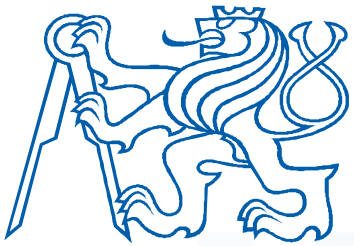
České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra telekomunikační techniky

A7B32KBE – 12.přednáška

Elektronický podpis

Ing. Tomáš Vaněk, Ph.D. tomas.vanek@fel.cvut.cz



Obsah

- Elektronický podpis
- Digitální podpis
- EP a české zákony

Jiří Peterka – Báječný svět elektronického podpisu

http://www.bajecnysvet.cz/

Druhy podpisů

Ze striktně právního hlediska lze rozlišovat tyto druhy podpisů:

- ***podpis,***
- ***vlastnoruční podpis***
- ***ověřený podpis***
- ***vlastnoručně psaný podpis***

  (čl. 4 odst. 1 sdělení č. 179/1996 Sb. . o přístupu České republiky k Úmluvě o společném tranzitním režimu)
- ***elektronický podpis***
- ***podpis na listině, který osoba uznala za vlastní***

  (74 zákona č. 358/1992 Sb. – Zákon o notářích a jejich činnosti)

Význam podpisu

Význam podepsaného dokumentu (z pohledu podepisující osoby):

- důkaz, že osoba je obsahem dokumentu vázána
- podepsaný dokument představuje věrohodnou záruku pro splnění určitých závazků (peněžních, hmotných, časových atd.)
- potvrzuje autorství textu dokumentu
- pokud podepsaný dokument sepsal někdo jiný, pak podepisující osoba potvrzuje svým podpisem stvrzuje, že souhlasí s obsahem daného dokumentu
- prokazuje skutečnost, že podepisující osoba byla v daném čase přítomna na stanoveném místě

Elektronický podpis

Elektronický podpis

Důvody zavádění elektronického podpisu :

- nutnost zavedení ekvivalentu ke klasickému podpisu
- velký počet dokumentů v elektronické podobě
- existence některých dat pouze v digitální podobě
- zamezení snadnému padělání

- U elektronického podpisu je nutné zajistit
  - **identifikaci podepisující osoby**
  - **neporušenost doručeného dokumentu (datová integrita)**
  - **nepopiratelnost**
  - **právní akceptovatelnost**
  - **utajení obsahu zprávy (šifrování) - VOLITELNÉ**
  - **zjištění, zda dokument existoval v daném čase (časová razítka) - VOLITELNÉ**

Digitální vs. Elektronický podpis

Digitální podpis

- využívá asymetrické kryptografie
- konkrétní technické řešení
- digitální podepisování chápeme jako dnes bezpečnostně nejlepší způsob realizace elektronického podepisování

Elektronický podpis

- obecnější pojem
- **technologicky neutrální**
- zahrnuje v sobě kromě digitálního podpisu i všechny jiné metody zajišťující požadované vlastnosti (např. biometrické metody)
- vhodný pro použití v legislativních dokumentech
- přesná definice je v ZoEP

Digitální vs. Elektronický podpis

- Pojmy z jiné oblasti
  - digitální podpis je pojem kryptologický/matematický
  - elektronický podpis je pojem zejména právní a normotvorný
- Odlišný pohled
  - definice elektronického podpisu stanovuje požadavky (ale neřeší jak jich dosáhnout)
  - nástroje pro digitální podpis se soustředí na plnění stanovených požadavků

Co je elektronický podpis?

ZoEP definuje v 2a) EP jako údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené.

EP slouží jako metoda k jednoznačnému ověření totožnosti podepsané osoby ve vztahu k datové zprávě

EP vychází z Direktivy Evropské komise č. 1999/93/EC

Této velmi obecné definici vyhoví i podpis textem obyčejného e-mailu.

http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

Co je elektronický podpis ?

Z kryptografického hlediska se EP chápe jako soustava dílčích kryptografických funkcí zabezpečující:

- Identifikaci
- Autentizaci
- Integritu
- Nepopiratelnost

ZEP - zaručený elektronický podpis

Varianta EP, kterou většinou intuitivně chápeme jako EP se v českém právním řádu nazývá Zaručený EP (ZEP)

ZoEP definuje v 2b) zaručený elektronický podpis takový EP, který splňuje následující požadavky:

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

Vytvoření zaručeného EP

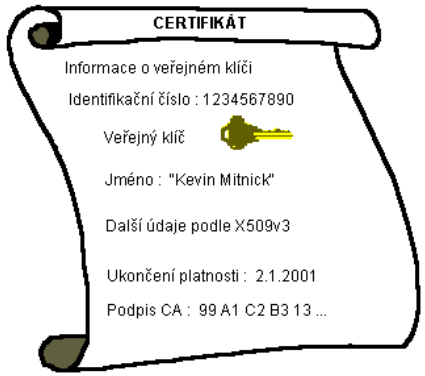
Datová zpráva , kterou chci podepsat

SHA-1
MD5

Otisk (hash) zprávy

RSA
DSA
ECC

Elektronický podpis zprávy (zašifrovaný otisk)

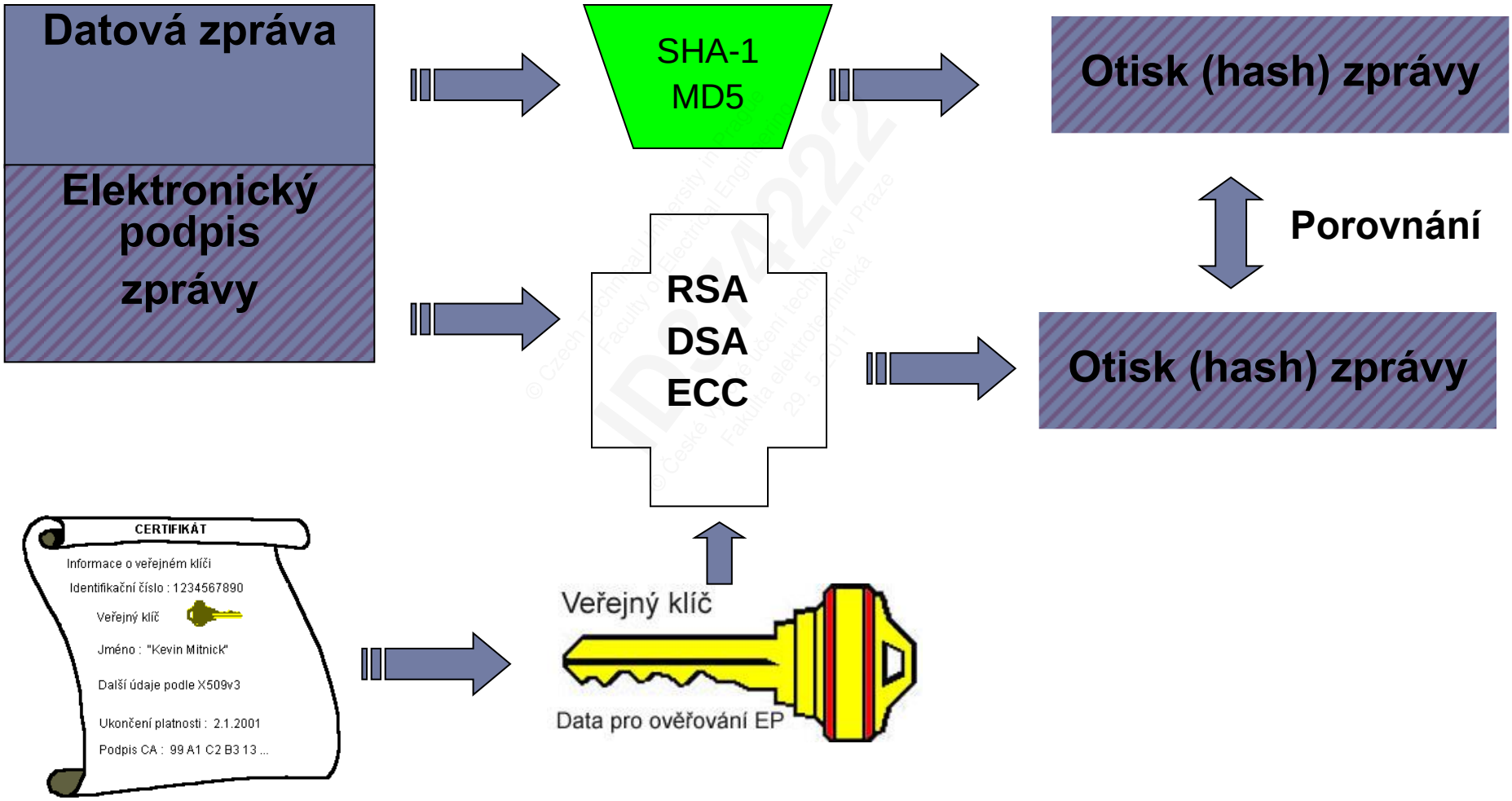


Elektronicky lze podepsat jakákoliv digitální data

- text (TXT, DOC, RTF, XLS,..)
- obrázek (BMP, JPG, GIF, PNG,…)
- hudba (WAV, MP3, …)
- video (AVI, MPG, …)
- spustitelný soubor (EXE, COM, …)
- cokoliv

Z hlediska generování podpisu se libovolná data chápou jako posloupnost jedniček a nul, která vstupují do hashovací funkce.

Ověření zaručeného EP



EP v této formě zajistí:

- Identifikaci odesilatele
- Datovou integritu (neporušenost)
- Nepopiratelnost
- Právní akceptovatelnost

Legislativa v ČR

Zákon o elektronickém podpisu

č.227/2000 Sb. ze dne 29.6.2000

Upravuje používání elektronického podpisu poskytování souvisejících služeb, kontrolu povinností stanovených tímto zákonem a nastiňuje základní podmínky udělení statutu akreditovaný poskytovatel certifikačních služeb. Definuje rozdíl mezi certifikátem obecným a kvalifikovaným.

Legislativa v ČR

Nařízení vlády č.304/2001 Sb. ze dne 25.7.2001

Úprava ZoEP, zejména činnost elektronických podatelen v rámci orgánů veřejné moci tak, aby bylo zajištěno přijímání podání v elektronické podobě při využití kvalifikovaných certifikátů dle výše uvedeného zákona.

Zákon č.226/2002 Sb. ze dne 9.5.2002

Změna 11 ZoEP upravujícího podmínky používání elektronického podpisu a certifikátů v oblasti orgánů veřejné moci.

Legislativa v ČR

Vyhláška Úřadu pro ochranu osobních údajů č.366/2001 Sb. ze dne 3.10.2001

Upřesňuje podmínky 6 ZoEP specifikujícího povinnosti poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty a 17 ZoEP, který definuje prostředky pro vytváření a ověřování zaručených elektronických podpisů. Stanovuje požadavky na celkovou bezpečnostní politiku poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty a kryptografické moduly, které používají poskytovatelé vydávající kvalifikované certifikáty

Legislativa v ČR

Zákon č.517/2002 Sb. ze dne 14.11.2002

Drobná úprava ZoEP (nahrazení slova "Úřad pro ochranu osobních údajů" a "Úřad" slovem "Ministerstvo informatiky")

Zákon č.440/2004 Sb. ze dne 24.6.2004

Úprava ZoEP specifikující podmínky poskytování zaručeného elektronického podpisu, elektronických značek, kvalifikovaných časových razítek a kvalifikovaných systémových certifikátů.

Legislativa v ČR

Zákon č.517/2002 Sb. ze dne 14.11.2002

Drobná úprava ZoEP (nahrazení slova "Úřad pro ochranu osobních údajů" a "Úřad" slovem "Ministerstvo informatiky")

Zákon č.440/2004 Sb. ze dne 24.6.2004

Úprava ZoEP specifikující podmínky poskytování zaručeného elektronického podpisu, elektronických značek, kvalifikovaných časových razítek a kvalifikovaných systémových certifikátů.

Legislativa v ČR

Nařízení vlády 495/2004Sb. ze dne 25.8.2004

nařizuje orgánům veřejné moci zřídit e-podatelny (nebo v případě malého objemu elektronické komunikace zajistit příjem a odesílání zpráv prostřednictvím e-podatelny jiného úřadu), vybavit příslušné zaměstnance zaručenými elektronickými podpisy a zajistit odpovídajícím způsobem ochranu zpracovávaných informací.

Vyhláška č. 496/2004 Sb. k elektronickým podatelnám

upravuje postup, jak mají orgány veřejné moci přijímat a odesílat datové zprávy prostřednictvím elektronické podatelny., které nařizuje orgánům veřejné moci elektronickou podatelnu zřídit a má sloužit jako návod, jak naplnit podmínky dané tímto nařízením vlády.

Legislativa v ČR

Zákon č. 110/2007 Sb., o některých opatřeních v soustavě ústředních orgánů státní správy, souvisejících se zrušením Ministerstva informatiky a o změně některých zákonů

- zrušení Ministerstva informatiky k 1.6.2007
- agendu převzalo Ministerstvo vnitra

Zákon č. 300/2008 Sb. o elektronických úkonech, osobních číslech a autorizované konverzi dokument

- schválen 25.6.2008
- účinnost od 1.7.2009

Elektronická značka

- technologicky se jedná o naprosto totéž jako ZEP
- rozdíl je v právní rovině
  - EP používá pouze fyzická osoba - 2e)
  - EZ může používat i právnická osoba nebo organizační složka státu
- ekvivalent úředního razítka

Elektronická podatelna

- místo pro vstup a výstup eln. materiálů do/z firmy/úřadu
- ověřuje platnost EP a QC příchozích zpráv
- pro státní úřady platí nařízení vlády 495/2004Sb. a vyhláška o elektronických podatelnách č. 496/2004Sb.

Otázky k EP

Je podepsaná zpráva současně zašifrovaná ? **NE**

Zpráva, která je elektronicky podepsána má zajištěnu **integritu** (je zabezpečena proti pozměnění obsahu zprávy) a **neodmítnutelnos**t odpovědnosti (odesilatel nemůže popřít odeslání takové zprávy).

Otázky k EP

Jaká je platnost EP ve srovnání s vlastnoručním podpisem?

EP podle zákona nemá v českém právním řádu při všech právních úkonech stejné účinky jako podpis vlastnoruční.

V oblasti soukromého práva lze činit právní úkony elektronicky a tyto úkony elektronicky podepisovat tam, kde právní předpis či jiné platné ujednání nedovozuje neplatnost tohoto úkonu, pokud není dodržena listinná forma.

V oblasti veřejného práva lze použít elektronický podpis pouze tam, kde to zákon dovoluje.

Otázky k EP

Musí úřad potvrdit, že datovou zprávu přijal? ANO

- potvrzení doručení elektronického podání, pokud bylo zasláno na adresu e-podatelny, upravuje vyhláška č. 496/2004 Sb.
- E-podatelna orgánu veřejné moci musí potvrdit doručení odesilateli zasláním datové zprávy, ve které je uvedeno datum a čas doručení datové zprávy a její charakteristika.
- Potvrzující zpráva musí být opatřena uznávaným podpisem pracovníka orgánu veřejné moci nebo elektronickou značkou orgánu.

- Podmínkou odeslání potvrzení je samozřejmě možnost zjistit z přijaté datové zprávy elektronickou adresu odesilatele.

Otázky k EP

Platí v ČR certifikáty vydané i v jiných zemích EU?

Otázku řeší 16 ZoEP

- certifikát vydaný cizím PCS v rámci EU jako kvalifikovaný je uznáván jako QC ve smyslu ZoEP
- certifikát vydaným PCS mimo rámec EU jako kvalifikovaný je uznán pokud

a) PCS byl akreditován jako APCS v některém ze států EU, nebo

b) PCS z některého členského státu EU převezme odpovědnost za platnost a správnost certifikátu ve stejném rozsahu jako u svých kvalifikovaných certifikátů, nebo

c) to vyplývá z mezinárodní smlouvy

Nesmyslné věty o EP

Mít / koupit / prodat / ztratit elektronický podpis …

Elektronický podpis se pro každý podepisovaný dokument vždy vytváří znovu, výsledek je jedinečný a záleží nejen na soukromém klíči podepisující osoby, ale i na obsahu datového souboru, který osoba podepisuje....

EP je pro každou podepsanou zprávu unikátní

Klasický podpis je naopak bez ohledu na podepisované informace stejný (nebo by měl být…)

Kde můžete získat kvalifikovaný certifikát?

- **První certifikační autorita, a. s.**

  Adresa: Podvinný mlýn 2178/6, Praha 9, 190 00

  www.ica.cz

- **Česká pošta, s. p.**

  Adresa: Olšanská 38/9, Praha 3, 225 99

  www.postsignum.cz

- **eIdentity a. s.**

  Adresa: Vinohradská 184/2396, Praha 3, 130 00

  www.eidentity.cz

Dotazy