MASARYKOVA UNIVERZITA

Ochrana OÚ, e-podpis a datové schránky

15.11. 2013

Digitální agenda a OÚ

- „Evropané nepřijmou technologii, které nedůvěřují – při používání on-line nástrojů se musí se cítit bezpečně. V případech počítačových útoků je proto nutné lépe koordinovat odpověď na evropské úrovni a zpřísnit pravidla **ochrany osobních údajů**. Lze zvážit i opatření, jež by provozovatelům internetových stránek ukládala informovat uživatele o tom, že se bezpečnost jejich osobní údajů ocitla v ohrožení.“
- Bezpečnost vnímána i před DA jako klíčová pro přijetí e-služeb
- Komunikace s VS správou klíčová + VS mnoho informací o občanech – nutné zajistit bezpečí pro důvěru občanů

Zákon č. 101/2000 Sb., o ochraně osobních údajů

- Snaha o naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí
- Stanovení práv a povinností při zpracování OÚ
- Podmínky pro předání OÚ do jiných států
- Zpracování OÚ
  - státními orgány,
  - orgány územní samosprávy,
  - jinými OVM i FO/PO
- Veškeré zpracovávání OÚ, automatizovaně i jinak

Na co se zákon nevztahuje

- Zpracování OÚ fyzickou osobou výlučně pro osobní potřebu
- Nahodilé shromažďování OÚ, pokud nejsou dále zpracovávány
- Zpracování OÚ „nezbytných pro plnění povinností správce stanovených zvláštními zákony pro zajištění: bezpečnosti ČR; (…) předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů; významného hospodářského zájmu ČR nebo EU; (…) výkonu kontroly, dozoru, dohledu a regulace spojených s výkonem veřejné moci v předchozích uvedených případech; činností spojených se zpřístupňováním svazků bývalé Státní bezpečnosti“

Vymezení údajů (§ 4)

- „a) **osobním** údajem jakákoliv informace týkající se určeného nebo **určitelného** subjektu údajů (…),
- b) **citlivým** údajem **osobní** údaj **vypovídající o** národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj (…),
- c) **anonymním** údajem takový údaj, který buď v původním tvaru nebo po provedeném zpracování **nelze vztáhnout** k určenému nebo určitelnému subjektu údajů,(…)
- l) **zveřejněným** osobním údajem osobní údaj **zpřístupněný** zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu,“

Zpracování a shromažďování (§ 4)

- „e) **zpracováním** osobních údajů jakákoliv operace nebo soustava operací, které správce nebo zpracovatel **systematicky** provádějí s osobními údaji, a to **automatizovaně nebo jinými prostředky** (…),
- f) **shromažďováním** osobních údajů systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů **za účelem** jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější **zpracování**,“

Povinnosti správce údajů (§ 5, odst. 1)

- Stanovit **účel** zpracování
- Stanovit **prostředky a způsob** zpracování
- Zpracovat pouze **přesné** OÚ, aktualizace hned po zjištění, pokud nelze, nutné znepřístupnění či označení
- **Shromažďovat a zpracovávat** OÚ pouze ke stanovenému **účelu** a jen v **nezbytném rozsahu**
- **Uchovávat** OÚ pouze po nezbytnou dobu, pak jen pro státní statistické služby, účely vědecké a archivnictví a co nejdřív anonymizovat
- Shromažďovat OÚ pouze **otevřeně**
- **Nesdružovat** OÚ získané k rozdílným účelům
- Nutné myslet na **soukromí** subjektu údajů

Souhlas subjektu údajů

- Klíčový souhlas subjektu údajů = „svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů“ (§ 4, odst. n)
- Zpracování jen se souhlasem SÚ, bez něj jen z vymezených výjimečných důvodů
- SÚ musí být informován o tom, pro jaký účel zpracování a k jakým OÚ je souhlas dáván, jakému správci a na jaké období, zda je poskytnutí povinné či dobrovolné
- Souhlas musí být správce schopen prokázat po celou dobu zpracování
- Odvolání souhlasu nutné písemně

Pravidla zpracování údajů

- Citlivé údaje lze zpracovávat jen ze zákonem vymezených důvodů (striktnější než běžné OÚ)
- „Při zpracování osobních údajů správce a zpracovatel dbá, **aby subjekt údajů neutrpěl újmu na svých právech**, zejména na právu na zachování lidské důstojnosti, a také dbá na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.“ (§ 10)
- Na požádání subjektu správce povinen předat informaci o zpracování OÚ daného subjektu
- Před zahájením zpracování nutné informovat ÚOOÚ o zákonem daných souvislostech
- § 27 stanovuje podmínky předání OÚ do jiných států

Ochrana OÚ

- „(1) Správce a zpracovatel jsou povinni přijmout taková **opatření**, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému **zneužití osobních údajů**. Tato povinnost platí i po ukončení zpracování osobních údajů.
- (2) Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a **provedená technicko-organizační opatření** k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.“ (§ 13)
- § 15 povinnost mlčenlivosti o OÚ (i po skončení zpracování)

Úřad pro ochranu osobních údajů

- Zřízen § 2 zák. 101/2000 Sb.
- Dozorový úřad pro oblast ochrany OÚ vyplývající z mezinárodních smluv, které jsou součástí právního řádu
- § 28, odst. 1 „Úřad je **nezávislý** orgán. Ve své činnosti postupuje nezávisle a řídí se pouze zákony a jinými právními předpisy.“
- V čele předseda, on i inspektoři jmenováni presidentem

Činnosti ÚOOÚ (§ 29)

- Dozor nad dodržováním povinností při zpracování OÚ,
- Vede registr zpracování OÚ,
- Přijímá podněty a stížnosti na porušení povinností při zpracování OÚ a informuje o jejich vyřízení,
- Zpracovává a zveřejňuje výroční zprávu o své činnosti,
- Vykonává další působnosti stanovené mu zákonem (např. zajištění ORG – přiděleno až s odstupem – díky Emilovi Budínovi),
- Projednává přestupky a jiné správní delikty a uděluje pokuty,
- Zajišťuje plnění požadavků z mezinárodních smluv,
- Poskytuje konzultace v oblasti ochrany OÚ,
- Spolupracuje s obdobnými úřady jiných států

Další zdroje k tématu

- Občanský zákoník (ochrana soukromí, osobnosti apod.) – účinné i platné znění
- Trestní zákoník, § 180 Neoprávněné nakládání s osobními údaji – zneužití či umožnění zneužití OÚ, ke kterým měli přístup díky svému povolání, zaměstnání nebo funkci; umožňuje postih i při nedbalosti
- Iuridicum Remedium + Big Brother Awards

MASARYKOVA UNIVERZITA

Datové schránky

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 má zřízenu DS (§ 17, odst. 1) => pro všechny dokumenty, které lze konvertovat do e-podoby
- Zpráva technicky zkontrolována, zašifrována, přidána příslušná systémová data (časová razítka) a „přijata k přepravě“
- Zprávy považovány za doručené v okamžiku přihlášení do datové schránky (ne zobrazení zprávy), příp. považovány za doručené (až na výjimky) po uplynutí desetidenní lhůty od jejich dodání do datové schránky (tzv. doručení fikcí)
- Po přijmutí doplněna systémová data (odesilatel si je 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 stejně obezřetně jako k účtu internetového bankovnictví
  - Používat kvalitní antivirovou ochranu 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)

MASARYKOVA UNIVERZITA

Elektronický podpis

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

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 (možnost volby)
- 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:
  „1. je jednoznačně spojen s podepisující osobou,
  2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
  3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
  4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat,“
- 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

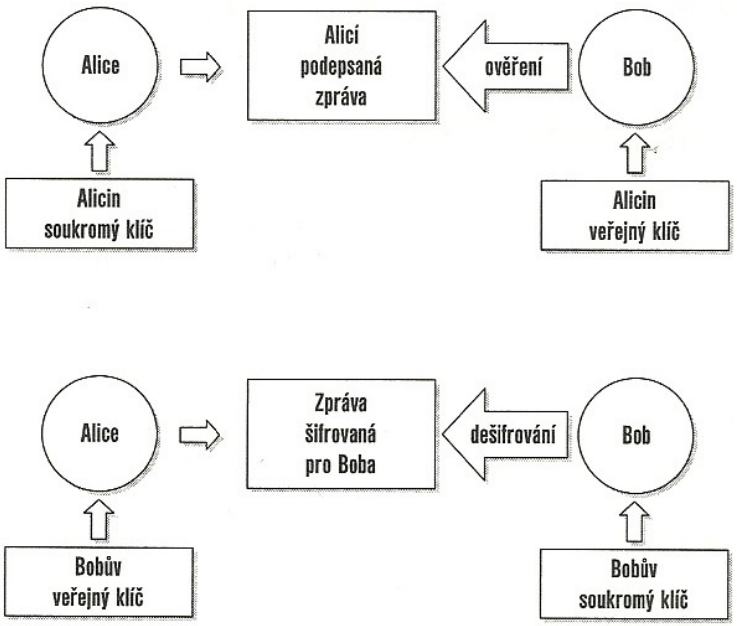
Tabulka 5.1: Obsah certifikátu

Proces vytváření podepsané a důvěrné zprávy

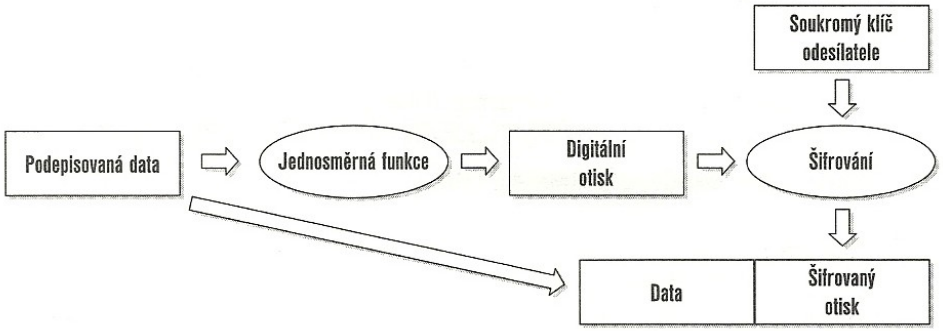
- Hash funkce (komprimace a vytvoření otisku/snímku zprávy)
- Aplikace privátního klíče odesilatele + veřejného klíče adresáta (zašifrování)
- Zpráva s e-podpisem
- Odeslání
- Příjem adresátem
- Aplikace privátního klíče adresáta + veřejného klíče odesílatele (užití hash funkce s pomocí veřejného klíče + 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



Obrázek 5.2: Schéma vytváření digitálního podpisu

Jak vypadá e-podpis?

- Elektronicky podepsaný dokument

Úkol č. 7

- Do 28. 11. 2013 (výjimečně!) poslat mi e-mail s e-podpisem (testovací) na kovarova@phil.muni.cz
- Podívat se, jak vypadá e-podpis v odpovědi a pokusit se ověřit jeho pravost

Zdroje

- Digitální agenda: Komise předkládá akční plán na zvýšení prosperity a kvality života v Evropě. *Evropská komise* [online]. 2010 [cit. 2013-11-15]. Dostupné z: http://ec.europa.eu/ceskarepublika/press/press_releases/10__581_cs.htm
- DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.
- Druhy elektronických podpisů, 5. díl. *ISVS.cz* [online]. 2007 [cit. 2013-11-15]. Dostupné z: http://www.isvs.cz/druhy-elektronickych-podpisu-5-dil/
- Informační systém datových schránek: základní informace. *Datové schránky* [online]. 2009 [cit. 2013-11-15]. Dostupné z: http://www.datoveschranky.info/assets/ke-stazeni/isds_ver3_0_web.pdf
- ŠMÍD, Vladimír. 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). *Fakulta informatiky Masarykovy univerzity* [online]. 2002 [cit. 2013-11-15]. Dostupné z: http://www.fi.muni.cz/~smid/zelpod1.html
- ŠTĚDROŇ, Bohumír. *Úvod do eGovernmentu v České republice: právní a technický průvodce*. 1. vyd. Praha: Úřad vlády České republiky, 2007, 172 s. ISBN 978-808-7041-253.
- Zákon č. 227/2000 Sb., o elektronickém podpisu, v platném znění
- MLYNÁŘ, Vladimír. Zákon o elektronickém podpisu. [online]. [cit. 2013-11-15]. Dostupné z: gjkt.kvalitne.cz/Files/E-podpis.ppt#7
- Zákon č. 101/2000 Sb., o ochraně osobních údajů, v platném znění

MASARYKOVA UNIVERZITA

Děkuji za pozornost.