

**Vyhláška**  
**Úřadu pro ochranu osobních údajů**  
**ze dne ..... 2001**

**o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu**  
**a o upřesnění požadavků na nástroje elektronického podpisu**

Úřad pro ochranu osobních údajů (dále jen „Úřad“) stanoví podle § 20 zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu):

**§ 1**  
**Předmět úpravy**

Tato vyhláška upřesňuje podmínky stanovené v § 6 a 17 zákona o elektronickém podpisu a způsob, jakým se jejich splnění bude dokládat, a požadavky, které musí splňovat nástroje elektronického podpisu, a náležitosti postupu a způsobu vyhodnocování shody nástrojů elektronického podpisu s těmito požadavky.

**§ 2**  
**Způsob dokládání splnění povinností stanovených v § 6 zákona o elektronickém podpisu**

(1) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty dokládá splnění povinností stanovených v § 6 zákona o elektronickém podpisu těmito dokumenty

- a) certifikační politikou,
- b) certifikační prováděcí směrnicí,
- c) celkovou bezpečnostní politikou,
- d) systémovou bezpečnostní politikou,
- e) plánem pro zvládání krizových situací a plánem obnovy a
- f) čestným prohlášením o dostatečnosti finančních zdrojů na provoz.

(2) Obsahem certifikační politiky je zejména

- a) stanovení zásad, které poskytovatel certifikačních služeb vydávající kvalifikované certifikáty uplatňuje při zajištění služeb spojených s elektronickými podpisy, a
- b) popis vlastností dat pro vytváření elektronického podpisu a jim odpovídajících dat pro ověřování elektronického podpisu, která si vytváří osoba žádající o vydání kvalifikovaného certifikátu, a k nimž má být vydán kvalifikovaný certifikát; kryptografické algoritmy a jejich parametry, které musí být pro tato data použity, jsou uvedeny v příloze č. 1 této vyhlášky.

(3) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty umožňuje trvalý dálkový přístup ke své certifikační politice.

(4) Obsahem certifikační prováděcí směrnice je zejména stanovení postupů, které poskytovatel certifikačních služeb vydávající kvalifikované certifikáty uplatňuje při zajištění služeb spojených s elektronickými podpisy.

(5) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty umožňuje trvalý dálkový přístup ke své certifikační prováděcí směrnici, s výjimkou těch částí, jejichž zveřejnění by mohlo ohrozit bezpečnost služeb spojených s elektronickými podpisy.

(6) Obsahem celkové bezpečnostní politiky je zejména stanovení cílů a popis způsobu zajištění celkové bezpečnosti poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty.

(7) Obsahem systémové bezpečnostní politiky je zejména stanovení cílů a popis způsobu zajištění bezpečnosti informačního systému, jehož prostřednictvím poskytovatel certifikačních služeb vydávající kvalifikované certifikáty zajišťuje služby spojené s elektronickými podpisy, a to zejména

- a) způsob uplatnění celkové bezpečnostní politiky ve vztahu k informačnímu systému, jehož prostřednictvím zajišťuje služby spojené s elektronickými podpisy,
- b) popis vazeb mezi informačním systémem, jehož prostřednictvím zajišťuje služby spojené s elektronickými podpisy, a jinými informačními systémy, které provozuje,
- c) způsob ochrany dat a jiných prvků informačního systému, jehož prostřednictvím zajišťuje služby spojené s elektronickými podpisy,
- d) popis bezpečnostních opatření a
- e) vyhodnocení analýzy rizik.

(8) Celková bezpečnostní politika a systémová bezpečnostní politika musí odpovídat požadavkům technických předpisů upravujících oblast informační bezpečnosti<sup>1</sup>.

(9) Obsahem plánu pro zvládání krizových situací je zejména stanovení postupů, které jsou uplatněny v případě mimořádné události. Mimořádnou událostí se pro účely této vyhlášky rozumí událost, která ohrožuje poskytování služeb spojených s elektronickými podpisy a která nastala v důsledku selhání informačního systému nebo výskytu faktoru, který není pod kontrolou poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty.

(10) Obsahem plánu obnovy je zejména stanovení postupů, pomocí nichž má být obnovena řádná funkce informačního systému, jehož prostřednictvím poskytovatel certifikačních služeb vydávající kvalifikované certifikáty zajišťuje služby spojené s elektronickými podpisy.

(11) Obsahem čestného prohlášení o dostatečnosti finančních zdrojů na provoz je

- a) prohlášení o dostatečnosti těchto zdrojů a jejich přehled,
- b) prohlášení o tom, že stát neeviduje u poskytovatele vydávajícího kvalifikované certifikáty pohledávky na daních, clu a poplatcích, pokutách, pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti nebo na pojistném na všeobecné zdravotní pojištění, a
- c) prohlášení o tom, že na žadatelův majetek nebyl prohlášen konkurz, není povoleno vyrovnání, popřípadě nevstoupil do likvidace.

---

<sup>1</sup> Například ISO 17799 Informační technologie - Soubor postupů pro řízení informační bezpečnosti, ČSN/ISO/IEC TR 13335 Informační technologie - Směrnice pro řízení bezpečnosti IT 1 – 3.

(12) Při zajišťování služeb spojených s elektronickými podpisy poskytovatel certifikačních služeb vydávající kvalifikované certifikáty postupuje podle dokumentů uvedených v odstavci 1 písm. a) až e).

### § 3

#### **Bezpečnost postupu při vydávání kvalifikovaných certifikátů a provozování seznamu certifikátů, které byly zneplatněny**

(1) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty podepisuje zaručeným elektronickým podpisem kvalifikované certifikáty a seznamy kvalifikovaných certifikátů, které byly zneplatněny. Tento zaručený elektronický podpis musí být založený na kvalifikovaném certifikátu poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty.

(2) Nástroj elektronického podpisu používaný pro podepisování podle odstavce 1 nelze použít pro jiné účely.

(3) Uvedení do provozu a změnu provozního režimu nástroje elektronického podpisu používaného pro podepisování podle odstavce 1 vyžaduje, aby je prováděly současně nejméně dvě fyzické osoby, zpravidla zaměstnanci poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty, které jsou jím pro tuto činnost určeny.

(4) V případě, že jsou data pro vytváření elektronického podpisu používána pro podepisování vydávaných kvalifikovaných certifikátů a pro podepisování seznamu kvalifikovaných certifikátů, které byly zneplatněny, nelze je použít jinak než pro tyto účely.

(5) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty zajistí dostupnost svého kvalifikovaného certifikátu nejméně dvěma na sobě nezávislými způsoby.

### § 4

#### **Provozování seznamu certifikátů, které byly zneplatněny**

(1) Seznam kvalifikovaných certifikátů, které byly zneplatněny, je provozován tak, aby jeho dostupnost byla zajištěna dvěma nezávislými způsoby, z nichž nejméně jeden musí umožnit dálkový přístup a musí být nepřetržitě dostupný.

(2) Doba mezi ukončením platnosti kvalifikovaného certifikátu a zveřejněním údaje o ukončení této platnosti v seznamu kvalifikovaných certifikátů, které byly zneplatněny, může činit nejvýše 24 hodin. Tento údaj obsahuje číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb, datum a čas s uvedením hodiny, minuty a sekundy, kdy je certifikát zneplatněn.

## § 5

### Používání bezpečného systému

(1) Používaný systém se považuje za bezpečný, pokud u dat, která zpracovává, je zajištěna důvěrnost, integrita, dostupnost, prokazatelnost jejich původu a odpovídá požadavkům technických předpisů upravujících oblast informační bezpečnosti<sup>2</sup>.

(2) Za účelem doložení bezpečnosti postupů podle § 6 odst. 1 písm. j) zákona o elektronickém podpisu poskytovatel certifikačních služeb vydávající kvalifikované certifikáty zajistí zaznamenávání událostí, které systém vykonává při

- a) vydání kvalifikovaných certifikátů,
- b) ukončení platnosti kvalifikovaných certifikátů,
- c) nakládání s daty pro vytváření elektronického podpisu a jim odpovídajícími daty pro ověřování elektronického podpisu poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty (dále jen „párová data poskytovatele“), a to během jejich celého životního cyklu, a
- d) nakládání s kvalifikovaným certifikátem poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty, a to během jeho celého životního cyklu.

(3) Záznamy o událostech podle odstavce 2 musí být pořizovány, uchovávány a zpracovávány se zachováním jejich dostupnosti, integrity, časové autentičnosti a důvěrnosti.

## § 6

### Bezpečnost postupu při nakládání s párovými daty poskytovatele

(1) Při vytváření, používání a uchovávání párových dat poskytovatele musí být jakákoliv manipulace s těmito daty prováděna

- a) výhradně fyzickými osobami, zpravidla zaměstnanci poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty, které jsou jím pro tuto činnost určeny,
- b) podle postupů stanovených certifikační prováděcí směrnici a
- c) podle bezpečnostních opatření stanovených systémovou bezpečnostní politikou.

(2) Při vytváření párových dat poskytovatele musí být použity algoritmy splňující kryptografické parametry uvedené v příloze č. 2 této vyhlášky.

(3) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty je povinen svá data pro vytváření elektronického podpisu zničit po ukončení jejich životního cyklu; o tom vyhotoví zápis, který obsahuje

- a) popis způsobu zničení dat,
- b) datum zničení dat,
- c) datum vyhotovení zápisu a
- d) podpis osoby oprávněné jménem poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty toto zničení zajistit.

---

<sup>2</sup> Například ISO/IEC 15408 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti informačních technologií, bezpečnostní profil odpovídající úrovni zaručitelnosti bezpečnosti 4.

(4) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty v případě neoprávněného použití nebo odůvodněné obavy ze zneužití svých dat pro vytváření elektronického podpisu užívaných pro podepisování vydávaných kvalifikovaných certifikátů a pro podepisování seznamu kvalifikovaných certifikátů, které byly zneplatněny, je bezodkladně zejména povinen

- a) ukončit platnost svého kvalifikovaného certifikátu, který byl k těmto datům vydán,
- b) ukončit platnost kvalifikovaných certifikátů, které mohou být tímto ohroženy,
- c) zpřístupnit informaci o ukončení platnosti svého kvalifikovaného certifikátu s uvedením důvodu ukončení platnosti způsobem umožňujícím dálkový přístup a
- d) informovat osoby, které byly tímto ukončením platnosti kvalifikovaného certifikátu poskytovatele dotčeny, o ukončení platnosti jejich kvalifikovaných certifikátů s uvedením důvodu tohoto ukončení.

## § 7

### **Objektová bezpečnost**

Pro zajišťování služeb spojených s elektronickými podpisy musí způsob zabezpečení ochrany objektů, použití technických prostředků, způsob zabezpečení fyzické ostrahy a režimová opatření pro účely objektové bezpečnosti splňovat požadavky stanovené zvláštním právním předpisem<sup>3</sup> pro stupeň utajení "důvěrné".

## § 8

### **Personální bezpečnost**

(1) Osoby přijaté do pracovního nebo obdobného poměru za účelem zajišťování služeb spojených s elektronickými podpisy musí být

- a) seznamovány s dokumenty uvedenými v § 2 odst. 1 písm. a) až e) v rozsahu, který odpovídá jejich pracovnímu zařazení, a
- b) proškoleny tak, aby jejich odborné předpoklady odpovídaly tomuto zařazení.

(2) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty pořizuje písemné záznamy o seznamování a proškolení podle odstavce 1.

## § 9

### **Ověření používání bezpečného systému a zajištění dostatečné bezpečnosti postupů, které tento systém podporují**

Požadavek na používání bezpečného systému a zajištění dostatečné bezpečnosti postupů, které tento systém podporují, se považuje za splněný, pokud je doložen

- a) dokumenty uvedenými v § 2 odst. 1 písm. a) až e) a
- b) hodnocením odpovídajícím požadavkům technických předpisů upravujících oblast informační bezpečnosti<sup>4</sup>.

---

<sup>3</sup> Vyhláška č. 339/1999 Sb., o objektové bezpečnosti.

<sup>4</sup> Například ISO/IEC 15408 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti informačních technologií, bezpečnostní profil odpovídající úrovni zaručitelnosti bezpečnosti 4.

## § 10

### **Prostředky pro bezpečné vytváření a ověřování elektronického podpisu**

(1) Prostředek pro bezpečné vytváření elektronického podpisu musí mít vlastnosti, které bezprostředně před podepsáním datové zprávy zajistí, aby podepisující osoba

- a) byla informována, že používá tento prostředek, a
- b) zadala přístupové heslo nebo byl uplatněn jiný obdobný autentizační mechanismus.

(2) Prostředek pro bezpečné vytváření a ověřování elektronického podpisu musí

- a) používat kryptografické algoritmy a jejich parametry, které jsou uvedeny v příloze č. 2 této vyhlášky, a
- b) obsahovat komponenty uvedené v příloze č. 3 této vyhlášky.

(3) Prostředky pro bezpečné vytváření a ověřování elektronického podpisu vyžadují dostatečnou záruku bezpečnosti; tento požadavek se považuje za splněný, pokud prostředek odpovídá požadavkům technických předpisů upravujících oblast informační bezpečnosti<sup>5</sup>.

(4) Splnění požadavků na prostředky pro bezpečné vytváření a ověřování elektronického podpisu stanovených v § 17 zákona o elektronickém podpisu se dokládá

- a) hodnocením prostředku pro bezpečné vytváření elektronického podpisu nebo pro bezpečné ověřování elektronického podpisu a seznamem technických předpisů upravujících oblast informační bezpečnosti, podle kterých byl hodnocen, a
- b) podrobným popisem funkce a technickou dokumentací prostředku pro bezpečné vytváření elektronického podpisu nebo pro bezpečné ověřování elektronického podpisu.

## § 11

### **Náležitosti postupu a způsobu vyhodnocování shody**

(1) Úřad vyhodnocuje na základě písemné žádosti shodu nástrojů elektronického podpisu určených pro podepisování vydávaných kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny, s požadavky stanovenými zákonem o elektronickém podpisu.

(2) Žádost podle odstavce 1 musí obsahovat

- a) výsledky obdobných hodnocení nástroje elektronického podpisu podle odstavce 1 a seznam technických předpisů upravujících oblast informační bezpečnosti<sup>6</sup>, podle kterých byl hodnocen, a

---

<sup>5</sup> Například ISO/IEC 15408 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti informačních technologií, bezpečnostní profil odpovídající úrovni zaručitelnosti bezpečnosti 4.

<sup>6</sup> Například Standard pro hodnocení bezpečnosti kryptografických modulů vydaný National institute of standards and technology v USA - FIPS PUB 140-1 úroveň 3.

b) podrobný popis funkce a technickou dokumentaci nástroje elektronického podpisu podle odstavce 1.

(3) Pokud nástroj elektronického podpisu podle odstavce 1 splňuje požadavky stanovené zákonem o elektronickém podpisu a Úřad vysloví shodu, je nástroj považován za bezpečný. Seznam nástrojů, u nichž byla vyslovena shoda, zveřejňuje Úřad ve svém Věstníku.

## § 12

### **Informační audit**

(1) Informační audit je proces objektivního získávání a vyhodnocování poznatků s cílem zjistit míru souladu mezi informacemi popisujícími zkoumané aktivity a požadavky technických předpisů upravujících oblast informační bezpečnosti.

(2) O provedení informačního auditu se vyhotovuje písemná zpráva, která obsahuje

- a) potvrzení, že celková bezpečnostní politika a systémová bezpečnostní politika odpovídají technickým předpisům upravujícím oblast informační bezpečnosti podle § 2 odst. 8,
- b) potvrzení, že systém odpovídá požadavkům technických předpisů upravujících oblast informační bezpečnosti podle § 5 odst. 1, a
- c) seznam dokumentů, které poskytovatel certifikačních služeb vydávající kvalifikované certifikáty předložil při provádění informačního auditu.

(3) Informační audit může provádět fyzická osoba, která má ukončené vysokoškolské vzdělání a má nejméně 5 let odborné praxe v oblasti informační bezpečnosti.

(4) Písemná zpráva podle odstavce 2, která nesmí být starší 6 měsíců, může nahradit podklady požadované v § 9 písm. b).

## § 13

### **Účinnost**

Tato vyhláška nabývá účinnosti dnem vyhlášení.

**Kryptografické algoritmy a jejich parametry****Podpisová schémata**

Podpisové schéma	Asymetrický algoritmus	Minimální parametry asymetrického algoritmu	Algoritmus na generování klíčů	Metoda určená pro padding	Hashovací funkce
001	RSA	MinModLen=1020	rsagen1	emsa-pkcs-v1_5, 2_0, 2_1	SHA1
002	RSA	MinModLen=1020	rsagen1	emsa-pss	SHA1
003	RSA	MinModLen=1020	rsagen1	emsa-pkcs-v1_5, 2_0, 2_1	RIPEMD160
004	RSA	MinModLen=1020	rsagen1	emsa-pss	RIPEMD160
005	DSA	pMinLen=1024 qMinLen=160	dsagen1	-	SHA1
006	ECDSA-F <sub>p</sub>	qMinLen=160 r0Min=10 <sup>4</sup> MinClass=200	ecgen1	-	SHA1
007	ECDSA-F2 <sup>m</sup>	qMinLen=160 r0Min=10 <sup>4</sup> MinClass=200	ecgen1	-	SHA1
008	RSA	MinModLen=1020	rsagen1	emsa-pkcs-v1_5, 2_0, 2_1	MD5
009	RSA	MinModLen=1020	rsagen1	emsa-pss	MD5

**Algoritmy pro generování klíčů**

Označení generátoru klíčů	Používané označení	Asymetrický algoritmus	Metoda generování náhodných čísel	Parametry náhodného generátoru
4.01	rsagen1	RSA	trueran	EntropyBits≥128
4.02	dsagen1	DSA	trueran nebo pseuran (FIPS 186-2)	EntropyBits≥128 nebo SeedLen≥128
4.03	ecgen1	ECDSA-F <sub>p</sub> nebo ECDSA-F2 <sup>m</sup>	trueran nebo pseuran	EntropyBits≥128 nebo SeedLen≥128

**Metody generování náhodných čísel**

Označení náhodného generátoru	Používané jméno	Parametry náhodného generátoru
5.01	trueran	EntropyBits
5.02	pseuran	SeedLen
5.03	FIPS186-2-31	SeedLen
5.04	FIPS186-2-32	SeedLen



## Kryptografické algoritmy a jejich parametry

### Podpisová schémata

Podpisové schéma	Asymetrický algoritmus	Minimální parametry asymetrického algoritmu	Algoritmus na generování klíčů	Metoda určená pro padding	Hashovací funkce
001	RSA	MinModLen=1020	rsagen1	emsa-pkcs-v2_0, 2_1	SHA1
002	RSA	MinModLen=1020	rsagen1	emsa-pss	SHA1
003	RSA	MinModLen=1020	rsagen1	emsa-pkcs-v2_0, 2_1	RIPEMD160
004	RSA	MinModLen=1020	rsagen1	emsa-pss	RIPEMD160
005	DSA	pMinLen=1024 qMinLen=160	dsagen1	-	SHA1
006	ECDSA-F <sub>p</sub>	qMinLen=160 r0Min=10 <sup>4</sup> MinClass=200	ecgen1	-	SHA1
007	ECDSA-F2 <sup>m</sup>	qMinLen=160 r0Min=10 <sup>4</sup> MinClass=200	ecgen1	-	SHA1

### Algoritmy pro generování klíčů

Označení generátoru klíčů	Používané označení	Asymetrický algoritmus	Metoda generování náhodných čísel	Parametry náhodného generátoru
4.01	rsagen1	RSA	trueran	EntropyBits≥128
4.02	dsagen1	DSA	trueran nebo pseuran (FIPS 186-2)	EntropyBits≥128 nebo SeedLen≥128
4.03	ecgen1	ECDSA-F <sub>p</sub> nebo ECDSA-F2 <sup>m</sup>	trueran nebo pseuran	EntropyBits≥128 nebo SeedLen≥128

### Metody generování náhodných čísel

Označení náhodného generátoru	Používané jméno	Parametry náhodného generátoru
5.01	trueran	EntropyBits
5.02	pseuran	SeedLen
5.03	FIPS186-2-31	SeedLen
5.04	FIPS186-2-32	SeedLen

## **Komponenty**

### **1. Komponenty vztahující se k důvěryhodnému prostředí**

#### Komponenta

- a. prohlížení podepsaných datových zpráv
- b. prohlížení atributů elektronického podpisu,
- c. interakce podepisující osoby s prostředkem pro bezpečné vytváření/ověřování elektronického podpisu (interakce pod kontrolou uživatele),
- d. zajišťující způsob a postup autentizace (např. čipová karta s PINem) podepisující osoby na základě autentizujících dat anebo biometrických vlastností,
- e. připravující pro datovou zprávu příslušný otisk,
- f. řídící interakci mezi systémem a prostředkem pro bezpečné vytváření/ověřování elektronického podpisu.

### **2. Komponenty vztahující se k vlastním aplikacím**

#### Komponenta

- a. pro výběr datové zprávy,
- b. pro vlastní vytváření datové zprávy (např. vestavěný textový editor),
- c. zobrazující úplný obsah kvalifikovaného certifikátu podepisující osoby,
- d. vytvářející výstupní normalizované formáty,
- e. používaná pro získání kvalifikovaného certifikátu podepisující osoby,
- f. používaná pro získání časové značky (pokud je používána),
- g. zobrazující jméno vlastníka prostředku pro bezpečné vytváření elektronického podpisu.