

OCHRANA OÚ, DATOVÉ SCHRÁNKY, E-PODPIS

Informační politika

4.11. 2011

OCHRANA OÚ

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 služeb IP
- Komunikace s VS správou klíčová – problém = velký problém + VS k dispozici mnoho informací o občanech – nutné zajistit jejich 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 orgány veřejné moci i FO/PO
- Veškeré zpracovávání OÚ, automatizovaně nebo jinými prostředky

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; obrany ČR; veřejného pořádku a vnitřní bezpečnosti; předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů; významného hospodářského zájmu ČR nebo EU; významného finančního zájmu ČR nebo EU, kterým je zejména stabilita finančního trhu a měny, fungování peněžního oběhu a platebního styku, jakož i rozpočtová a daňová opatření; 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**. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu,
- 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**, který umožňuje přímou identifikaci nebo autentizaci 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**. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace,
- 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 nejdříve 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)
- Správce může zpracovávat OÚ jen se souhlasem subjektu údajů, bez něj jen z vymezených výjimečných důvodů
- Subjekt údajů 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 (§ 12)
- Před zahájením zpracování nutné informovat ÚOOÚ o zákonem daných souvislostech (§ 16), výjimky v § 18 (např. zpracování veřejně dostupných informací, zpracování dané zvláštními zákony atp.)
- § 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 (§ 29):
 - dozor nad dodržováním povinností stanovených zákonem při zpracování OÚ,
 - vede [registr zpracování OÚ](#),
 - přijímá podněty a stížnosti na porušení povinností stanovených zákonem při zpracování OÚ a informuje o jejich vyřízení,
 - zpracovává a veřejnosti zpřístupňuje [výroční zprávu](#) o své činnosti,
 - vykonává další působnosti stanovené mu zákonem,
 - projednává přestupky a jiné správní delikty a uděluje pokuty podle tohoto zákona,
 - zajišťuje plnění požadavků vyplývajících z mezinárodních smluv,
 - poskytuje konzultace v oblasti ochrany OÚ,
 - spolupracuje s obdobnými úřady jiných států
- ÚOOÚ ukládá pokuty - výše sankcí 100 000,- Kč až 10 000 000,- Kč

Další zdroje k tématu

- Občanský zákoník, §§ 11-13 ochrana soukromí, osobnosti apod.
- 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](#)

DATOVÉ SCHRÁNKY

Výchozí dokumenty pro Informační systém datových schránek (ISDS)

- [Zákon č. 300/2008 Sb.](#), o elektronických úkonech a autorizované konverzi dokumentů (účinnost od 1.7. 2009)
- Vyhlášky:
 - [Vyhláška č. 192/2009 Sb.](#), kterou se mění vyhláška č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů
 - [Vyhláška č. 191/2009 Sb.](#), o podrobnostech výkonu spisové služby
 - [Vyhláška č. 193/2009 Sb.](#), o stanovení podrobností provádění autorizované konverze dokumentů
 - [Vyhláška č. 194/2009 Sb.](#), o stanovení podrobností užívání a provozování informačního systému datových schránek
 - [Novela Vyhlášky č. 194/2009 Sb.](#), o stanovení podrobností užívání a provozování informačního systému datových schránek
- [Provozní řád](#)

ISDS

- [ISDS](#) + [výukové prostředí](#) minule
- [Rozhraní](#) datových schránek
- 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 (volitelně – nutné povolit, pak dohledatelná adresa každým) – volitelné subjekty o zřízení žádají (zdarma), povinné zřízeno automaticky a bezodkladně
- ISDS = IS VS, obsahuje informace o datových schránkách a jeho uživatelích, správcem MV ČR, provozovatelem držitel poštovní licence => ISDS 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).“ (...)
„Datová schránka není e-mailová schránka. (...) Datová schránka **není nic, co znáte**, nic, o čem by vás mohlo napadnout, že to je.“
(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“
- Zřízení DS:
 1. Vyplnit si žádost na internetu (příp. jinak)
 2. Vytisknout příslušné jedinečné údaje nutné pro identifikaci žádosti
 3. Návštěva libovolného CzechPOINT, kde asistent podle dodaných údajů získá vyplněnou žádost, ověří totožnosti, žádost vytiskne a nechá ji podepsat
 4. Do tří dnů ministerstvo žádost zpracuje a v případě kladného vyřízení zadá pokyn k odeslání obálky s přístupovými údaji do vlastních rukou
- Alternativy zřízení: přijít na CzechPOINT bez předvyplněné žádosti, poslat žádost doporučeným dopisem s podpisem ověřeným u notáře nebo na úřadě, poslat žádost na ePodatelnu ministerstva (nutný e-podpis od kvalifikované certifikační autority)

Subjekty pro datové zprávy

- „elektronické úkony státních orgánů, orgánů územních samosprávných celků, Pozemkového fondu České republiky a jiných státních fondů, zdravotních pojišťoven, Českého rozhlasu, České televize, samosprávných komor zřízených zákonem, notářů a soudních exekutorů (dále jen „orgán veřejné moci“) vůči fyzickým osobám a právnickým osobám, elektronické úkony fyzických osob a právnických osob vůči orgánům veřejné moci a elektronické úkony mezi orgány veřejné moci navzájem prostřednictvím datových schránek,“ (§ 1, odst. 1)
- Oprávněná osoba může pověřit pověřenou osobu, stanovit jí rozsah přístupu do DS
- DS lze využít transparentně pro výměnu písemností v rámci spisových služeb díky dohodě dodavatelů

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. Umožňuje-li to povaha dokumentu a má-li fyzická osoba, podnikající fyzická osoba nebo právnická osoba zpřístupněnu svou datovou schránku, orgán veřejné moci doručuje dokument této osobě prostřednictvím datové schránky, pokud se nedoručuje veřejnou vyhláškou nebo na místě.“ (§ 17, odst. 1) => pro všechny dokumenty, které lze konvertovat do e-podoby (ne např. 3D předměty)
- 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 přijetí doplněna systémová data (odesílatel 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 zabezpečení přístupu prostřednictvím certifikátu (e-podpis)
 - Aktualizace OS a bezpečnostního softwaru
 - K datové schránce vhodné přistupovat stejně obezřetně jako k internetovému účtu v bance
 - Používat kvalitní antivirovou ochranu
 - Používat obousměrný osobní firewall
 - Nepracovat na internetu pod účtem administrátora
 - Zálohovat důležitá data
 - Používat bezpečné bezdrátové připojení
 - Nedůvěřovat neověřeným zprávám, může se jednat o podvodné zprávy
 - Instalujte a užívejte pouze legální software z prověřených zdrojů
- Oprávněná osoba je dle zákona povinna zacházet s přístupovými údaji k DS tak, aby nemohlo dojít k jejich zneužití (§ 9, odst. 2)

ELEKTRONICKÝ PODPIS

Elektronický podpis

- Zaveden v ČR zákonem č. 227/2000 Sb., o elektronickém podpisu ze dne 29.6. 2000 (pak 12 novelizací), krom e-podpisu novelizace mnoha správních předpisů, zákoníků atd. pro dosažení rovnoprávnosti tradičního a e-prostředí
- Klíčový předpoklad pro datové schránky
- Podpora podnikání v e-prostředí (odstranění překážek, podpora vzniku důvěryhodnějšího prostředí pro PO)
- Usnadnění komunikace mezi VS a občanem (možnost volby)
- Výhledově snížení nákladů na chod VS

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 = certifikát, splňující podmínky v § 12 (např. identifikace podepisující osoby, doba platnosti, omezení...)
- Certifikační autorita = poskytovatel certifikačních služeb
- Kvalifikované časové razítko = „datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, **že uvedená data v elektronické podobě existovala před daným časovým okamžikem,**“ (§ 2, písm. r)
- Pravidlo vzájemného uznávání certifikátů v rámci EU (na stejné úrovni a se stejnou působností)
- Při porušení zákona sankce pro poskytovatele certifikačních služeb až do 10 milionů Kč

E-podpis a VS

- Pro komunikaci s orgány VS nutné využití služeb akreditovaného poskytovatele certifikačních služeb
- (Akreditovaným) e-podpisem podepsané dokumenty mají právně stejnou platnost jako dokumenty listinné podepsané vlastnoručně
- VS přijímá a odesílá e-datové zprávy prostřednictvím e-podatelný
- Předpokládá se, že odesílatel před podpisem zprávu četl

Poskytovatelé e-podpisu

- Poskytovatel – musí vést seznam zneplatněných certifikátů (ze strany příjemců zpráv možnost verifikace; prevence zneužití)
- Akreditovaní poskytovatelé:
 - [První certifikační autorita](#) od 15.3. 2002
 - [Česká pošta](#) od 15.7. 2005
 - [eIdentity](#) od 12.9. 2005

Úrovně zabezpečení e-podpisem

- Zpráva podepsaná (ne však chráněná proti čtení neoprávněnou osobou) – při dešifrování ale adresát pozná, zda byla zpráva „po cestě“ někým měněna
- Důvěrná zpráva = zpráva podepsaná a zároveň chráněná proti čtení obsahu neoprávněnou osobou (obsah mohou číst pouze vybrané osoby, které se prokáží správným dešifrovacím kódem = privátní klíč)

Šifrování (Kryptografie)

- Symetrická šifra
 - Méně náročná
 - Rychlejší
 - Méně bezpečná
 - Nutnost zpřístupnit příjemci zprávy kód pro dešifrování
 - Vhodné před vznikem certifikačních autorit či pro soukromou linii komunikace bez účasti CA
- Asymetrická šifra
 - Náročnější (technicky)
 - Pomalejší
 - Více bezpečná

Asymetrická šifra

- Dvojice klíčů
 - Privátní (soukromý) klíč
 - Veřejný klíč
 - => Generuje pomocí SW certifikační autorita
- Spolehlivé zpřístupnění veřejného klíče => certifikační autorita
- Privátní klíč => osoba, které náleží, je povinna ho chránit a předcházet zneužití, při (podezření na) zneužití povinnost hlásit poskytovateli certifikačních služeb

Proces podepisování a zabezpečování zprávy

- Hash funkce (komprimace a vytvoření otisku/snímku zprávy)
- Aplikace privátního klíče odesílatele + 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

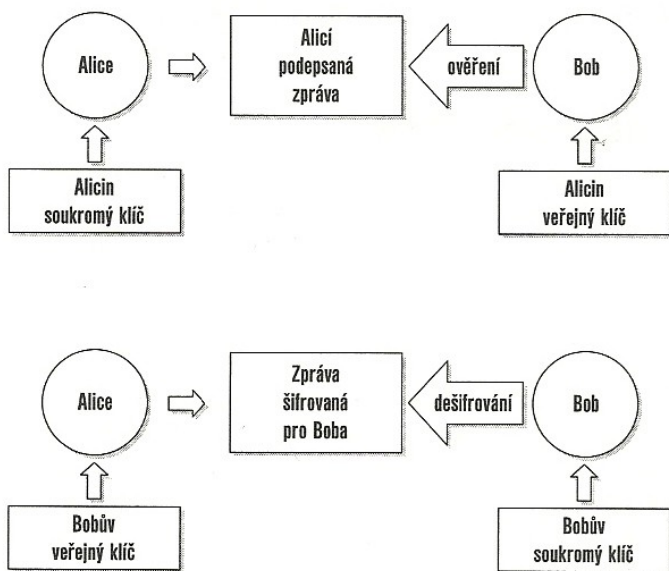
Certifikovaný klíč

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

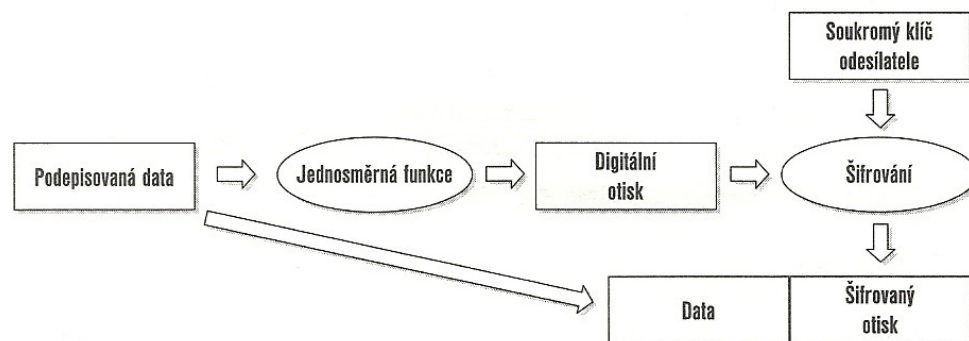
Tabulka 5.1: Obsah certifikátu

- Nepopiratelnost podpisu zajištěna soukromým klíčem, který je jedinečný a zpětně nezjistitelný, a kvalifikovaným certifikátem (vytváří autorita, ne kdokoli, nutné ověřovat platnost)
- 4 třídy certifikátů (čím vyšší, tím víc požadavků), pro komunikaci se státní správou min. úroveň 3

Digitální podpis a šifrování



Obrázek 2.10: Šifrování versus podepisování



Obrázek 5.2: Schéma vytváření digitálního podpisu

Zdroje

- DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno : Computer Press, 2004. 190 s. ISBN 8025101061.
- [Druhy elektronických podpisů](#)
- [Digitální agenda: Komise předkládá akční plán na zvýšení prosperity a kvality života v Evropě](#)
- [Informační systém datových schránek: základní informace](#)
- ŠTĚDRŮŇ, 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. 227/2000 Sb., o elektronickém podpisu
- [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 \(ppt presentace\)](#)