FILOZOFICKÁ FAKULTA
Masarykova univerzita

E-podpis, datové schránky, otevřená data

UNIVERSITAS MASARYKIANA BRUNENSIS
FACULTAS PHILOSOPHICA

Od ISVS k základním registrům

- IS VS nespolupracují, duplikované informace
- Zaznamenané e-informace pro VS musí být správné, aktuální, úplné, spolehlivě vedené, a tedy věrohodné
- Proto vytvořeny, zabezpečeny a celou VS společně využívány informace v registrech VS – referenční datové zdroje
- Jeden z klíčových plánovaných (2006) registrů hospodářský zahrnující všechny související, např. živnostenský, obchodní, registr ekonomických subjektů ČSÚ a další menší
- Zákon č. 111/2009 Sb., o základních registrech
- Plán přípravy nedodržen, spuštění až 1. 7. 2012

Systém základních registrů

- ROB (registr obyvatel) – o občanech a cizincích s povolením k pobytu
- ROS (registr osob) – o PO, podnikajících FO, OVM i nekomerčních subjektech (OS, církve…)
- RUIAN (registr územní identifikace, adres a nemovitostí)
- RPP (registr práv a povinností) – referenční o působnosti OVM, mj. oprávnění, informace o změnách v údajích ap.
- IS ZR (informační systém základních registrů) – rámec pro fungování 4 ZR
- ORG – převodník
- Správa základních registrů (úřad pro provazby)

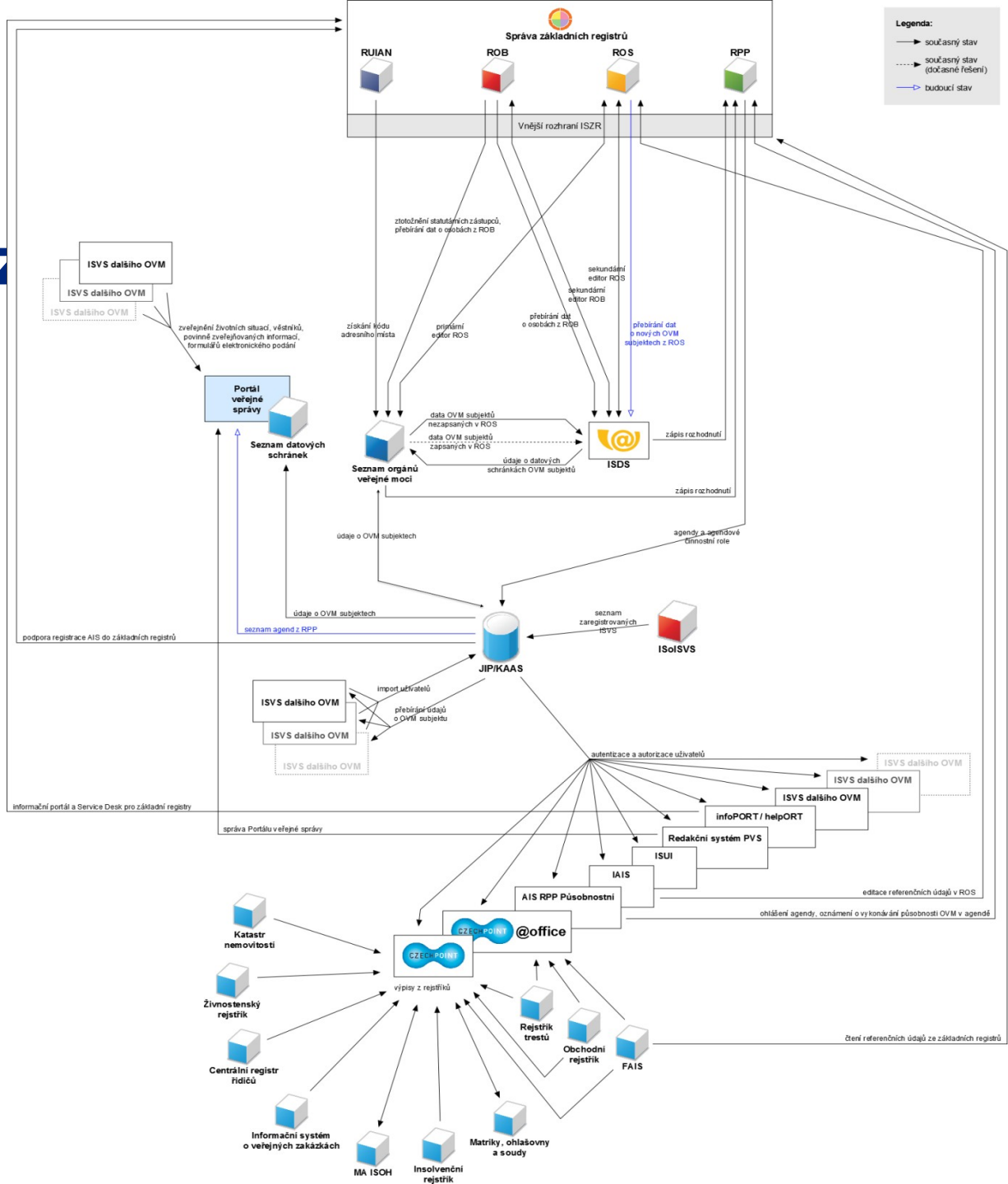
Definice IS ZR

- IS ZR = referenční rozhraní
- Komplexní služby definované v katalogu eGON služeb, pro všechny subjekty s ohledem na oprávnění
- Publikuje služby ZR
- Ověřuje oprávnění pro přístup
- Zaznamenává a ukládá všechny logy
- Rozhraní na technologii KIVS
- Určeno pro VS

FILOZOFICKÁ FAKULTA
Masarykova univerzita

Co z toho vylez

- Kmenové projekty eGovernmentu a jejich vazby (Strategický rámec rozvoje eGovernmentu 2014+)



FILOZOFICKÁ FAKULTA
Masarykova univerzita

Podpora otevřeného přístupu k informacím VS

- Koncepce katalogizace otevřených dat VS ČR + Metodika publikace otevřených dat veřejné správy ČR
- Sada doporučení vázaná na akční plán EU přenesený do ČR 2012 (+ plán na 3-5 let, zpožděný)
- Projekt Implementace strategií v oblasti otevřených dat veřejné správy ČR 1. 2. 2015 – 30. 11. 2015
- Idea ekonomického pozitiva dat ze SS (až 40 miliard Eur ročně)
- Doklad realizace politiky a nakládání s veřejnými prostředky (mj. proti korupci a posílení aktivního občanství)
- Dána základní a navazující úroveň
- Problém s geodaty (INSPIRE)
- Nutné legislativní změny (hl. z. o SPI), aby bylo povinné + forma k harmonizaci

Otevřená data dle MV ČR

- Datové sady zveřejněné na internetu:
  - úplná,
  - snadno dostupná + strojově čitelná při vynaložení minima možných nákladů,
  - používající standardy s volně dostupnou specifikací,
  - zpřístupněna za jasných podmínek užití s minimem omezení
- Požadavky na užití (viz CC):
  - neomezují ve způsobu použití,
  - opravňují k dalšímu šíření,
  - musí být uveden autor dat (i při dalším šíření),
  - při dalším šíření ostatní stejná oprávnění s daty nakládat

Charakteristiky otevřených dat (v souladu s Open Knowledge Foundation stanovila Sunlight Foundation)

- úplnost: maximální možný rozsah, lze dát zákonem
- primární: zveřejněna původcem, např. referenční údaje ze ZR, data z IS VS, agregovaná data, kde nelze primární (např. výsledky voleb) nebo statistiky nad primárními (na ně odkaz)
- zveřejnění bez odkladu, stálá dostupnost při vynaložení minima nákladů pro získání
- snadná dostupnost, strojová čitelnost, otevřené standardy (=> libovolné využití)
- zpřístupnění za jasných podmínek s minimem omezení, neomezující přístup (diskriminace)

Přínosy katalogu otevřených dat VS

- Usnadnění přístupu k datům veřejné správy => využitelnost, centrální místo, ale ne výhradní, informace o lokaci a postupu získání dat
- Vytvoření předpokladu pro snazší opětovné použití dat veřejné správy => nejen G2C a G2B, ale i G2G
- Vytvoření předpokladu pro využívání otevřených propojitelných dat (linked data) => z různých zdrojů, vč. vazby na vlastní pro hledání skrytých souvislostí, poskytovatel zveřejní primární data a propojení na sekundární (ne jejich správa) nutné otevřené standardy (W3C)
- Vytvoření předpokladu pro dosažení vyšší transparentnosti veřejné správy

Role pro Datový katalog

- správce DK: MV ČR
- provozovatel DK: zajištění chodu a údržby, SW/HW a bezpečnost
- poskytovatel dat: jakýkoli orgán VS s kompetencí či povinností zveřejňovat, příp. správce IS VS, rozhoduje o podmínkách zveřejnění a pověřuje kurátora správou dat
- kurátor dat: osoba zajišťující zveřejnění a údržbu záznamů, vč. klasifikace a vazby na ISDP a IS o ISVS
- redaktor: obsahová kontrola záznamů (ověření korektnosti záznamu ve všech polích), komunikace s poskytovateli dat a označení záznamu pro zveřejnění, v působnosti MV ČR
- koncový uživatel: vyhledává záznamy a dává podněty správci k novým či revizi, lze i bez registrace a zdarma

Postup katalogizace

- Rozhodnutí, zda data určená veřejnosti => forma zveřejnění (formát, přístup k datům, zajištění aktuálnosti)
- Export do formátu (doporučeno na XML/RDF) a publikace dat (snadná nalezitelnost, např. odkaz z homepage) => vyplnění povinných atributů záznamu
- Provázání s ISDP a IS o ISVS
- Manuální katalogizace a redakce záznamů (jen část automatizovaně podpořena)
  - katalogizace v ČJ a AJ (evropský DK – Publicdata.eu)
  - část údajů kurátor, část redaktor
  - plánování využití EUROVOC (oblasti/obory činnosti) a CZ-NACE (ekonomické činnosti)

Typy dat a formátů

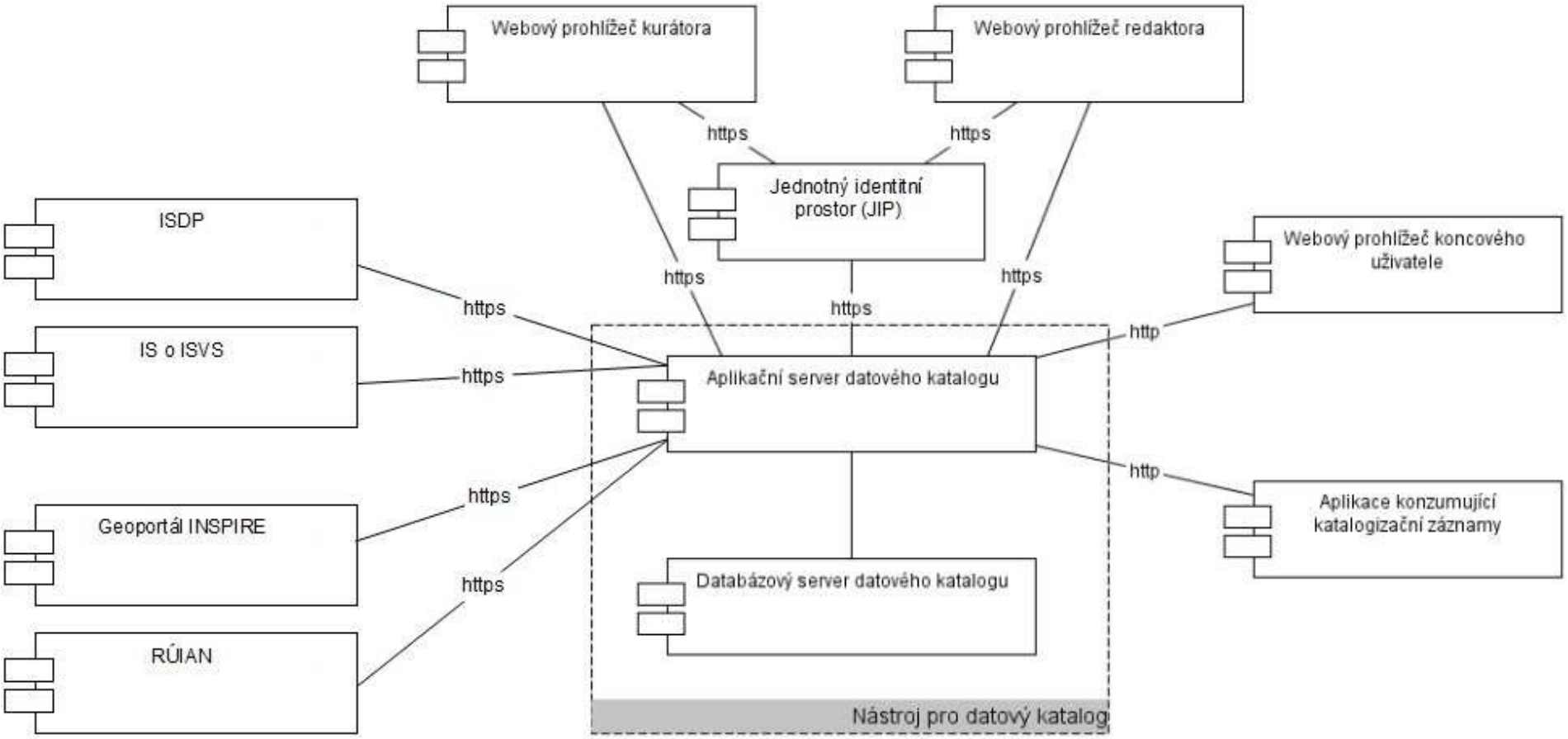
- Nejdříve data povinně zveřejněná dle zákonů a statistická, z výkazů a přehledů, z rejstříků (pokud veřejná), prostorová
- Vhodné vyjít ze statistik návštěvnosti a žádostí dle 106 (o co zájem)
- Nutná právní analýza, co a jak lze zveřejnit => primární, anonymizovaná, agregovaná => stanovení licencí (příklady), ty nutné zveřejnit s daty
- Licence ideálně pro libovolné využití, ne/komerční, spojitelná, transformovatelná, zahrnutá do vlastních databází...
- Preferovaný XML/RDF formát, otevřený (volně dostupná specifikace) pro možnost tvorby vlastních aplikací, až při nenalezení vhodného formátu lze vytvořit vlastní
- V metodice popsány ne/vhodné formáty a možnosti jejich použití

Kvalita a bezpečnost DK

- Kvalitativní ukazatele: unikátnost záznamů, úplnost DK, relevance záznamu, správnost a úplnost, platnost odkazu na data, shoda vyplněných a odkazovaných dat, správnost klasifikace
- Pro kontrolu kvality zapojeni uživatelé (zpětná vazba, ne úpravy) + strojové učení
- Bezpečnost technická + organizační (vyškolení)
- Bezpečnostní politika vytvořená při implementaci, podstatná přesnost a aktuálnost pro kvalitu a důvěryhodnost + zajištění integrity a dostupnosti obsahu (obnovení do stavu max. 1 hod. před událostí, možnost určení původce změn)
- Jednotný identitní prostor (JIP) pro jednoznačnou autentizace uživatelů IS VS, před zavedením lze využít kvalifikované certifikáty (každý pracovník VS oprávněný jako kurátor)

FILOZOFICKÁ FAKULTA
Masarykova univerzita

Softwarová architektura nástroje pro katalogizaci dat



Linked (open) data

- Konkrétní i abstraktní objekty reálného světa přidělena neměnná URI (jednoznačné identifikátory)
- Striktní dodržování HTTP URI, při přístupu strojově čitelný formát RDF pro data s propojením na jiné objekty (souvislosti)
- Přispět spojením může kdokoli, v tvrzeních lze vyhledávat jako dnes v dokumentech, ale přesněji
- Datový model RDF = graf, kde uzly = objekty (URI) a údaje (texty, čísla...), hrany = propojení
- Typy hran definovány v slovníku (ontologii) – struktura dat a sémantika

Čísla předpokládané realizace

- 7301 OVM různého počtu záznamů, do malé (řádově jednotky záznamů) patří i větší části obce, MŠ, ZŠ, SŠ a profesní komory
- Průměrná doba:
  - Vytvoření záznamu kurátorem, vč. oprav 90 min.
  - Redakce 1 záznamu, vč. oprav 30 min.
- Kurátor/redaktor cca 25 tis. Kč, vč. osobního ohodnocení, tj. 34 550 Kč měsíčně hrubého

Zajímavé odkazy

- Národní katalog otevřených dat + Registr smluv
- EU projekt COMSODE pro platformu a metodiky open data
- Fórum expertů Otevrenadata.cz
- Iniciativa OpenData.cz (neaktualizována)
- Soutěže: Hackathon a
  Soutěž o nejlepší aplikaci nad otevřenými daty

Zdroje

- Koncepce katalogizace otevřených dat VS ČR
- Metodika publikace otevřených dat veřejné správy ČR
- Otevřená data. MV ČR [online]. 22. 6. 2015 [cit. 2015-10-29]. Dostupné z: http://www.mvcr.cz/clanek/otevrena-data.aspx
- PETERKA, Jiří. Kolik budou stát základní registry? Lupa [online]. 25. 7. 2011 [cit. 2014-9-06]. ISSN 1213-0702. Dostupné z: http://www.lupa.cz/clanky/kolik-budou-stat-zakladni-registry/
- REICHL, Jiří. Schválen návrh novely zákona o základních registrech a novely krizového zákona. Ministerstvo vnitra České republiky. [online]. 2010 [cit. 2014-09-26]. Dostupné z: http://www.mvcr.cz/clanek/schvalen-navrh-novely-zakona-o-zakladnich-registrech-a-novely-krizoveho-zakona.aspx
- ŠPAČEK, David. *EGovernment: cíle, trendy a přístupy k jeho hodnocení*. Vyd. 1. V Praze: C.H. Beck, 2012, xix, 258 s. Beckova edice ekonomie. ISBN 978-807-4002-618.
- Testovací prostředí. Datové schránky [online]. © 2011 [cit. 2014-10-1]. Dostupné z: http://www.datoveschranky.info/cz/o-datovych-schrankach/testovaci-prostredi-id34697/
- Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů
- Zákon č. 300/2008 o e-úkonech, osobních číslech a autorizované konverzi dokumentů, ve znění pozdějších předpisů

Elektronický podpis

- Zaveden v ČR zákonem v r. 2000, krom e-podpisu novelizace mnoha správních předpisů, zákoníků atd. pro dosažení rovnoprávnosti tradičního a e-prostředí
- K 19. 9. 2016 nahrazen zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce <= eIDAS - Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
- Klíčový předpoklad pro datové schránky
- Usnadnění komunikace mezi VS a občanem (volba)
- Výhledově snížení nákladů na chod VS
- Předpokládá se, že odesilatel před podpisem zprávu četl

Účely e-podpisu

- Zrovnoprávnění e-komunikace s tradiční (listinnou)
- Zajištění důvěryhodnosti konání v e-prostředí
- Zajištění jednoznačné identifikace odesilatele
- Zajištění závaznosti a vymahatelnosti konání v e-prostředí
- Šifrování zprávy proti
  - Čtení neoprávněnou osobou
  - Změně zprávy neoprávněnou osobou

Definice podpisů

- Kvalifikovaný e-podpis – veřejnoprávní podepisující nebo výkon působnosti
- Uznávaný e-podpis vůči veřejnoprávnímu
- Elektronická pečeť pro potvrzení bez požadavku podpisu (dříve e-značka)
- Kvalifikované elektronické časové razítko

Definice – certifikování

- Certifikát
  - Umožňuje ověřovat identitu odesílatele
  - Prostředek pro vytváření e-podpisů
- CA = poskytovatel certifikačních služeb, musí vést seznam zneplatněných certifikátů (verifikace), akreditovaní:
  - První certifikační autorita od 15.3. 2002
  - Česká pošta od 15.7. 2005
  - eldentity od 12.9. 2005
- Pravidlo vzájemného uznávání certifikátů v rámci EU (na stejné úrovni a se stejnou působností)

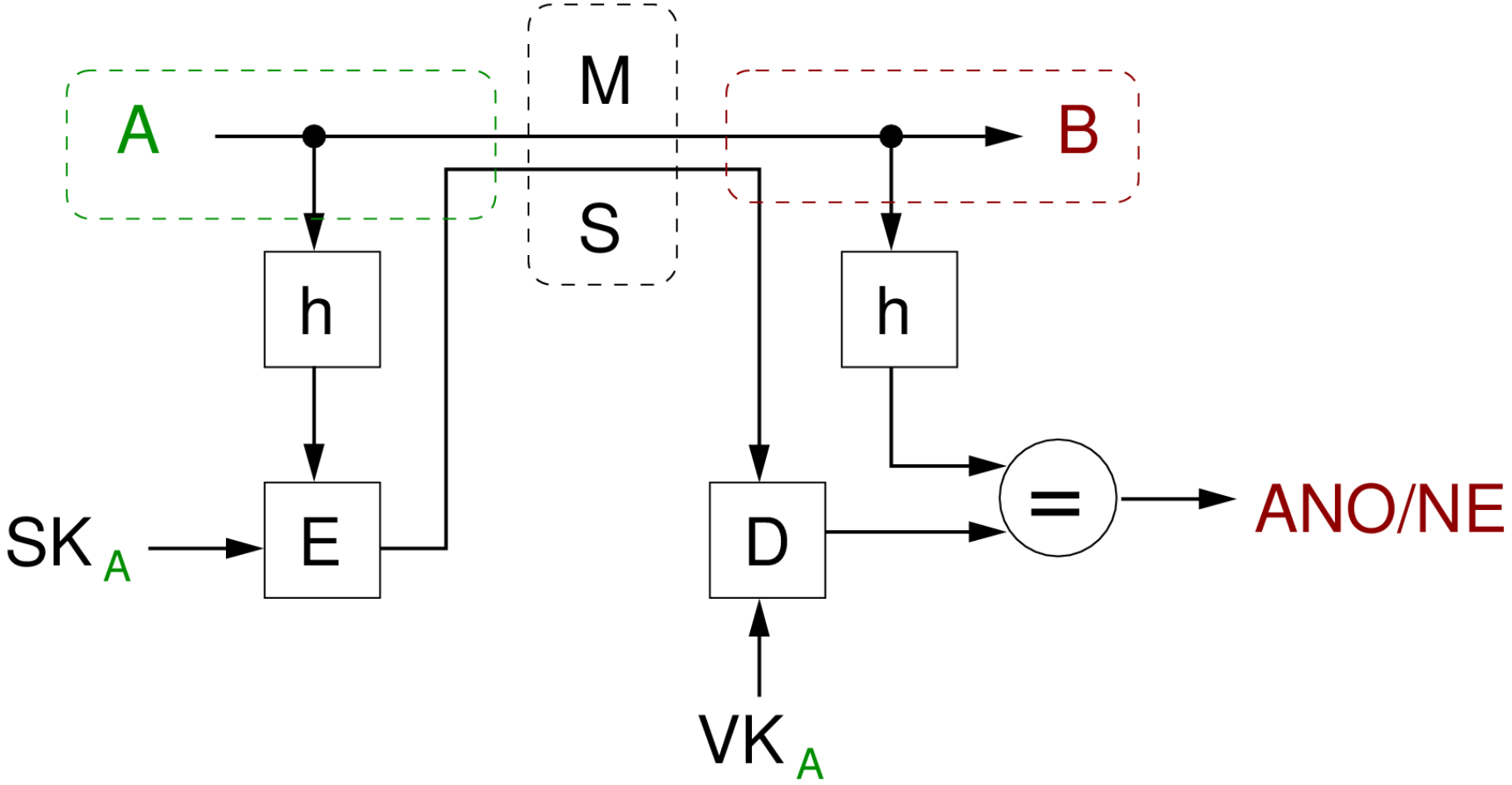
Asymetrická šifra

- Dvojice klíčů: privátní a veřejný
- CA: generuje klíče pomocí SW, spolehlivé zpřístupnění veřejného klíče
- Privátní klíč
  - majitel povinen chránit a předcházet zneužití,
  - při (podezření na) zneužití povinnost hlásit CA
- Certifikát:

Obsah certifikátu veřejného klíče	
Položka	**Popis**
ID certifikátu	Jednoznačné sériové číslo
Datum vydání	Kdy byl certifikát vydán
Platnost do	Časové omezení platnosti
Omezení certifikátu	Účel, pro který lze certifikát použít (např. podepisování)
ID certifikační autority	Kdo certifikát vydal
Algoritmy CA	Jaké algoritmy používá pro podepisování certifikační autorita
Veřejný klíč CA	Nemusí být součástí certifikátu
ID vlastníka	Rodné číslo či IČO
Veřejný klíč vlastníka	Vlastní certifikovaný klíč
Podpis	Předchozí data jsou podepsána soukromým klíčem CA

Tabulka 5.1: Obsah certifikátu

Digitální podpis

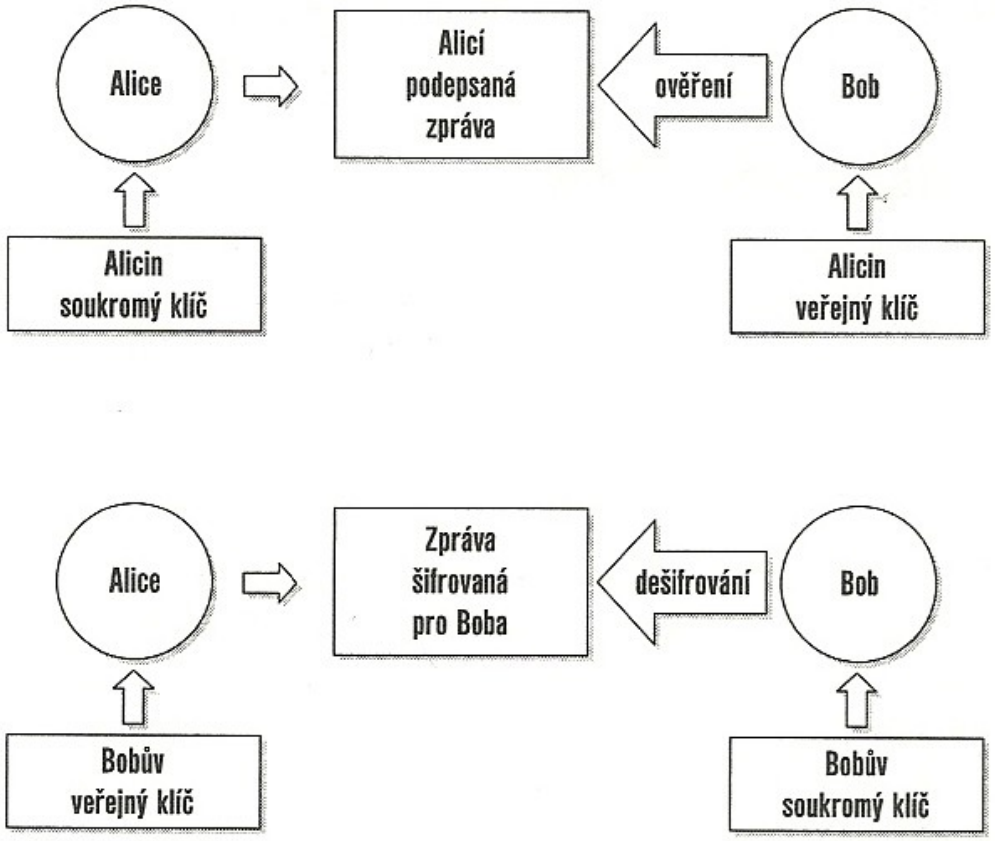


Proces vytváření podepsané a důvěrné zprávy

- Hash funkce (komprimace a vytvoření otisku/snímku zprávy)
- Aplikace privátního klíče odesilatele + veřejného klíče adresáta (zašifrování)
- Zpráva s e-podpisem
- Odeslání
- Příjem adresátem
- Aplikace privátního klíče adresáta + veřejného klíče odesílatele (užití hash funkce s pomocí veřejného klíče + porovnání => mezi výsledky hash fce na začátku a na konci nesmí být rozdíl)

- => verifikace (podpisu) a verifikace neporušení při přenosu

Digitální podpis a šifrování



Obrázek 2.10: Šifrování versus podepisování

Jak vypadá e-podpis?

- Elektronicky podepsaný dokument

Úkol

- Poslat mi e-mail s e-podpisem (testovací) na kovarova@phil.muni.cz
  - Podepsaný e-mail, ne podepsaný dokument!
- Podívat se, jak vypadá e-podpis v odpovědi a pokusit se ověřit jeho pravost (není nutné už komentovat, jen si to zkusit)

Co si pamatujete o zákonu o elektronickém podpisu?

- Volné psaní + metoda kostka:
  - **Popiš:** Podívej se zblízka a popiš (1,5 min.)
  - **Porovnej:** Čemu se podobá, od čeho se liší (2 min.)
  - **Asociuj:** Nač si vzpomeneš, co ti připomíná (3 min.)
  - **Analyzuj:** Z čeho se skládá, jak je to udělané (3,5 min.)
  - **Aplikuj:** K čemu se to hodí, jak to můžeme použít (3 min.)
  - **Argumentuj:** Zaujmi stanovisko pro/proti (můžeš použít jakékoli argumenty – logické i pošetilé) (2 min.)
- Sdílejte 2-3, pak dáme dohromady zdařilé

Otázky

- Jaké jsou funkce e-podpisu?
- Kdo může číst elektronicky podepsanou zprávu? A důvěrnou?
- Co to je: e-podpis, certifikát, certifikační autorita, časové razítko, pečeť?
- Když je dokument elektronicky podepsaný, může držitel podpisu tvrdit, že ho nečetl?
- Vyjmenujte české akreditované CA.
- Na jakém typu šifrování je založen princip e-podpisu?
- Co to je hash?
- Kdo zajišťuje utajení soukromého klíče?

ISDS

- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů (účinnost od 1.7. 2009), vyhlášky, provozní řád
- ISDS + výukové prostředí, rozhraní DS
- ISDS ke komunikaci mezi VS a PO v obchodním rejstříku (povinně), VS a podnikajícími FO (volitelně), VS a FO (volitelně) a orgány VS navzájem (povinně); od 1. 1. 2010 i mezi PO, podnikajícími FO a FO navzájem (volitelně – nutné povolit, pak dohledatelná adresa každým)
- Volitelné subjekty o zřízení žádají (zdarma), povinné zřízeno automaticky a bezodkladně
- Provozovatelem ISDS držitel poštovní licence => záznam jen o „obálce“, ne obsahu
- ISDS „je systém rychlý (datová zpráva je doručena prakticky okamžitě), spolehlivý (datová zpráva se nemůže ztratit), auditovatelný (je jednoduše dokazatelné, kdo datovou zprávu podal a komu byla doručena).” (ISDS: základní informace)

Datová schránka

- „ Datová schránka je elektronické úložiště, které je určeno k
  a) doručování orgány veřejné moci,
  b) provádění úkonů vůči orgánům veřejné moci,
  c) dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob.“ (§ 2)
- Datová zpráva = „doporučený dopis”

Doručení zprávy do datové schránky

- „Umožňuje-li to povaha dokumentu, orgán veřejné moci jej doručuje jinému orgánu veřejné moci prostřednictvím datové schránky, pokud se nedoručuje na místě.“, podobně pro PO/podnikající FO/FO, pokud zřízena DS (§ 17, odst. 1) => pro vše, co lze konvertovat do e-podoby
- Zpráva technicky zkontrolována, zašifrována, přidána systémová data (časová razítka) a „přijata k přepravě“
- Zprávy považovány za doručené při přihlášení do datové schránky (ne zobrazení zprávy), příp. (až na výjimky) po uplynutí desetidenní lhůty od dodání do datové schránky (tzv. doručení fikcí)
- Po přijmutí doplněna systémová data (odesilatel může vyžádat)

Bezpečnost datových schránek

- Nezbytná (využití pro komunikaci VS, zákon, důvěra občanů…)
- Stanovena bezpečnostní pravidla/doporučení:
  - Ke vstupu nutné přihlašovací jméno a heslo (stanovena pravidla podoby), doporučeno rozšířit certifikátem (e-podpis)
  - Aktualizace OS a bezpečnostního SW
  - K DS přistupovat obezřetně jako k internetovému bankovnictví
  - Kvalitní antivirová ochrana a obousměrný osobní firewall
  - Nepracovat na internetu pod účtem administrátora
  - Zálohovat důležitá data
  - Používat bezpečné bezdrátové připojení
  - Nedůvěřovat neověřeným zprávám (možný podvod)
  - Instalace a užívání pouze legálního SW z prověřených zdrojů
- Oprávněná osoba povinna zacházet s přístupovými údaji k DS tak, aby nemohlo dojít k jejich zneužití (§ 9, odst. 2)

Otázky

- Uveďte, mezi kterými subjekty je povinná komunikace pomocí DS.
- Uveďte, mezi kterými subjekty je volitelná komunikace pomocí DS.
- Kdy je datová zpráva doručena?
- Mohou být využívány datové schránky bez e-podpisu? A e-podpis bez datové schránky?

Zdroje

- DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. 190 s. ISBN 8025101061.
- Druhy elektronických podpisů
- Informační systém datových schránek: základní informace
- ŠTĚDROŇ, Bohumír. Úvod do eGovernmentu: Právní a technický průvodce. 1. vyd. Praha: Úřad vlády České republiky, 2007. 172 s. ISBN 978-80-87041-25-3.
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, v platném znění
- Zákon č. 227/2000 Sb., o elektronickém podpisu, v platném znění
- Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění zákona č.226/2002 Sb. (komentář)
- Zákon o elektronickém podpisu (ppt presentace)

FILOZOFICKÁ
FAKULTA
Masarykova univerzita

Děkuji za pozornost.

UNIVERSITAS MASARYKIANA BRUNENSIS
FACULTAS PHILOSOPHICA