V Y H L Á Š K A

Úřadu pro ochranu osobních údajů

ze dne 3. října 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) odhadem dostatečnosti finančních zdrojů a doklady o tom, že disponuje těmito finančními zdroji.

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

(6) 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 (dále jen „informační systém pro certifikační služby“). Systémová bezpečnostní politika obsahuje zejména

a) způsob uplatnění celkové bezpečnostní politiky ve vztahu k informačnímu systému pro certifikační služby,
b) popis vazeb mezi informačním systémem pro certifikační služby a jinými informačními systémy, které provozuje poskytovatel certifikačních služeb vydávající kvalifikované certifikáty,
c) způsob ochrany dat a jiných prvků informačního systému pro certifikační služby,
d) popis bezpečnostních opatření a
e) vyhodnocení analýzy rizik.

(7) Požadavky na celkovou bezpečnostní politiku a systémovou bezpečnostní politiku Úřad zveřejňuje ve Věstníku Úřadu.

(8) 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 nastává zejména v důsledku selhání informačního systému nebo výskytu faktoru, který není pod kontrolou poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty.

(9) Obsahem plánu obnovy je zejména stanovení postupů pro obnovu řádné funkce informačního systému pro certifikační služby.

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

(11) Dostatečností finančních zdrojů je schopnost poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty finančně zabezpečit řádné provozování služeb spojených s elektronickými podpisy i s ohledem na riziko odpovědnosti za škody.

§ 3

Bezpečnost postupu při vydávání kvalifikovaných certifikátů a provozování seznamu kvalifikovaných 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 změna provozního režimu nástroje elektronického podpisu používaného pro podepisování podle odstavce 1 vyžadují, aby je prováděly současně nejméně dvě fyzické osoby, které jsou pro tuto činnost určeny poskytovatelem certifikačních služeb vydávajícím kvalifikované certifikáty.

(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 pro jiné účely.

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

(6) Seznam kvalifikovaných certifikátů, které byly zneplatněny, je provozován tak, aby jeho dostupnost byla zajištěna nejméně dvěma na sobě nezávislými způsoby, které umožňují dálkový přístup a jsou nepřetržitě dostupné.

(7) Doba mezi ukončením platnosti kvalifikovaného certifikátu a zveřejněním údaje o ukončení této platnosti v seznamu kvalifikovaných certifikátů, které byly zneplatněny, může činit nejvýše 12 hodin. Tento údaj obsahuje číslo kvalifikovaného certifikátu unikátní u poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty, datum a čas s uvedením hodiny, minuty a sekundy, od kdy byl kvalifikovaný certifikát zneplatněn.

§ 4

Bezpečnost informačního systému pro certifikační služby

(1) Používaný informační systém pro certifikační služby se považuje za bezpečný, pokud u dat, která zpracovává, je zajištěna důvěrnost, integrita, dostupnost a prokazatelnost jejich původu a pokud odpovídá požadavkům technické normy upravující oblast informační bezpečnosti. [1)]

(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 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

[1)] ČSN ISO/IEC 15408 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti informačních technologií, bezpečnostní profil odpovídající úrovni zaručitelnosti bezpečnosti 4.

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 celého životního cyklu tohoto certifikátu.

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

(4) Prostory, kde dochází k činnosti podle odstavců 1 až 3 a podle § 5 odst. 1, musí být zabezpečeny obdobně jako objekty kategorie „D“ podle zvláštního právního předpisu. [2)]

(5) Za účelem doložení bezpečnosti postupů podle § 6 odst. 1 písm. j) a k) zákona o elektronickém podpisu poskytovatel certifikačních služeb vydávající kvalifikované certifikáty pořizuje písemné záznamy o tom, že osoby jím určené k zajišťování služeb spojených s elektronickými podpisy jsou

a) seznamovány v potřebném rozsahu s dokumenty uvedenými v § 2 odst. 1 písm. a) až e) a
b) proškolovány tak, aby jejich odborné předpoklady odpovídaly vykonávané činnosti.

§ 5

Bezpečnost postupu při nakládání s párovými daty poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty

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

a) výhradně fyzickými osobami, které jsou pro tuto činnost určeny poskytovatelem certifikačních služeb vydávajícím kvalifikované certifikáty,
b) podle postupů stanovených certifikační prováděcí směrnicí a
c) v souladu se systémovou bezpečnostní politikou.

(2) Při vytváření párových dat poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty musí být použity kryptografické algoritmy a jejich parametry, které jsou uvedeny 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 pořizuje zápis, který obsahuje

a) popis způsobu zničení dat,
b) datum zničení dat,
c) datum pořízení zápisu a
d) jméno, příjmení a podpis osoby určené poskytovatelem certifikačních služeb vydávajícím kvalifikované certifikáty k tomu, aby zničení dat zajistila.

(4) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty v případě neoprávněného použití nebo vzniku důvodné obavy ze zneužití svých dat pro vytváření elektronického podpisu užívaných pro podepisování vydávaných kvalifikovaných certifikátů

[2)] Vyhláška č. 339/1999 Sb., o objektové bezpečnosti.

a pro podepisování seznamu kvalifikovaných certifikátů, které byly zneplatněny, je bezodkladně povinen

a) ukončit platnost svého kvalifikovaného certifikátu, který byl k těmto datům vydán,
b) ukončit platnost kvalifikovaných certifikátů, které byly těmito daty podepsány,
c) zpřístupnit informaci o ukončení platnosti svého kvalifikovaného certifikátu s uvedením důvodu ukončení platnosti, a to nejméně dvěma na sobě nezávislými způsoby, které umožňují dálkový přístup a jsou nepřetržitě dostupné, a
d) informovat osoby, které byly dotčeny ukončením platnosti kvalifikovaného certifikátu podle písmene a) o ukončení platnosti jejich kvalifikovaných certifikátů vydaných tímto poskytovatelem certifikačních služeb. V informaci musí být uveden důvod ukončení platnosti kvalifikovaného certifikátu podle písmene a).

§ 6

Ověření bezpečnosti používání informačního systému pro certifikační služby a zajištění dostatečné bezpečnosti postupů, které tento systém podporují

Požadavek na bezpečnost používání informačního systému pro certifikační služby 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),
b) výsledkem hodnocení, podle něhož jsou splněny požadavky technické normy upravující oblast informační bezpečnosti, [1)] a
c) písemným posudkem, jehož součástí je potvrzení, že podle kontroly bezpečnostní shody, která byla provedena podle technické normy upravující oblast informační bezpečnosti, [3)] je používání informačního systému pro certifikační služby v souladu se způsoby zajištění bezpečnosti stanovenými v dokumentech uvedených v § 2 odst. 1 písm. c) a d). Kontrola bezpečnostní shody musí být prováděna opakovaně, a to vždy nejpozději do 12 měsíců od provedení poslední kontroly bezpečnostní shody.

§ 7

Prostředky pro bezpečné vytváření a ověřování zaručeného elektronického podpisu

(1) Prostředek pro bezpečné vytváření zaručeného 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 zaručeného elektronického podpisu musí používat kryptografické algoritmy a jejich parametry, které jsou uvedeny v příloze č. 2 této vyhlášky.

(3) Prostředek pro bezpečné vytváření zaručeného elektronického podpisu vyžaduje dostatečnou záruku bezpečnosti; tento požadavek se považuje za splněný, pokud prostředek odpovídá požadavkům technické normy upravující oblast informační bezpečnosti. [1)]

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

[3)] ČSN ISO/IEC TR 13335 Informační technologie - Směrnice pro řízení bezpečnosti IT 1 - 3.

a) výsledkem hodnocení prostředku pro bezpečné vytváření zaručeného elektronického podpisu a seznamem technických norem upravujících oblast informační bezpečnosti, podle kterých byl hodnocen, a
b) podrobným popisem funkce a technickou dokumentací prostředku pro bezpečné vytváření zaručeného elektronického podpisu.

(5) Požadavky uvedené v odstavcích 2 až 4 musí splňovat rovněž prostředek pro bezpečné ověřování zaručeného elektronického podpisu.

§ 8

Náležitosti postupu a způsobu vyhodnocování shody nástrojů elektronického podpisu

(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) podrobný popis funkce a technickou dokumentaci nástroje elektronického podpisu podle odstavce 1 a
b) výsledek hodnocení kryptografických funkcí, které používá nástroj elektronického podpisu podle odstavce 1 a které musí odpovídat požadavkům Úřadu na kryptografické moduly. Tyto požadavky Úřad zveřejňuje ve Věstníku Úřadu. Toto hodnocení zajišťuje zpravidla dodavatel příslušného nástroje elektronického podpisu.

(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 Věstníku Úřadu.

§ 9

Účinnost

Tato vyhláška nabývá účinnosti dnem vyhlášení.

Předseda:

RNDr. **Neuwirt** v. r.

Příloha č. 1 k vyhlášce č. .../... Sb.

Kryptografické algoritmy a jejich parametry pro data pro vytváření elektronického podpisu a jim odpovídající data pro ověřování elektronického podpisu, která si vytváří osoba žádající o vydání kvalifikovaného certifikátu, a k nimž má být vydán kvalifikovaný certifikát

Podpisové schéma	Asymetrický algoritmus	Minimální parametry asymetrického algoritmu	Metoda určená pro padding	Hašovací funkce
001	RSA	MinModLen=1020	emsa-pkcs #1-v1.5	SHA1
002	RSA	MinModLen=1020	emsa-pss	SHA1
003	RSA	MinModLen=1020	emsa-pkcs #1-v1.5	RIPEMD160
004	RSA	MinModLen=1020	emsa-pss	RIPEMD160
005	DSA	pMinLen=1024 qMinLen=160	-	SHA1
006	ECDSA-F_p	qMinLen=160 r0Min=10^4 MinClass=200	-	SHA1
007	ECDSA-$F2^m$	qMinLen=160 r0Min=10^4 MinClass=200	-	SHA1
008	RSA	MinModLen=1020	emsa-pkcs #1-v1.5	MD5
009	RSA	MinModLen=1020	emsa-pss	MD5

Příloha č. 2 k vyhlášce č. .../... Sb.

Kryptografické algoritmy a jejich parametry pro vytváření párových dat poskytovatele a pro prostředky pro bezpečné vytváření a ověřování zaručeného elektronického podpisu

Podpisová schémata

Podpisové schéma	Asymetrický algoritmus	Minimální parametry asymetrického algoritmu	Algoritmus pro generování klíčů	Metoda určená pro padding	Hašovací funkce
001	RSA	MinModLen=1020	rsagen1	emsa-pkcs #1-v1.5	SHA1
002	RSA	MinModLen=1020	rsagen1	emsa-pss	SHA1
003	RSA	MinModLen=1020	rsagen1	emsa-pkcs #1-v1.5	RIPEMD160
004	RSA	MinModLen=1020	rsagen1	emsa-pss	RIPEMD160
005	DSA	pMinLen=1024 qMinLen=160	dsagen1	-	SHA1
006	ECDSA-F_p	qMinLen=160 r0Min=10^4 MinClass=200	ecgen1	-	SHA1
007	ECDSA-$F2^m$	qMinLen=160 r0Min=10^4 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_p nebo ECDSA-$F2^m$	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	FIPS 186-2-31	SeedLen
5.04	FIPS 186-2-32	SeedLen