

525

VYHLÁŠKA

ze dne 14. prosince 2005

o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací

Národní bezpečnostní úřad stanoví podle § 53 písm. a), b), c), d), g), h) a j) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, (dále jen „zákon“):

§ 1

Náležitosti žádosti o certifikaci kryptografického prostředku
(K § 49 odst. 1 zákona)

(1) Žádost o certifikaci kryptografického prostředku obsahuje

- a) identifikaci žadatele
 1. obchodní firmou, popřípadě názvem, sídlem a identifikačním číslem, je-li žadatelem právnická osoba,
 2. obchodní firmou, popřípadě jménem a příjmením, případně odlišujícím dodatkem, trvalým pobytem a místem podnikání, liší-li se od trvalého pobytu, datem narození a identifikačním číslem, je-li žadatelem fyzická osoba, která je podnikatelem, nebo
 3. názvem, sídlem, identifikačním číslem a jménem a příjmením odpovědné osoby, jde-li o orgán státu,
- b) jméno a příjmení kontaktního zaměstnance žadatele a kontaktní spojení na něj,
- c) číslo platného osvědčení podnikatele a stupeň utajení utajované informace, pro přístup k níž osvědčení podnikatele opravňuje, je-li žadatelem podnikatel,
- d) obchodní název a úplné typové označení kryptografického prostředku,
- e) určení kryptografického prostředku (účel užití a stupeň utajení, pro který má být kryptografický prostředek používán),
- f) obchodní firmu, sídlo či místo podnikání výrobce kryptografického prostředku,
- g) způsob zajištění výroby a distribuce klíčového materiálu.

(2) K certifikaci kryptografického prostředku Evropské unie nebo některého jejího členského státu anebo Organizace Severoatlantické smlouvy, který je určen k ochraně utajovaných informací, žadatel předkládá žádost podle odstavce 1 a kopii certifikátu nebo obdobného dokumentu vydaného certifikačním orgánem Evropské unie nebo příslušným národním certifikačním orgánem jejího členského státu anebo Organizací Severoatlantické smlouvy.

§ 2

Náležitosti žádosti o certifikaci kryptografického pracoviště
(K § 50 odst. 1 zákona)

Žádost o certifikaci kryptografického pracoviště obsahuje

- a) identifikaci žadatele podle § 1 odst. 1 písm. a),
- b) jméno a příjmení kontaktního zaměstnance žadatele a kontaktní spojení na něj,
- c) číslo platného osvědčení podnikatele a stupeň utajení utajované informace, pro přístup k níž osvědčení podnikatele opravňuje, je-li žadatelem podnikatel,
- d) identifikaci kryptografického pracoviště (název, adresa a umístění),
- e) určení kryptografického pracoviště (účel užití),
- f) seznam příkládané dokumentace nezbytné k provedení certifikace kryptografického pracoviště.

§ 3

Náležitosti opakované žádosti o certifikaci kryptografického prostředku
(K § 49 zákona)

Opakovaná žádost o certifikaci kryptografického prostředku obsahuje

- a) identifikaci žadatele podle § 1 odst. 1 písm. a),
- b) úplnou identifikaci vydaného certifikátu (držitel certifikátu, evidenční číslo, datum vydání, doba platnosti),
- c) identifikaci certifikovaného kryptografického prostředku (obchodní název, typové označení, variantní provedení, určení, název a sídlo výrobce kryptografického prostředku),
- d) jméno a příjmení kontaktního zaměstnance žadatele a kontaktní spojení na něj,
- e) odůvodnění opakované žádosti.

§ 4

Náležitosti opakované žádosti o certifikaci kryptografického pracoviště
(K § 50 zákona)

Opakovaná žádost o certifikaci kryptografického pracoviště obsahuje

- a) identifikaci žadatele podle § 1 odst. 1 písm. a),
- b) úplnou identifikaci vydaného certifikátu (držitel certifikátu, evidenční číslo, název kryptografického pracoviště, datum vydání, doba platnosti),
- c) identifikaci kryptografického pracoviště (podrobná specifikace určení a umístění pracoviště),
- d) odůvodnění opakované žádosti.

§ 5

Dokumentace nezbytná k provedení certifikace kryptografického prostředku

(K § 49 zákona)

(1) K provedení certifikace kryptografického prostředku se v jejím průběhu předkládá kryptografický prostředek, dokumentace a ostatní podklady nezbytné pro její provedení.

(2) Seznam dokumentace a ostatních podkladů, jejich formu a obsah stanovuje bezpečnostní standard, který Národní bezpečnostní Úřad (dále jen „Úřad“) poskytne žadateli. Časový plán předložení dokumentace a ostatních podkladů nezbytných pro provedení certifikace poskytne Úřad žadateli.

(3) Pro provedení certifikace kryptografického prostředku je zejména požadována dokumentace obsahující

- a) určení a vymezení způsobu použití kryptografického prostředku,
- b) typ uživatelského prostředí a systémové začlenění kryptografického prostředku,
- c) technický popis a návod k obsluze kryptografického prostředku,
- d) požadavky na instalaci a testování kryptografického prostředku,
- e) platná osvědčení kryptografického prostředku nebo již vydané certifikáty,
- f) popis řešení a struktury použitých kryptografických klíčů,
- g) blokové schéma a popis kryptografického prostředku s vyznačením součinnostních vazeb jednotlivých jeho částí.

(4) Úřad po skončení certifikace vrátí navrhovateli poskytnutý kryptografický prostředek, technické prostředky, materiály a originální technickou dokumentaci kryptografického prostředku. Ostatní podklady předložené k certifikaci se žadateli o certifikaci nevracejí.

§ 6

Dokumentace nezbytná k provedení certifikace kryptografického pracoviště

(K § 50 zákona)

(1) K žádosti o certifikaci kryptografického pracoviště se přikládá

- a) dokumentace zabezpečení fyzické bezpečnosti kryptografického pracoviště, v rozsahu stanoveném ve zvláštním právním předpisu¹⁾,
- b) dokumentace provozně-bezpečnostního zabezpečení kryptografického pracoviště,
- c) prohlášení odpovědné osoby nebo jí pověřené osoby o splnění požadavků na fyzickou a personální bezpečnost kryptografického pracoviště.

(2) Dokumentace přiložená k žádosti o certifikaci a případně další vyžádané doplňující podklady potřebné k provedení certifikace se žadateli nevracejí.

§ 7

Vzor certifikátu kryptografického prostředku a obsah certifikační zprávy

(K § 46 odst. 7 a 13 zákona)

(1) Vzor certifikátu kryptografického prostředku je uveden v příloze č. 1 k této vyhlášce.

(2) Přílohou certifikátu kryptografického prostředku je certifikační zpráva, která obsahuje

- a) požadavky na výrobu, dopravu a servis kryptografického prostředku,
- b) specifikaci kryptografického prostředku,
- c) výsledky certifikačního řízení,
- d) ekvivalentní hodnotu parametru S1 podle zvláštního právního předpisu¹⁾,
- e) podmínky provozování kryptografického prostředku,
- f) případná omezení podmiňující platnost certifikátu kryptografického prostředku.

§ 8

Vzor certifikátu kryptografického pracoviště a obsah certifikační zprávy

(K § 46 odst. 8 a 13 zákona)

(1) Vzor certifikátu kryptografického pracoviště je uveden v příloze č. 2 k této vyhlášce.

(2) Přílohou certifikátu kryptografického pracoviště je certifikační zpráva, která obsahuje

- a) jednoznačné určení kryptografického pracoviště,
- b) podmínky provozování kryptografického pracoviště,
- c) rozsah případných změn, které podmiňují platnost certifikátu kryptografického pracoviště.

¹⁾ Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

§ 9

Způsob a podmínky provádění certifikace kryptografického prostředku

(K § 49 zákona)

(1) Úřad stanovuje pořadí, ve kterém je prováděna certifikace kryptografických prostředků, její rozsah a způsob provedení.

(2) Certifikace kryptografického prostředku je rozdělena do samostatně uzavíraných etap, které provádí odborná pracoviště Úřadu, odborné pracoviště orgánů státu, právnické osoby, nebo podnikající fyzické osoby. Na základě výsledků hodnocení etap vydá Úřad rozhodnutí. Samostatně jsou hodnoceny

- a) předložená žádost o certifikaci kryptografického prostředku, kryptografický prostředek a přiložená dokumentace,
- b) kryptologické parametry kryptografického prostředku,
- c) technické parametry kryptografického prostředku,
- d) výroba klíčových materiálů a jejich distribuce,
- e) požadavky na výrobu, provozování a ochranu kryptografického prostředku,
- f) požadavky na začlenění kryptografického prostředku do komunikačního nebo informačního systému,
- g) použitelnost pro ochranu utajovaných informací České republiky, Evropské unie, nebo Organizace Severoatlantické smlouvy.

(3) Úřad vede evidenci certifikovaných kryptografických prostředků. K certifikovanému kryptografickému prostředku se vede certifikační spis, do kterého se zakládá žádost o provedení certifikace, dokumentace a ostatní podklady poskytnuté žadatelem, další vyžádané doplňující podklady potřebné k provedení certifikace, certifikační zpráva a kopie vydaného certifikátu.

(4) Skartační lhůta certifikačního spisu začíná běžet uplynutím doby platnosti certifikátu.

(5) Pro certifikaci kryptografického prostředku prováděnou na základě opakované žádosti podle § 3 platí odstavce 1 až 4 obdobně.

§ 10

Způsob a podmínky provádění certifikace kryptografického pracoviště

(K § 50 zákona)

(1) Úřad stanovuje pořadí, ve kterém je prováděna certifikace kryptografických pracovišť, její rozsah

a způsob provedení.

(2) Certifikace kryptografického pracoviště je rozdělena do samostatně uzavíraných etap, které provádí odborná pracoviště Úřadu, odborné pracoviště orgánů státu, právnické osoby, nebo podnikající fyzické osoby. Na základě výsledků hodnocení etap vydá Úřad rozhodnutí. Samostatně jsou hodnoceny

- a) předložená žádost o certifikaci kryptografického pracoviště a předložená dokumentace,
- b) účel kryptografického pracoviště a jeho technické vybavení,
- c) provozně-bezpečnostní zabezpečení kryptografického pracoviště,
- d) splnění požadavků na fyzickou a personální bezpečnost kryptografického pracoviště,
- e) výsledek kontroly kryptografického pracoviště ze strany Úřadu.

(3) Úřad vede evidenci certifikovaných kryptografických pracovišť. K certifikovanému kryptografickému pracovišti se vede certifikační spis, do kterého se zakládá žádost o certifikaci, dokumentace a ostatní podklady poskytnuté žadatelem, další vyžádané doplňující podklady potřebné k provedení certifikace, certifikační zpráva a kopie vydaného certifikátu.

(4) Skartační lhůta certifikačního spisu začíná běžet uplynutím doby platnosti certifikátu kryptografického pracoviště.

(5) Pro certifikaci kryptografického pracoviště prováděnou na základě opakované žádosti podle § 4 platí odstavce 1 až 4 obdobně.

§ 11

Náležitosti žádosti orgánu státu nebo podnikatele o uzavření smlouvy o zajištění činnosti

(K § 52 zákona)

(1) Žádost o uzavření smlouvy o zajištění činnosti²⁾ obsahuje

- a) identifikaci žadatele podle § 1 odst. 1 písm. a),
- b) číslo platného osvědčení podnikatele a stupeň utajení utajované informace, pro přístup k níž osvědčení podnikatele opravňuje, je-li žadatelem podnikatel,
- c) jméno a příjmení kontaktního zaměstnance žadatele a kontaktní spojení na něj,
- d) rozsah přikládání dokumentace.

(2) K žádosti podle odstavce 1 se přikládá dokumentace obsahující

²⁾ § 46 odst. 15 a § 52 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

- a) adresu umístění pracoviště provádějícího požadované činnosti,
- b) prohlášení odpovědné osoby nebo jí pověřené osoby o splnění požadavků na fyzickou a personální bezpečnost pracoviště,
- c) rozsah požadovaných činností,
- d) personální zabezpečení požadovaných činností,
- e) technické a organizační zajištění požadovaných činností.

§ 12

Účinnost

Tato vyhláška nabývá účinnosti dnem 1. ledna 2006.

Ředitel:

Mgr. Mareš v. r.