MASARYKOVA UNIVERZITA

E-podpis a datové schránky
E-zdravotnictví, e-archivnictví

13.11. 2015

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

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 (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 (volitelné – 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)

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
- 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
- Pro VS nutný akreditovaný, pak podepsaná zpráva rovnoprávná s listinnou

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

- E-podpis = „údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě“ (§ 2)
- Zaručený e-podpis: jednoznačně pro člověka, prostředky vzniku jen v jeho moci, možné zjištění pozdější změny zprávy
- E-značka jako zaručený e-podpis pro jiné než FO

Definice - certifikování

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

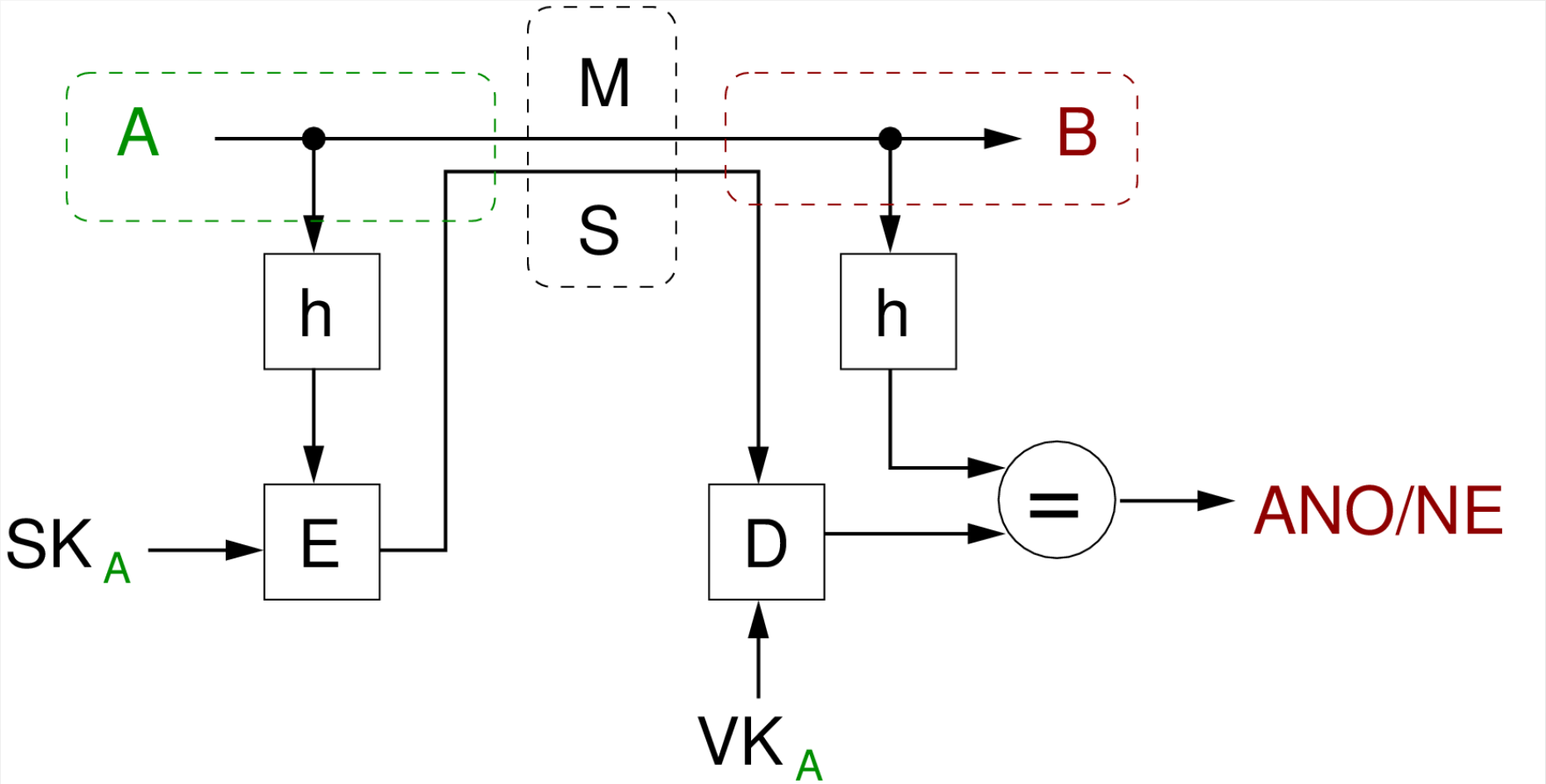
Asymetrická šifra

- Dvojice klíčů: privátní a veřejný
- CA: generuje klíče pomocí SW, spolehlivé zpřístupnění veřejného klíče
- Privátní klíč => osoba, které náleží, je povinna ho chránit a předcházet zneužití, při (podezření na) zneužití povinnost hlásit poskytovateli certifikačních služeb
- 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

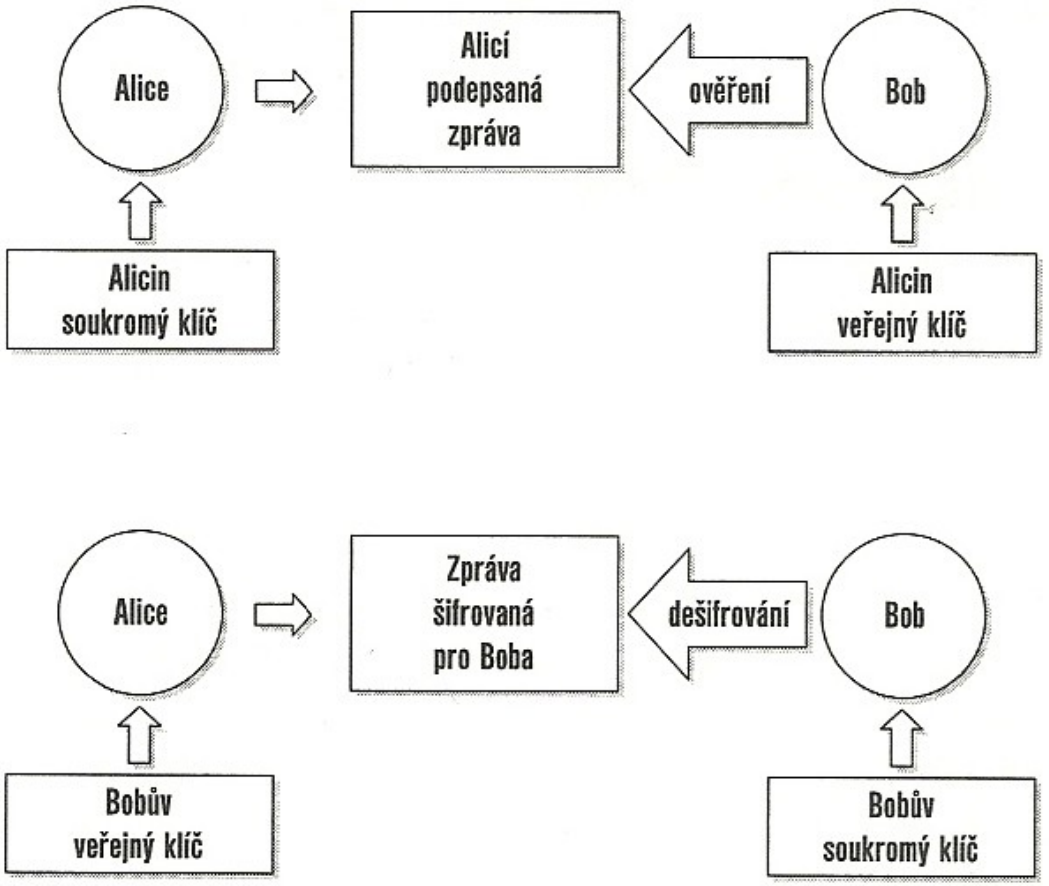


Proces vytváření podepsané a důvěrné zprávy

- 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 funkce 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 č. 7

- 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

- 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?
- Jaké jsou funkce e-podpisu?
- Kdo může číst elektronicky podepsanou zprávu? A důvěrnou?
- Co to je: e-podpis, certifikát, kvalifikovaný certifikát, certifikační autorita, časové razítko, e-značka?
- 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?

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)

MASARYKOVA UNIVERZITA

E-zdravotnictví, e-archivnictví

e-Zdravotnictví

- Lepší a efektivnější zdravotní péče
- Propojení a spolupráce zdravotnických zařízení:
  - Koordinace aktivit při ohrožení zdraví obyvatel,
  - Sdílení dat mezi zdravotnickými organizacemi
  - Místo průkazů pojištěnců čipové karty
- Prevence: informace o zdravém životním stylu (Systém poskytování veřejných zdravotnických informací), telekonzultace

E-zdravotnictví - regulace

- Z. č. 20/1966 Sb. o péči o zdraví lidu (od 1990 víc než 50x novelizován) nahrazen z. č. 372/2011 o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)
- Ukotveno dobrovolné hodnocení zdravotnické oblasti + dány podmínky (§§ 98-106)
- Pro IP klíčové:
  - Informování pacienta (komunikace)
  - Zdravotnická dokumentace (informace o pacientovi)
  - Zdravotnické IS (elektronizace zdravotnictví)

§ 28 poučení nemocného o zákrocích a jeho souhlas

- Nutný svobodný a informovaný souhlas pacienta
- Pacient má právo na:
  - Konzultace s jiným zdravotníkem (mimo neodkladnou péči, vazbu, výkon trestu apod.)
  - Seznámení s vnitřním řádem instituce
  - Informaci o ceně za služby
  - Informace o zúčastněných pracovnících

§ 31-32 Povinnosti poskytovatele péče informovat pacienta

- Zdravotní stav (bezodkladně, srozumitelně a v dostatečném rozsahu, vyjmenovány), léčebný postup a změny
- Možnost vzdát se práva na informace, příp. zakázat či dovolit informování osob
- Pozůstalí právo na informace o zemřelém, pokud nezakázal
- Výjimka vždy, když je to může ohrozit

§ 52-55 zdravotnická dokumentace

- Možnost práce s rodným číslem
- Vždy nutné datum zápisu a identifikace pracovníka
- Listinná i e-, při digitalizaci listinná uchována
- Nelze nic mazat – i při změně nutná čitelná původní verze
- Pro e-ZD nutné zajistit:
  - Ochrana proti změně i nečitelnosti (LTP)
  - Identifikátory pracovníků
  - Autorizace

§ 65-66 přístup k ZD

- Do ZD o pacientovi mohou za přítomnosti pověřeného zaměstnance nahlížet a pořizovat výpisy či kopie: pacient, zákonný zástupce, pacientem určené osoby, pozůstalí (když nezakázáno)
- Nahlížet + kopie zaměstnanci (nebo kontrolující) pro výkon povolání
- Při čistě e-ZD může oprávněný nahlížet i dálkově a tvořit kopie
- Většina nahlížení dokumentována

§ 70-78 NZIS

- Jednotný systém pro:
  - Údaje o zdraví obyvatel, pracovnících, službách…
  - Vedení registrů
  - Pro VaV a statistiky
- OÚ bez souhlasu subjektů, zákon je jmenuje (mnoho), správce (Ministerstvo) na žádost poskytuje oprávněným
- Zdroje:
  - Národní zdravotnický IS provozován Ústavem zdravotnických informací a statistiky
  - Národní referenční centrum (od 1.1.2016 Kancelář zdravotního pojištění, z.s.)

E-zdravotnictví mimo stát

- Datové rozhraní komunikací zdravotních IS a centrálních referenčních zdravotních záznamů
- Klasifikační systémy a e-Health Technology Assessment
- Elektronizace pre/postgraduálního vzdělávání
- Systémy podpory klinického rozhodování, standardy, klinické protokoly
- Telemedicína
- …

Telemedicína

- „zdravotnická informace je přenášena prostřednictvím telefonu, Internetu nebo jiných sítí za účelem konzultace a někdy dálkových medicínských výkonů nebo vyšetření“
  - Telekonzultace pro diagnostické, terapeutické a edukační účely
  - Telemonitoring - domácí zdravotní péče (pooperační a pro starší generaci)
  - Jak vypadá telemedicína? (do 1:15, 2:54-6:30)

MASARYKOVA UNIVERZITA

E-archivnictví

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Archivnictví

- Z. č. 499/2004 Sb., dozorčí orgán MV
- V analogové i digitální podobě
- S rozvojem e- otázky LTP (long term preservation), zajištěním čitelnosti, apod. => nutné úpravy z. a nalezení řešení problémů
- Klíčová autenticita (e-podpis) – každou změnou (nejen obsahovou) mizí + možnost prolomení šifrování
- Problém s datovou náročností (audio-vizuální dok.)
- Co po nás zbude

Zákon č. 499/2004 Sb.

- Rozlišuje dokument a archiválii
- „záznam, který byl vzhledem k době vzniku, obsahu, původu, vnějším znakům a trvalé hodnotě dané politickým, hospodářským, právním, historickým, kulturním, vědeckým nebo informačním významem vybrán [archivem] ve veřejném zájmu k trvalému uchování a byl vzat do evidence archiválií; (…) i pečetidla, razítka a jiné hmotné předměty“
- Uchovávat dokumenty a umožnit výběr archiválií musí veřejno- i soukromoprávní původci

Zákon č. 499/2004 Sb. (2)

- Vývoz mimo ČR jen se souhlasem MV, vždy jen na dobu určitou a z důvodu: vystavování, konzervování, restaurování, vědecké zkoumání
- Lze nahlížet jen na základě žádosti
  - Obsahující OÚ jen se souhlasem subjektu
  - Přístupné pouze starší 30 let
  - Výjimky vzniklé z činnosti st. orgánů před 1990

Soustava archivů

- Veřejné archivy
  - Národní archiv
  - Archiv bezpečnostních složek
  - Státní oblastní archivy
    - Státní oblastní archiv v Praze
    - Státní oblastní archiv v Třeboni
    - Státní oblastní archiv v Plzni
    - Státní oblastní archiv v Litoměřicích
    - Státní oblastní archiv v Zámrsku
    - Moravský zemský archiv v Brně
    - Zemský archiv v Opavě
  - Specializované archivy
  - Bezpečnostní archivy
  - Archivy územních samosprávných celků
- Soukromé archivy (zřizují FO/PO)

Spisová služba

- „zajištění odborné správy dokumentů došlých a vzešlých z činnosti původce (…) zahrnující jejich řádný příjem, evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování ve skartačním řízení, a to včetně kontroly těchto činností“
- Státní orgány (mnoho, jmenováno v zákoně) povinně
- Možná e- (preferovaná) i listinná
- Dok. označeny jednoznačným identifikátorem a evidovány
- Všechny k téže věci spojeny ve spis
- Jmenný rejstřík pro vyhledávání, ověřování a automatické zpracovávání údajů o adresách odesílatelů a adresátech dok. (údaje pro jednoznačnou identifikaci)
- Požadavek na e-podpis/e-značku/kvalifikované časové razítko

E-archivnictví

- 2012 přidáno: „ V případě dokumentů v digitální podobě se jejich uchováváním rozumí rovněž zajištění věrohodnosti původu dokumentů, neporušitelnosti jejich obsahu a čitelnosti, tvorba a správa metadat náležejících k těmto dokumentům v souladu s tímto zákonem a připojení údajů prokazujících existenci dokumentu v čase. Tyto vlastnosti musí být zachovány do doby provedení výběru archiválií.“ (§ 3)
- Týká se born digital i digitalizovaných dokumentů
- I u e-archivnictví jde o relevanci, selekci a stanovení skartačních znaků, ale selekce náročnější

Problémy e-archivace

- Dlouhodobá = nekončící finanční i časové náklady
- Problémy = daň za krátkou trvanlivost e-nosičů a příliš rychlý vývoj ICT
- E-prostředí = nové pole pro komerční sféru (vývoj IS, zabezpečení, BOJ O STANDARDY)
- Muzeum HW pro uchování dat nesmysl
- Média podobné => nutné řešit migrací na média novější
- Na HW závislý OS a na něm aplikace => nejsložitější

Principy e-archivace

- Emulace: archivace původního SW, stále nutné migrovat data na nová média
- Migrace: průvodním jevem zajištění uchování a využívání e-dokumentů bez původního SW
- Virtualizace: prvky migrace i emulace pro vybrané datové formáty (JPEG, PDF); vytvoření interpretační struktury

Národní digitální archiv versus Národní digitální knihovna?

- Není důvod konkurovat:
  - Rozdílná úloha (jiná „sběrná oblast“)
  - Důraz na jiné problémy dlouhodobého ukládání
  - Rozdílná metadata

Archiv	Knihovna
Ochrana dat	Ochrana dat
Bezpečnost	Zpřístupnění
Právní relevance	Autorskoprávní problematika
Přejímání od původce, výběr	Automatizované akvizice, všechno

Otázky

- Co řeší e-zdravotnictví?
- Můžu veřejně hodnotit kvalitu svých lékařů?
- Na jaké informace v oblasti zdravotnictví mám právo?
- Zjistí můj lékař vše o mém zdraví bez mého přispění?
- Můžu zjistit OÚ mého souseda, spolupracovníka STB, bez jeho souhlasu?
- Jaké problémy mohou nastat při e-archivaci?
- Co se stane s e-mailem a dopisem, který pošlu na obecní úřad?
- Když si budete chtít uchovat své e-dokumenty, co byste udělali? Když by chtěl dokumenty uchovat živnostenský úřad, musí něco dělat jinak?

Zdroje

- PAČES, Pavel. Archivace digitálních dokumentů. *Co po nás zbude* [online]. 2008 [cit. 2013-9-18]. Dostupné z: http://www.cnz.cz/ke-stazeni/2008/konference/prezentace/paces.pdf
- VÁLEK, Jiří. Elektronizace zdravotnictví (e-Health). Telekomunikace [online]. 6. 3. 2009. Dostupné z: http://www.zdrav.cz/modules.php?op=modload&name=News&file=article&sid=8963
- Zákon o archivnictví a spisové službě, v platném znění
- Zákon o zdravotních službách, v platném znění

MASARYKOVA UNIVERZITA

Děkuji za pozornost.