Zákon o elektronickém podpisu

Zaručený elektronický podpis

- Je jednoznačně spojen s podepisující osobou (jen fyzická osoba!);
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě;
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou;
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Současná legislativa

- Zákon o elektronickém podpisu 227/2000
- Vyhláška k ZEP 336/2001
- Novela ZEP 440/2004
- Nařízení vlády provádějící ZEP 495/2004
- Vyhláška o podatelnách 496/2004

Provádění ZEP

- pokud úřad je povinen zpracovávat „uznávané elektronické podpisy“
  - vytvoří podatelnu
  - koupí počítač a programy
  - vystaví pro zaměstnance certifikáty

  - co dělat při výskytu virů
  - … ☺

O elektronických podatelnách

- přijetí a doručení datové zprávy
  - postup při chybě
- odeslání datové zprávy
- identifikace osob
  - jednoznačná identifikace osob na základě desetimístného čísla 1100100100-4294967295
  - toto číslo nesmí být osobním údajem
- §4, odst a) osobním údajem jakýkoliv údaj týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu. O osobní údaj se nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřené množství času, úsilí či materiálních prostředků

ZEP

- Základní struktura vychází ze směrnice EU
  - elektronický podpis
    - údaje logicky spojené se zprávou, umožňují ověření totožnosti odesílatele
  - zaručený elektronický podpis
    1. jednoznačně spojen s podepisující osobou
    2. umožňuje identifikovat osobu ve vztahu k datové zprávě
    3. vytvořen a připojen prostředky pod výhradní správou podepisujícího
    4. připojen tak, že to umožňuje zjistit následnou změnu zprávy

Složité pojmy

- data pro vytváření elektronických podpisů
- data pro ověřování elektronických podpisů
- prostředek pro vytváření elektronických podpisů
- prostředek pro ověřování elektronických podpisů
- prostředek pro bezpečné vytváření elektronických podpisů
- nástroj elektronických podpisů
- poskytovatel certifikačních služeb

Povinnosti

- podepisující osoby
  - zacházet s prostředky a daty náležitě …
  - uvědomit poskytovatele, že hrozí zneužití dat pro podepisování …
  - podávat správné informace pro kvalifikovaný certifikát
- poskytovatele certifikačních služeb
  - viz § 5 – vydávání certifikátů, vedení seznamu, bezpečné nástroje, finanční zdroje, dokumentace,
- nejsou – ověřující osoby

Povinnosti poskytovatele

- §5,1,f) zajistit provozování bezpečného a veřejně přístupného seznamu vydaných kvalifikovaných certifikátů, a to i dálkovým přístupem, a údaje v něm obsažené při každé změně okamžitě aktualizovat

- 7 Poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, musí neprodleně ukončit platnost certifikátu, pokud o to podepisující osoba požádá, nebo v případě, že byl certifikát vydán na základě nepravdivých, nebo chybných údajů.

Akreditace

- §11, „orgány veřejné moci“ mohou používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb.

Náležitosti kvalifikované certifikátu

- označení, že je kvalifikovaný
- obchodní jméno poskytovatele
- jméno a příjmení podepisující osoby, nebo její pseudonym
- data pro ověřování podpisu
- zaručený elektronický podpis poskytovatele
- číslo
- počátek a konec platnosti
- údaje o omezení použití
- odst 2. další osobní údaje jen se svolením osoby

Zrušení kvalif. certifikátu

- § 15 – úřad může nařídit zneplatnění certifikátu
  …podepisující používá prostředek pro podepisování, který vykazuje bezpečnostní nedostatky, které by umožnily padělání zaručených podpisů nebo změnu podepisovaných údajů.

Prostředek pro bezpečné ověřování podpisu

- zajistí, že
  - ověřovaná data odpovídají datům zobrazeným
  - podpis spolehlivě ověřen a řádně zobrazen
  - ověřovatel může zjistit obsah podepsaných dat
  - pravost a platnost certifikátu byla spolehlivě zjištěna
  - výsledek ověření a totožnost podepisující osoby spolehlivě zjištěny
  - uvedeno použití pseudonymu
  - zjistit veškeré změny ovlivňující bezpečnost

Novela zákona

- hodně rozsáhlá
- **přidání elektronické značky**
  - jednoznačně spojena s podepisující osobou
  - prostředky musí být pod výhradní kontrolou podepisujícího
  - připojena tak, že je možné zjistit následnou změnu dat
  - umístění soukromého klíče např. na serveru
- označující osoba

Elektronický podpis vs. značka

- Elektronický podpis
  - podepisující osoba je fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby;
  - pro ověření podpisu je vydáván certifikát (veřejného klíče).
- Elektronická značka
  - označující osobou fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou;
  - pro ověření podpisu je vydáván systémový certifikát (veřejného klíče).
- Technologicky jde o totéž
  - Jen úroveň ochrany soukromého klíče je jiná.

Novela zákona

- **nový pojem kvalifikované časové razítko**
  - vydává kvalifikovaný poskytovatel
  - spojuje data s časovým okamžikem
  - součástí je elektronická značka kvalif. poskytovatele

Kvalifikované časové razítko

- unikátní číslo razítka
- označení pravidel použitých při vydání
- identifikace vydavatele
- čas
- data, pro které bylo razítko vydáno
  - použití podpisu, nebo značky zaručuje, že dojde-li k porušení obsahu datové zprávy … je toto možné zjistit.
- značku vydavatele

Novela zákona

- kvalifikovaný systémový certifikát
  - certifikát pro vydávání elektronických značek
- elektronická podatelna
  - příjem a odesílání elektronických zpráv

- zjednodušila se definice povinností poskytovatele
- stále musí existovat veřejně dostupná databáze certifikátů

Novela

- odpovědnost za škodu
  - za škodu způsobenou porušením povinností stanovených tímto zákonem odpovídá poskytovatel certifikačních služeb *vydávající kvalifikované certifikáty* podle zvláštních právních předpisů.

Vyhláška k ZEP

- upřesňuje §6 (povinnosti poskytovatele certifikačních služeb) a 17 (prostředky pro bezpečné vytváření a ověřování podpisů)
- dokumenty
  - certifikační politika - zásady
  - certifikační prováděcí směrnice - postupy
  - celková bezpečnostní politika
  - systémová bezpečnostní politika
  - plán pro krizové situace
  - finanční plán (dostatečnost finančních zdrojů)

Prostředky pro bezpečné vytváření

- má vlastnosti, které zaručí, že
  - osoba ví, že prostředek používá
  - osoba se autentizuje k prostředku
- algoritmy podle přílohy
- prostředek musí být bezpečně ohodnocen
  - FIPS 140
- to samé musí platit pro ověřování podpisu

Prosba – terminologie

- Nekryptujeme ani neenkryptujeme – **šifrujeme**
- Nešifrujeme soukromým klíčem – **podepisujeme**
- Nerozšifrováváme – **dešifrujeme**
- Neautentikujeme, neautentifikujeme a neidentizujeme – **autentizujeme** a **identifikujeme**

- Haš, hash – oba OK
- Čistý text, vstupní text, otevřený text – OK