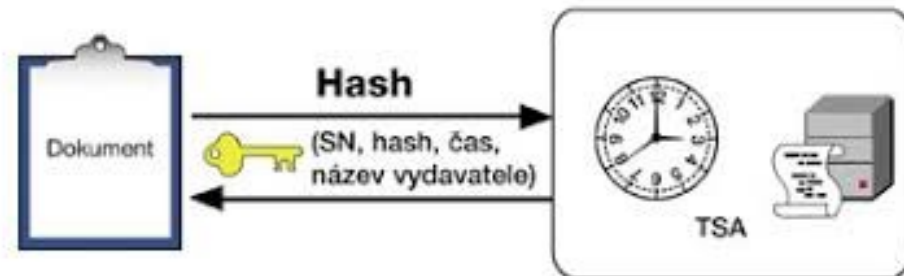
- Bez specifických požadavků na certifikát

Uznávaný elektronický podpis = společné označení pro a. i b.

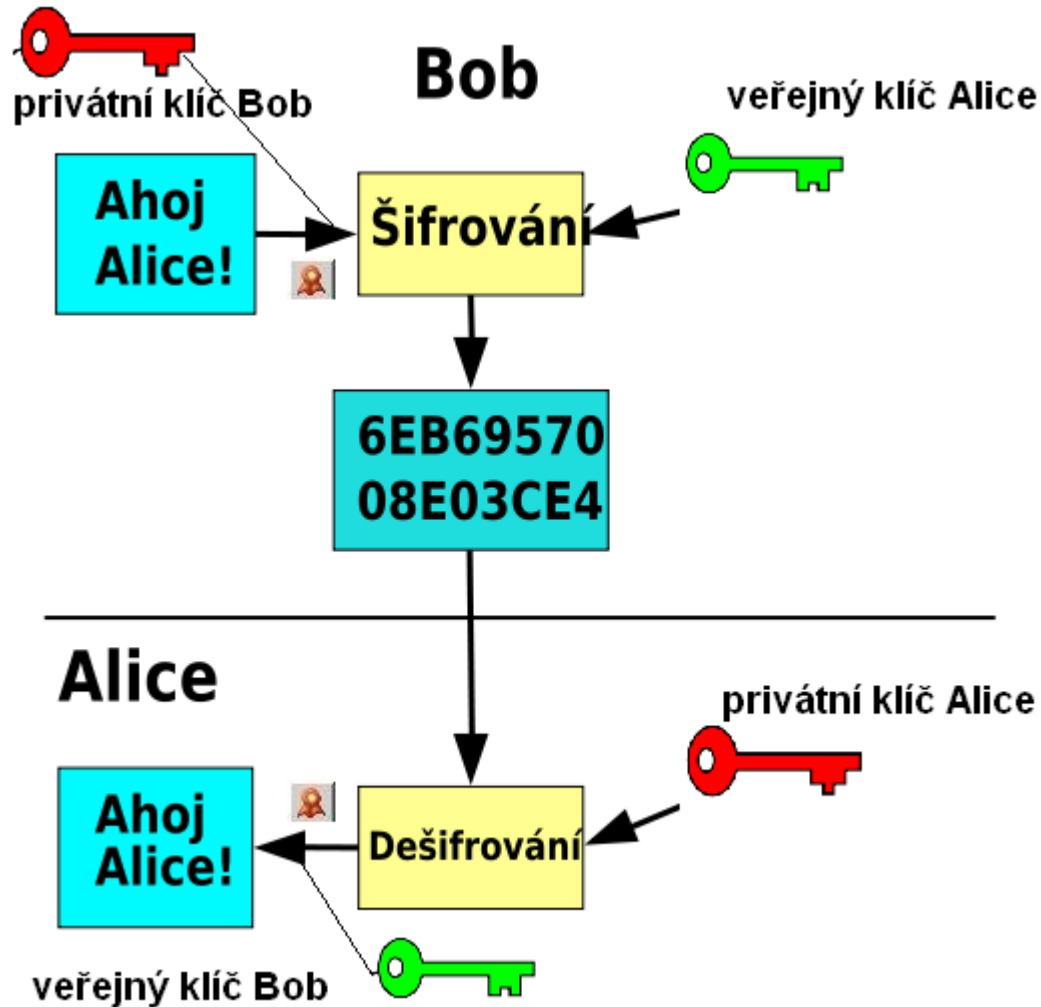


Elektronické časové razítko

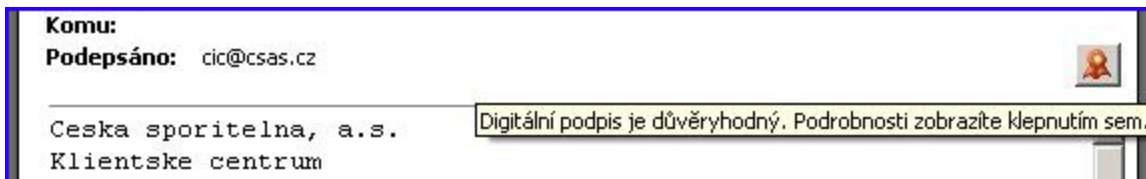
- Doložení, že dokument v daném okamžiku existoval v příslušné podobě.
- Kombinuje se s elektronickým podpisem
 - „Prodlužují“ platnost el. podpisu
- Omezená platnost, ale delší než el. podpis
- Prosté a kvalifikované razítko



Šifrovaný email



- Bob **podepíše** zprávu Alici svým **soukromým klíčem**
- E-mail **zašifruje** **veřejným** klíčem Alice
- Alice **dešifruje** zprávu svým **privátním** klíčem
- **Ověří** Bobův podpis pomocí jeho **veřejného** klíče



Další odkazy

□ Kniha Báječný svět elektronického podpisu (zdarma)

<http://knihy.nic.cz/> (pdf)

□ <https://www.lupa.cz/n/elektronicky-podpis/>



M U N I
M E D

Institut
biostatistiky
a analýz

Elektronická identita a vzdálené ověřování



Vzdálené ověřování osoby



... aneb jak se vzdáleně prokázat, že jsem to já



1) Něco jedinečného vím



Prostředky prokazování identity

2) Něco jedinečného mám

Úroveň důvěryhodnosti (Level of assurance)

- **Nízká**
- **Značná**
- **Vysoká**



Bezpečnostní úroveň prokázání elektronické identity

□ Prostředky dle úrovně důvěryhodnosti:

□ Nízká (Low) - např.: login + heslo

□ Značná (Substantial)

- dvoufaktorová autentizace = potvrzovací SMS, OTP = One Time Password

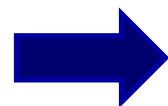
□ Vysoká (High) (čipová karta, elektronický občanský průkaz)



Prostředky prokazování identity

O vydávání těchto prostředků a vlastní ověřování přístupů se stará

- Hesla
- Tokeny
- Karty
- Biometrika
- Mobilní telefony



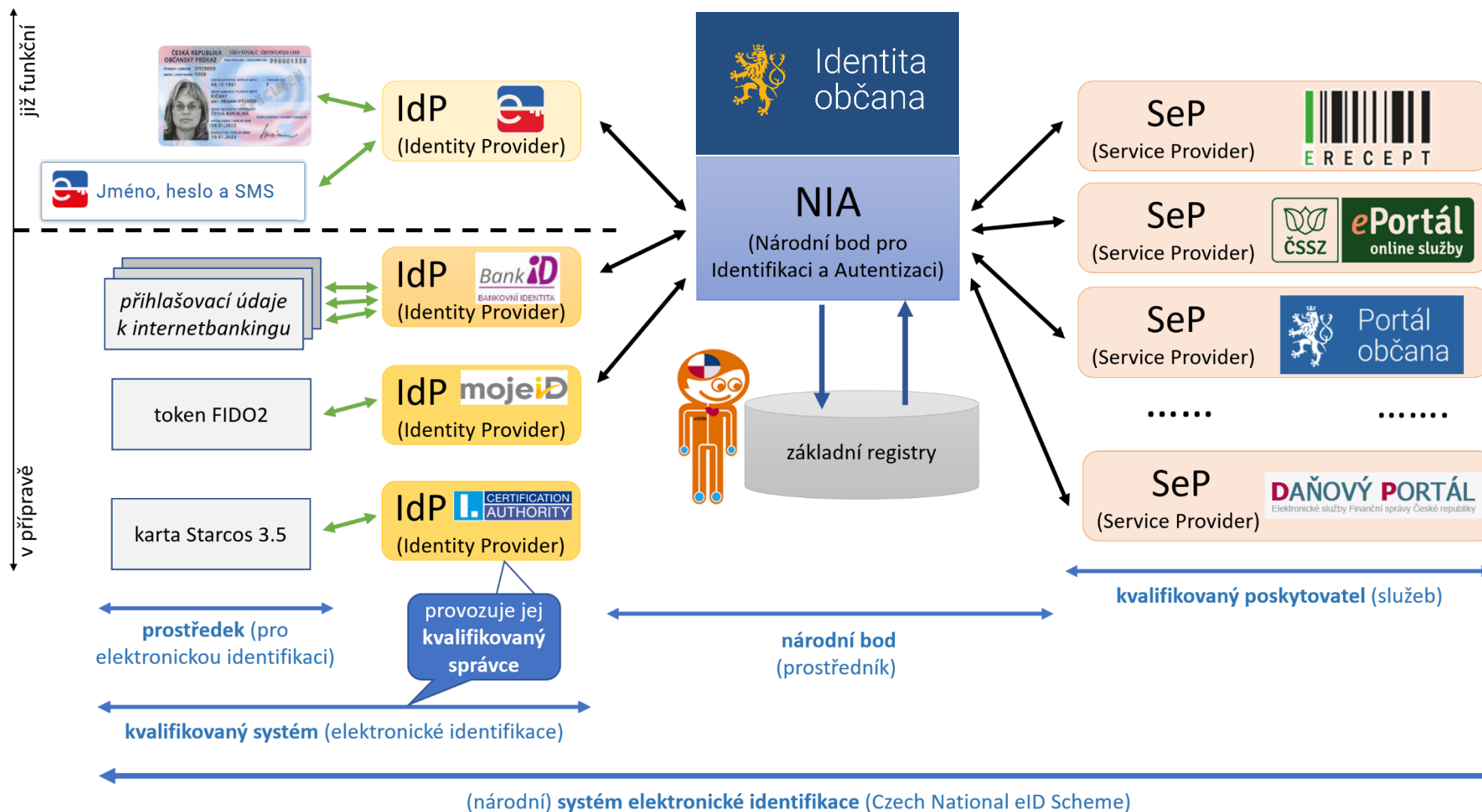
- A) Poskytovatel cílové služby

- B) Dle NIA konceptu „Identity provider“
Poskytovatel identitních prostředků



Ověřování e-identity ZP: budoucí ideální stav

Zdroj: <https://www.lupa.cz/clanky/bankovni-identita-jak-privest-ke-sluzbam-e-governmentu-az-5-5-milionu-lidi/>



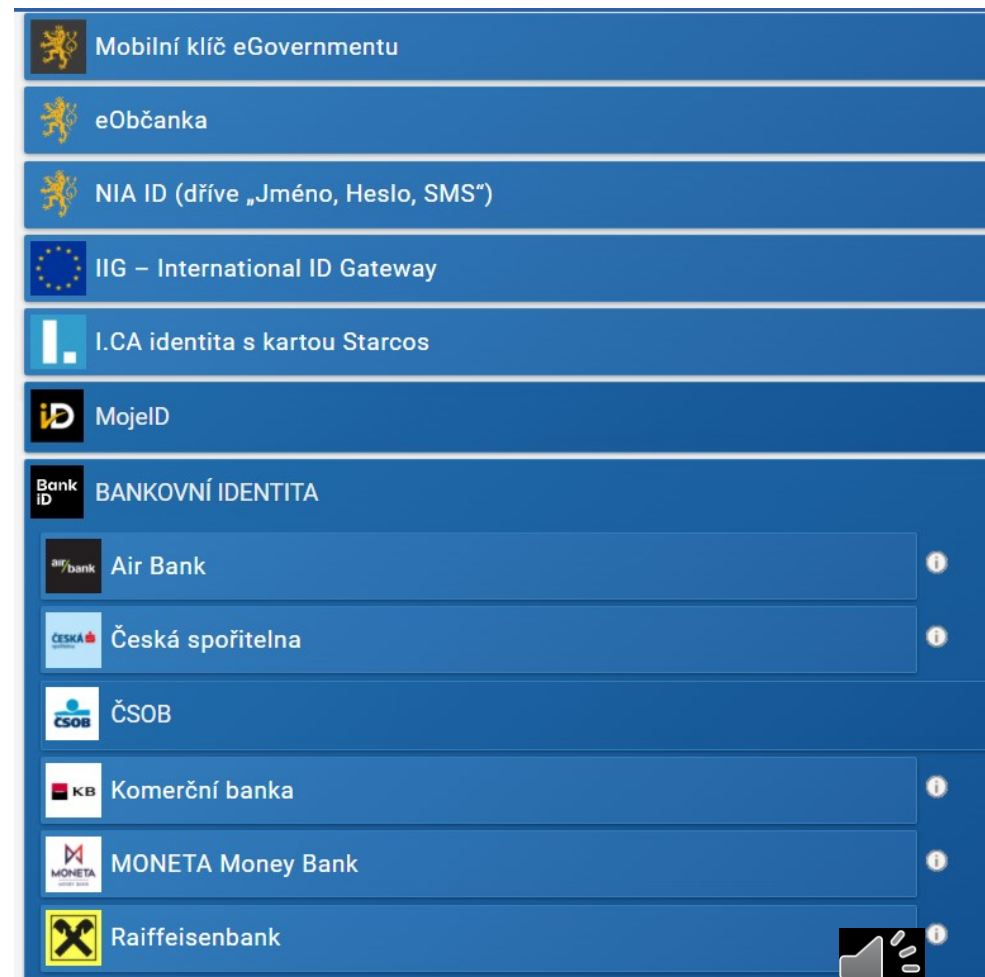
Poskytovatel identitních prostředků

➤ Stát

- Elektronický občanský průkaz od **1. 7. 2018**
- Heslo + jednorázový SMS kód
- Mobilní klíč eGovernmentu

➤ Soukromý poskytovatel

- Bankovní identita
- MojeID
- ...



NIA prostředky – statistika (březen 2023)

Celkem státních ID prostředků	1 518 591
Celkem nestátních ID prostředků	10 565 485
Celkem ID prostředků	12 084 076
Počet profilů alespoň s jedním aktivním prostředkem	6 087 908
Celkový počet unikátních přihlášení	2 432 241
Konverze - procentuální zastoupení těch, kdo se skutečně přihlásili z těch, kdo se přihlásit mohli	39.95%

<https://archi.gov.cz/nap:nia>

Český E-government

- NIA
- Datové schránky
- Základní registry
- Elektronický občanský průkaz
- eDoklady
- Portál občana

Datové schránky

- Funguje jako „webový email“, místo emailové adresy je kód datové schránky
- V komunikaci se státní správou lze použít ke stejnému účelu jako elektronický podpis
- Zřízení a komunikace se státní správou **zdarma**
- Není omezena platnost jako u certifikátů
- Uchovává dokumenty pouze 90 dnů
- Komunikace mimo orgány státní moci je zpoplatněna
- Zřízení na poště, jednoduchý formulář a OP nebo přes NIA identitu
 - Fyzická osoba
 - Fyzická osoba – podnikatel
 - Právnícká osoba



Základní registry

- ROB – registr obyvatel
 - Propojené s evidencí obyvatel a cizinců
 - Omezený přístup
- ROS – registr osob (podnikatelských)
- RUIAN – Registr územní identifikace, adres a nemovitostí

- Agendy státní správy
 - Rodné číslo x AIFO (agendový identifikátor fyzické osoby)
 - Různá identifikace občana v různých agendách



Elektronický občanský průkaz

- Vydávaný od 1.7. 2018
- Kontaktní technologie
- Umožňuje přihlášení k elektronickým službám státu
- Nutná aktivace na úřadu
- Umožňuje nahrát podpisový certifikát
- Potřebujete čtečku karet (v notebooku či externí)
- Přístupové kódy (PIN)
 - BOK, IOK, DOK, PIN, PUK, QPIN

eDoklady

- Mobilní aplikace
- Nutná registrace přes NIA prostředek
- <https://edoklady.gov.cz/>
- Ověřování probíhá přes Bluetooth. V rámci předání je přenášena i fotografie. QR kód slouží pouze pro navázání kontaktu, veškerá další komunikace probíhá přes Bluetooth. Ověřovatel posílá žádost ověřovanému, ten posílá odpověď s údaji (nebo žádost zamítá)

Portál občana

- <https://obcan.portal.gov.cz>
- Přihlášení přes NIA (např. eOP) nebo datovou schránku
- Postupný náběh služeb
- Přehled dokladů
- e-Receipt
- Sdílená zdravotnická dokumentace
 - NIX-ZD (Vysočina)