Ročník 1999

SBÍRKA ZÁKONŮ
ČESKÉ REPUBLIKY

Částka 29 **Rozeslána dne 27. dubna 1999** **Cena Kč 12,90**

O B S A H:

76

VYHLÁŠKA

Národního bezpečnostního úřadu

ze dne 14. dubna 1999

o zajištění kryptografické ochrany utajovaných skutečností, provádění certifikace kyptografických prostředků a náležitostech certifikátu

Národní bezpečnostní úřad (dále jen „Úřad“) stanoví podle § 52 odst. 5 a § 53 odst. 3 zákona č. 148/ /1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, (dále jen „zákon“):

§ 1

Předmět úpravy

Tato vyhláška stanoví způsoby použití, nasazování a evidence kryptografických prostředků používaných k ochraně utajovaných skutečností (dále jen „kryptografický prostředek“), používání klíčových materiálů, zjišťování odborné způsobilosti pracovníků kryptografické ochrany utajovaných skutečností, postup a způsob certifikačního procesu kryptografických prostředků a náležitosti certifikátu.

§ 2

Pro účely této vyhlášky se rozumí

a) informací znalost, kterou je možné jakoukoliv formou sdělovat,

b) utajovanou informací informace, která je klasifikována stupněm utajení,

c) kryptografií vědní disciplína, která rozvíjí a aplikuje matematické a fyzikální principy pro tvorbu metod a prostředků k ochraně informací za účelem jejich skrytí před nepovolanou osobou, zajištění jejich autentičnosti, zabránění jejich modifikaci, odmítnutí nebo neoprávněnému použití, (dále jen „ochrana informací“),

d) klíčovými materiály souhrn kryptografických klíčů určených pro kryptografický prostředek,

e) kryptografickými prostředky zařízení, předměty, programy nebo kryptografické postupy, včetně kryptografických klíčů, které zajišťují ochranu informací,

f) kryptografickým klíčem specifická informace použitá spolu s kryptografickým prostředkem k ochraně informací,

g) autentizací proces potvrzení, a tím i ustavení identity uživatele, procesu nebo jiného prvku s požadovanou mírou záruky,

h) identifikačními prostředky prostředky nebo systémy sloužící k prokazování identity fyzické osoby, zejména průkazy totožnosti, optické snímače, biometrické snímače a systémy, digitální podpis a magnetické, čipové nebo bezkontaktní karty,

i) auditem bezpečnostní proces zajišťující spolu s identifikací a autentizací uživatele, že uživatel je individuálně odpovědný za svou činnost při nakládání s utajovanými skutečnostmi,

j) nosičem informací prvek schopný uchovávat informaci,

k) kompromitací případ neoprávněného nakládání s utajovanými skutečnostmi, který svými následky může způsobit porušení ochrany utajované skutečnosti při použití kryptografického prostředku,

l) kryptograficky významným prvkem prostředek, vlastnost nebo metoda podílející se na kvalitě ochrany utajovaných skutečností, zejména kryptografický algoritmus a kryptografický klíč, generátor počátečních nastavení nebo nosič kryptografických klíčů,

m) subsystémem kryptografického prostředku zařízení používané bezprostředně s kryptografickým prostředkem a umožňující jeho požadovanou činnost v rámci systému sloužícího k ochraně utajovaných skutečností a jehož hodnocení je součástí certifikace kryptografického prostředku,

n) kompromitujícím vyzařováním takové vyzařování, zejména elektrické, elektromagnetické, optické a akustické, které svým výskytem může způsobit únik utajovaných skutečností,

o) bezpečnostním standardem zvláštní právní předpis, jehož obsah je shodný s mezinárodní technickou normou, směrnicí nebo standardem a českou státní normou nebo specifikací vydanou mezinárodní organizací a který stanoví postupy, pokyny, technická řešení, bezpečnostní parametry a organizační opatření na ochranu utajovaných skutečností.

§ 3

Používání a nasazování kryptografických prostředků

(1) Pro kryptografickou ochranu utajované skutečnosti lze použít jen takový kryptografický prostředek, který byl certifikován Úřadem pro stupeň utajení shodný se stupněm utajení utajované skutečnosti nebo pro stupeň utajení vyšší.

(2) Nasazení kryptografického prostředku a jeho použití se provádí v souladu s bezpečnostními standardy vydanými podle § 8 odst. 1 písm. o) zákona.

(3) V informačním systému, který zpracovává, přenáší, ukládá nebo archivuje (dále jen „nakládá“) utajované skutečnosti klasifikované do různých stupňů utajení, musí být použit kryptografický prostředek, který je certifikován Úřadem pro stupeň utajení shodný s nejvyšším stupněm utajení utajované skutečnosti, se kterým informační systém nakládá, nebo pro stupeň utajení vyšší.

(4) Za bezchybný stav a správné použití kryptografického prostředku odpovídá pracovník kryptografické ochrany utajovaných skutečností.

(5) Úřad zajišťuje používání kryptografické ochrany utajovaných informací Severoatlantické aliance v informačních systémech.

(6) Údaje o provozu nasazeného kryptografického prostředku, který je certifikován pro stupeň utajení „Přísně tajné“ nebo „Tajné“, se vedou v „Knize provozu kryptografického prostředku“.

§ 4

Klíčové materiály

(1) Klíčové materiály tvoří součást kryptografického prostředku. Způsob manipulace s klíčovými materiály stanoví bezpečnostní standardy.

(2) Nezabezpečené klíčové materiály, materiály bez technické nebo kryptografické ochrany se klasifikují stupněm utajení, který je shodný se stupněm utajení utajované skutečnosti, k jejíž ochraně jsou klíčové materiály určeny, nebo stupněm utajení vyšším.

(3) Zabezpečené klíčové materiály, materiály s technickou nebo kryptografickou ochranou se klasifikují stupněm utajení, který je shodný se stupněm utajení utajované skutečnosti, k jejíž ochraně jsou klíčové materiály určeny, nebo stupněm utajení nižším.

(4) Výroba klíčových materiálů, jejich distribuce a ničení nepoužitých klíčových materiálů se řídí bezpečnostními standardy.

(5) Nepoužité klíčové materiály přidělené Úřadem orgánu státu nebo organizaci musí být vráceny zpět Úřadu, pokud z bezpečnostních standardů nevyplývá jiný postup.

(6) Úřad zajišťuje používání a distribuci klíčových materiálů Severoatlantické aliance.

§ 5

Opatření při kompromitaci

(1) Zjistí-li statutární orgán, že došlo ke kompromitaci, oznámí tuto skutečnost neprodleně písemně Úřadu.

(2) V případě kompromitace je statutární orgán povinen k zajištění ochrany utajovaných skutečností chráněných kryptografickými prostředky neprodleně přijmout zejména tato opatření:

a) zabránit dalšímu používání kompromitovaných klíčových materiálů, kryptografických prostředků, systémů (dále jen „kompromitované prostředky“),

b) zabezpečit ochranu utajovaných skutečností jinými nekompromitovanými kryptografickými prostředky, pokud jsou k dispozici; pokud takto nelze zabezpečit ochranu utajovaných skutečností, je nezbytné použít jiných prostředků k této ochraně uvedených v § 47 až 51 zákona,

c) v případě, že se jedná o utajované skutečnosti uložené v systému zapojeném do počítačové nebo komunikační sítě, zajistit její fyzické odpojení od komunikačních prostředků,

d) zdokumentovat všechny okolnosti předcházející zjištěné kompromitaci a rovněž okolnosti bezprostředně následující, včetně soupisu osob přicházejících do styku s kompromitovaným prostředkem.

§ 6

Pracovníci kryptografické ochrany utajovaných skutečností

(1) Pracovník kryptografické ochrany utajovaných skutečností musí být určenou osobou minimálně pro ten stupeň utajení, pro který je certifikován kryptografický prostředek, se kterým tento pracovník jako obsluha pracuje.

(2) Pracovníkem kryptografické ochrany utajovaných skutečností je operátor, speciální obsluha a auditor, jejichž činnost stanoví bezpečnostní standardy.

§ 7

Odborná způsobilost pracovníků kryptografické ochrany

(1) Úřad nebo jím pověřená organizace zajišťuje přípravu odborné způsobilosti pracovníků kryptografické ochrany.

(2) Odbornou způsobilost pracovníků kryptografické ochrany pro stupně utajení „Vyhrazené“, „Důvěrné“ a „Tajné“ ověřuje Úřad nebo jím pověřená organizace. Odbornou způsobilost pracovníků kryptografické ochrany pro stupeň utajení „Přísně tajné“ ověřuje Úřad.

(3) Pracovníku, který prokáže odbornou způsobilost, vydá Úřad potvrzení o odborné způsobilosti pracovníka kryptografické ochrany utajovaných skutečností, jehož vzor je uveden v příloze č. 1.

(4) Doba platnosti potvrzení o odborné způsobilosti pracovníka kryptografické ochrany utajovaných skutečností je pro stupeň utajení „Vyhrazené“ 6 let

a pro stupeň utajení „Důvěrné“, „Tajné“ nebo „Přísně tajné“ 5 let.

(5) Platnost potvrzení o odborné způsobilosti pracovníka kryptografické ochrany utajovaných skutečností zaniká

a) uplynutím doby platnosti podle odstavce 6, nebo

b) zánikem platnosti vydaného osvědčení.[1])

§ 8

Požadavky k certifikaci kryptografických prostředků

(1) Úřad stanovuje bezpečnostními standardy kritéria certifikace, požadavky na systémy opatření tvořící kryptografickou ochranu utajovaných skutečností a na kryptografické prostředky, které mohou být použity k zajištění kryptografické ochrany pro jednotlivé stupně utajení utajovaných skutečností.

(2) Kryptografické prostředky musí používat kryptografické algoritmy stanovené bezpečnostními standardy a mezinárodními standardy schválenými Úřadem nebo algoritmy vyvinuté Úřadem.

(3) Systém opatření tvořící kryptografickou ochranu utajovaných skutečností musí zabezpečit utajované skutečnosti před únikem a neoprávněným nakládáním. Systém opatření je nutné aplikovat i na jejich subsystémy.

(4) Kryptografické prostředky používané pro ochranu utajovaných skutečností a jejich subsystémy zpracovávající utajované skutečnosti v otevřeném, tj. nezašifrovaném tvaru nebo nakládající s kryptograficky významnými prvky, musí být odolné proti kompromitaci vlivem kompromitujícího vyzařování.

(5) Odolnost ochrany je ověřována podle bezpečnostních standardů a je odstupňována podle stupně utajení chráněných utajovaných skutečností.

§ 9

Postup a způsob certifikace kryptografického prostředku

(1) O provedení certifikace kryptografického prostředku pro požadovaný stupeň utajení utajovaných skutečností jsou oprávněni požádat

a) orgán státu,

b) organizace, které bylo pro tento stupeň utajení utajovaných skutečností vydáno potvrzení,

c) fyzická osoba, která byla pro tento stupeň utajovaných skutečností určena.

(2) Certifikace kryptografického prostředku se provádí na základě žádosti. Vzor žádosti o certifikaci kryptografického prostředku je uveden v příloze č. 3.

(3) K žádosti o certifikaci kryptografického prostředku se přikládají

a) vydané certifikáty jiných autorizovaných zkušeben, včetně výsledků měřících protokolů, a seznam norem, kterým kryptografický prostředek vyhověl,

b) potřebný počet kusů kryptografického prostředku k provedení jeho certifikace a v případě potřeby provedení jejich instalace v podmínkách certifikačního pracoviště nebo provedení úvodního seznámení s kryptografickým prostředkem.

(4) V závislosti na určení použití kryptografického prostředku se k žádosti o jeho certifikaci dále přikládá

a) pro stupeň utajení „Vyhrazené“ dokumentace uvedená v příloze č. 2 odst. 1,

b) pro stupeň utajení „Důvěrné“ dokumentace uvedená v příloze č. 2 odst. 2,

c) pro stupeň utajení „Tajné“ dokumentace uvedená v příloze č. 2 odst. 3,

d) pro stupeň utajení „Přísně tajné“ dokumentace uvedená v příloze č. 2 odst. 4.

(5) Úřad si v případě potřeby může dále vyžádat

a) další doplňující podklady nebo údaje potřebné k provedení certifikace kryptografického prostředku,

b) seznámení svého hodnotitelského týmu s kryptografickým prostředkem, a to zejména s instalací, parametry, pravidly používání, použitými kryptografickými klíči a klíčovým hospodářstvím,

c) poskytnutí možnosti využít uživatelského prostředí žadatele o certifikaci, ve kterém bude kryptografický prostředek používán, za účelem posouzení vlivu tohoto prostředí na bezpečnostní požadavky ochrany utajovaných skutečností,

d) doložení úrovně bezpečnostních opatření při výzkumu, vývoji, výrobě a distribuci certifikovaného prostředku a klíčového hospodářství.

(6) Úřad převezme žádost o certifikaci kryptografického prostředku, zkontroluje úplnost dokumentace přiložené podle odstavců 3 a 4 a potvrdí převzetí potřebného počtu kusů kryptografického prostředku. V případě zjištění nedostatků v úplnosti dokumentace přiložené podle odstavců 3 a 4 vyzve Úřad žadatele, aby ve stanoveném termínu nedostatky odstranil. Neodstraní-li žadatel vytčené nedostatky, Úřad certifikaci neprovede a žádost, včetně všech podkladů a krypto-

[1]) § 37 zákona č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů.

grafických prostředků, vrátí žadateli. Na tento důsledek musí být žadatel upozorněn.

(7) Bude-li k provedení certifikace potřebné předložit další podklady nebo zabezpečit činnosti uvedené v odstavci 5, vyzve Úřad žadatele o předložení podkladů nebo zabezpečení činností ve stanoveném termínu. Nepředloží-li žadatel požadované podklady nebo nezabezpečí-li požadované činnosti, Úřad v certifikaci nepokračuje a žádost, včetně všech podkladů a kryptografických prostředků, vrátí žadateli. Na tento důsledek musí být žadatel ve výzvě upozorněn.

(8) Hodnocení kryptografického prostředku se provádí posouzením podkladů předložených žadatelem a ověřením shody zjištěných parametrů kryptografického prostředku s bezpečnostními standardy.

(9) Na základě výsledků hodnocení Úřad posoudí způsobilost kryptografického prostředku k ochraně utajovaných skutečností. Zjistí-li Úřad shodu hodnoceného kryptografického prostředku s bezpečnostními standardy, schválí jeho způsobilost a vydá žadateli certifikát. Vzor certifikátu kryptografického prostředku je uveden v příloze č. 4.

(10) Nesplňuje-li hodnocený kryptografický prostředek způsobilost pro požadovaný stupeň utajení a zjistí-li Úřad jeho shodu s bezpečnostními standardy pro nižší než požadovaný stupeň utajení, vydá Úřad certifikát pro tento nižší stupeň utajení.

(11) Uznat certifikát kryptografického prostředku potvrzující ověření a schválení způsobilosti pro ochranu utajovaných skutečností vydaný cizí mocí lze, pouze pokud tak stanoví mezinárodní smlouva, kterou je Česká republika vázána, nebo na základě vzájemnosti a shody hodnotících kritérií. Ve Věstníku Úřadu se uveřejní seznam certifikačních pracovišť cizí moci, jejichž certifikát kryptografického prostředku lze uznat, a seznam kryptografických prostředků certifikovaných cizí mocí, jejichž certifikát byl uznán Úřadem.

(12) Ve Věstníku Úřadu se uveřejní seznam certifikovaných technických prostředků pro jednotlivé stupně utajení s uvedením doby platnosti certifikátu.

(13) Úřad po skončení certifikace vrátí žadateli o certifikaci pouze jím předložené kryptografické prostředky. Žádost o certifikaci kryptografického prostředku, dokumentaci přiloženou k žádosti podle odstavce 3 a další doplňující podklady a údaje potřebné k provedení certifikace vyžádané podle odstavce 5 se žadateli o certifikaci nevracejí a zůstávají součástí certifikačního spisu.

(14) Doba platnosti certifikátu kryptografického prostředku vydaného Úřadem je

a) pro stupeň utajení „Vyhrazené“ 6 let,
b) pro stupně utajení „Důvěrné“, „Tajné“ nebo „Přísně tajné“ 5 let.

(15) Platnost certifikátu kryptografického prostředku zaniká uplynutím doby jeho platnosti nebo rozhodnutím Úřadu v případě, že kryptografický prostředek pozbyl shody s bezpečnostními standardy.

§ 10

Náležitosti certifikátu kryptografického prostředku

Certifikát kryptografického prostředku obsahuje

a) identifikaci kryptografického prostředku včetně označení verze, pro který je vydáván,
b) identifikaci certifikátu přidělenou Úřadem,
c) identifikaci držitele,
d) identifikaci dodavatele,
e) stupeň utajení utajovaných informací, pro který byla schválena jeho způsobilost,
f) dobu platnosti certifikátu.

§ 11

Vedení přehledu certifikovaných kryptografických prostředků

(1) Úřad vede přehled certifikovaných kryptografických prostředků. K certifikovanému kryptografickému prostředku se vede certifikační spis, do kterého se zakládá žádost o certifikaci kryptografického prostředku, dokumentace přiložená k žádosti o certifikaci podle § 10 odst. 3, další doplňující podklady nebo údaje potřebné k provedení certifikace vyžádané podle § 10 odst. 5, výsledky certifikačního řízení a kopie vydaného certifikátu.

(2) Certifikační spis lze skartovat nejdříve po 15 letech ode dne ukončení platnosti certifikace kryptografického prostředku.

Ustanovení přechodná a závěrečná

§ 12

Přechodná ustanovení

(1) Kryptografický prostředek, který byl ke dni účinnosti zákona používán k ochraně státního, hospodářského nebo služebního tajemství podle dosavadní právní úpravy,[2]) kterému bylo nejpozději ke dni předcházejícímu den účinnosti zákona vydáno Ministerstvem vnitra osvědčení nebo u kterého bylo ke dni předcházejícímu den účinnosti zákona schváleno Mi-

[2]) Směrnice Federálního ministerstva vnitra ze dne 6. června 1973 pro zabezpečování ochrany skutečností tvořících předmět státního, hospodářského a služebního tajemství při jejich zpracování pomocí výpočetní techniky.

nisterstvem vnitra jeho používání k ochraně státního, hospodářského a služebního tajemství, se považuje za certifikovaný kryptografický prostředek podle této vyhlášky nejpozději do 31. prosince 2001.

(2) Statutární orgán stanoví, které kryptografické prostředky uvedené v odstavci 1 považuje za certifikované kryptografické prostředky podle této vyhlášky.

(3) Algoritmy, které byly schváleny Ministerstvem vnitra pro použití ve státní správě přede dnem účinnosti této vyhlášky, se považují za algoritmy schválené Úřadem.

(4) Osvědčení pracovníka šifrové služby vydané Ministerstvem vnitra nebo Ministerstvem obrany před nabytím účinnosti této vyhlášky se považuje za potvrzení o odborné způsobilosti pracovníka kryptografické ochrany utajovaných skutečností podle § 8 této vyhlášky. Platnost osvědčení končí, pominou-li podmínky pro jeho vydání, nebo uplynutím doby, na kterou bylo vydáno, nejpozději do 31. prosince 2001.

§ 13

Účinnost vyhlášky

Tato vyhláška nabývá účinnosti dnem vyhlášení.

Ředitel:
Ing. **Kadlec** v. r.

Příloha č. 1 k vyhlášce č. 76/1999 Sb.

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

Pošt. přihr. 2100
160 49 Praha 6

Č. j.:

POTVRZENÍ
odborné způsobilosti pracovníka
kryptografické ochrany

vydané Národním bezpečnostním úřadem podle § 52 zákona č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů.

Držitel:

rodné číslo:

Národní bezpečnostní úřad na základě žádosti držitele č. j. .....

uděluje

osvědčení odborné způsobilosti pracovníka kryptografické ochrany utajovaných skutečností č. . . . . pro stupeň utajení

a kryptografický prostředek

Toto potvrzení má platnost do:

Datum vydání potvrzení:

V Praze dne:

Ředitel
Národního bezpečnostního úřadu

Příloha č. 2 k vyhlášce č. 76/1999 Sb.

Seznam předkládané dokumentace k žádosti o certifikaci kryptografického prostředku

Předkládaná dokumentace k certifikaci kryptografického prostředku musí být v českém jazyce a v tištěné nebo elektronické podobě na běžných nosičích elektronického zpracování ve srozumitelném tvaru.

Dokumentace musí obsahovat následující údaje, podle stupně utajení chráněných nebo zpracovávaných utajovaných skutečností:

(1) Vyhrazené

a) určení a vymezení způsobu použití prostředku,
b) typ uživatelského prostředí a systémové začlenění prostředku,
c) návod k obsluze prostředku,
d) základní kryptografické parametry, typ kryptografického algoritmu, matematický model všech použitých kryptografických metod v hodnoceném kryptografickém prostředku,
e) verifikační data a programy pro ověření matematického modelu algoritmu kryptografického prostředku,
f) verifikační data a programy pro ověření a testování funkce prostředku,
g) popis klíčového hospodářství, mohutnost a struktura klíčů kryptografického prostředku,
h) způsob generování kryptografických klíčů kryptografického prostředku,
i) blokové schéma a popis prostředku s vyznačením součinnostních vazeb dílčích částí,
j) blokové schéma a popis dílčích částí – modulů prostředku,
k) podrobně komentované zdrojové texty jednotlivých modulů prostředku,
l) celkový zdrojový text programového vybavení prostředku umožňující překlad do tvaru shodného s certifikovaným prostředkem a jeho kontrolu,
m) základní kryptografický rozbor prováděný při vývoji kryptografického prostředku,
n) základní bezpečnostní rozbor prováděný při vývoji prostředku,
o) dokumentace a výsledky prováděných bezpečnostních analýz prostředku,
p) posouzení možnosti změny kryptografického algoritmu z hlediska modifikace kryptografického prostředku a licenční politiky,
r) postup instalace prostředku,
s) v případech stanovených zákonem nezbytné homologační osvědčení prostředku nebo již udělené certifikáty,
t) způsob ochrany prostředku proti kompromitaci utajovaných skutečností nebo kryptologicky významných prvků parazitním vyzařováním.

(2) Důvěrné, dokumentaci uvedenou v odstavci 1 této přílohy a dále

a) princip fyzické realizace prostředku,
b) úplnou technickou dokumentaci prostředku a popis funkčních a technických parametrů,
c) způsob tvorby a plnění klíčového hospodářství prostředku,
d) způsob generování počátečních nastavení prostředku,
e) diagnostický systém prostředku,
f) popis použitých metod autentizace a identifikace prostředku,
g) deinstalace prostředku.

(3) Tajné, dokumentaci uvedenou v odstavci 2 této přílohy a dále

a) podrobný popis fyzické realizace kryptografického algoritmu, všech jeho používaných režimů činnosti, včetně kontrolních příkladů,
b) časový diagram hlavních funkčních stavů a dílčích bloků a popis základních funkčních režimů prostředku,
c) úplné schéma zapojení prostředku, včetně podrobného technického popisu, definičního obsahu programovatelných obvodů, mikroprogramů, pamětí apod.,
d) úplné komentované zdrojové texty celého programového vybavení,
e) bezpečnostní vlastnosti a technické parametry nosičů klíčů,
f) způsob distribuce klíčového hospodářství,
g) dobu platnosti klíčového hospodářství,
h) způsob ochrany klíčů a kryptografického algoritmu před kompromitací,
i) způsob likvidace kryptografických stop po deinstalaci,
j) popis použitých metod, vlastností a bezpečnostních úrovní auditních funkcí,
k) pravidla pro používání prostředku,
l) pravidla pro používání nosičů klíčů,
m) pravidla pro návrh topologie sítí prostředků,

n) odolnost prostředku proti modifikaci kryptograficky významných částí,

o) odolnost a způsob ochrany programových částí prostředku proti virové infekci,

p) způsob pasivní ochrany prostředku,

r) diagnostiku, průběh a způsoby testování a inicializace kryptograficky významných částí při certifikaci prostředku,

s) diagnostiku, průběh a způsoby testování a inicializace kryptograficky významných částí při sériové výrobě prostředku.

(4) Přísně tajné, dokumentaci uvedenou v odstavci 3 této přílohy a dále

a) detekce kryptograficky významných chyb,

b) reakce prostředku na vnější podněty rušení,

c) reakce prostředku na náhodné, popř. úmyslné změny pracovního prostředí,

d) reakce prostředku na výskyt vlastní závady nebo virového napadení,

e) odolnost prostředku proti chybě obsluhy,

f) způsob evidence prostředku a klíčového hospodářství,

g) bezpečnostní opatření při provádění sériové výroby prostředku,

h) způsob provádění servisní činnosti prostředku u uživatele,

i) bezpečnostní opatření výroby kryptografických klíčů,

j) způsob likvidace vadných dílů a komponent při sériové výrobě a servisu prostředku,

k) způsob likvidace použitých, popř. vadných nosičů kryptograficky významných prvků,

l) způsob aktivní ochrany prostředků.

Příloha č. 3 k vyhlášce č. 76/1999 Sb.

Žádost o certifikaci kryptografického prostředku

Stupeň ochrany utajovaných skutečností:

Vyhrazeno ☐ Důvěrné ☐ Tajné ☐ Přísně tajné ☐

Typ žadatele: státní správa ☐ právnická osoba ☐ fyzická osoba ☐ jiný ☐

Typ uživatele: státní správa ☐ právnická osoba ☐ fyzická osoba ☐ jiný ☐

Jméno žadatele:

Příjmení žadatele:

Rodné číslo:

Název organizace:

Adresa:

IČO:

Název prostředku:

Země původu:
Výrobce:

Dovozce (pouze u dovážených prostředků):

Určení prostředku:

Druh utajované skutečnosti:

archivovaná data ☐ fax ☐ hlas ☐ video ☐ radio ☐ telex ☐

grafika ☐ písemnost ☐ databáze ☐ jiná ☐

Bližší specifikace:

Typ prostředí zpracování a pohybu utajované skutečnosti:

PC ☐ datová síť: LAN ☐ WAN ☐ Internet ☐ jiná ☐

Bližší specifikace:

Typ kryptografické ochrany: on line ☐ off line ☐

Typ prostředku: programový ☐ technický ☐ kombinovaný ☐

Typ kryptografického systému:	s tajným klíčem ☐		s veřejným klíčem ☐
Typ kryptografického algoritmu:	blokový ☐	proudový ☐	vložené heslo ☐
Název kryptografického algoritmu:			
Mohutnost šifrovacího klíče:			

Datum podání žádosti:

Podpis žadatele:

Razítko certifikačního pracoviště

Datum přijetí žádosti:

Podpis příjemce žádosti:

Příloha č. 4 k vyhlášce č. 76/1999 Sb.

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

Pošt. přihr. 2100
160 49 Praha 6

Národní bezpečnostní úřad vydává podle § 53 zákona č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů

CERTIFIKÁT

Číslo: . . . . . .

kryptografického prostředku

.....

.....
(název, typové označení)

držitel certifikátu .....

sídlo ..... IČO .....

dodavatel .....

sídlo ..... IČO .....

kterým se potvrzuje ověření a schválení způsobilosti kryptografického prostředku pro zpracovávání utajovaných skutečností do stupně utajení

. . . . . .

Platnost certifikátu do .....

Datum vydání certifikátu .....

Razítko se státním znakem

V Praze dne.....

Ředitel
Národního bezpečnostního úřadu

Přílohy:

77

SDĚLENÍ

Ministerstva zahraničních věcí,

kterým se opravuje sdělení Ministerstva zahraničních věcí č. 228/1998 Sb., o sjednání Dohody mezi vládou České republiky a vládou Státu Izrael o vzájemné pomoci v celních otázkách, podepsané v Jeruzalémě dne 2. září 1997

Ministerstvo zahraničních věcí vyhlašuje opravu svého sdělení č. 228/1998 Sb., o sjednání Dohody mezi vládou České republiky a vládou Státu Izrael o vzájemné pomoci v celních otázkách, podepsané v Jeruzalémě dne 2. září 1997.

Ve třetím odstavci sdělení má správně být uvedeno: Dohoda vstoupila v platnost na základě svého článku 14 odst. 1 dne 1. října 1998.

Vydává a tiskne: Tiskárna Ministerstva vnitra, p. o., Bartůňkova 4, pošt. schr. 10, 149 01 Praha 415, telefon (02) 792 70 11, fax (02) 795 26 03 – **Redakce**: Ministerstvo vnitra, Nad Štolou 3, pošt. schr. 21/SB, 170 34 Praha 7-Holešovice, telefon: (02) 614 32341 a 614 33502, fax (02) 614 33502 – **Administrace**: písemné objednávky předplatného, změny adres a počtu odebíraných výtisků – MORAVIAPRESS, a. s., U Póny 3061, 690 02 Břeclav, telefon 0627/305 161, fax: 0627/321 417. Objednávky ve Slovenské republice přijímá a titul distribuuje Magnet-Press Slovakia, s. r. o., Teslova 12, 821 02 Bratislava, tel./fax: 00421 7 525 46 28, 525 45 59. **Roční předplatné** se stanovuje za dodávku kompletního ročníku včetně rejstříku a je od předplatitelů vybíráno formou záloh ve výši oznámené ve Sbírce zákonů. Závěrečné vyúčtování se provádí po dodání kompletního ročníku na základě počtu skutečně vydaných částek (první záloha činí 3000,– Kč) – Vychází podle potřeby – **Distribuce**: celoroční předplatné i objednávky jednotlivých částek – MORAVIAPRESS, a. s., U Póny 3061, 690 02 Břeclav, telefon: 0627/305 179, 305 153, fax: 0627/321 417. – **Drobný prodej – Benešov**: HAAGER – Potřeby školní a kancelářské, Masarykovo nám. 101; **Bohumín**: ŽDB, a. s., technická knihovna, Bezručova 300; **Brno**: GARANCE-Q, Koliště 39, Knihkupectví ČS, Kapucínské nám. 11, Knihkupectví M. Ženíška, Květinářská 1, M.C.DES, Cejl 76, SEVT, a. s., Česká 14; **České Budějovice**: Prospektrum, Kněžská 18, SEVT, a. s., Krajinská 38; **Hradec Králové**: TECHNOR, Hořická 405; **Chomutov**: DDD Knihkupectví –Antikvariát, Ruská 85; **Jihlava**: VIKOSPOL, Smetanova 2; **Kadaň**: Knihařství – Přibíková, J. Švermy 14; **Kladno**: eL VaN, Ke Stadionu 1953; **Klatovy**: Krameriovo knihkupectví, Klatovy 169/I.; **Liberec**: Podještědské knihkupectví, Moskevská 28; **Most**: Knihkupectví Růžička, Šeříková 529/1057; **Napajedla**: Ing. Miroslav Kučeřík, Svatoplukova 1282; **Olomouc**: BONUM, Ostružnická 10, Tycho, Ostružnická 3; **Ostrava**: LIBREX, Nádražní 14, Profesio, Hollarova 14, SEVT, a. s., Dr. Šmerala 27; **Pardubice**: LEJHANEC, s. r. o., Sladkovského 414; **Plzeň**: ADMINA, Úslavská 2, EDICUM, Vojanova 45, Technické normy, Lábkova pav. č. 5; **Praha 1**: FIŠER-KLEMENTINUM, Karlova 1, KANT CZ, s. r. o., Hybernská 5, LINDE Praha, a. s., Opletalova 35, Moraviapress, a. s., Na Florenci 7-9, tel.: 02/232 07 66, PROSPEKTRUM, Na Poříčí 7; **Praha 4**: PROSPEKTRUM, Nákupní centrum, Budějovická, SEVT, a. s., Jihlavská 405; **Praha 5**: SEVT, a. s., E. Peškové 14; **Praha 6**: PPP – Staňková Isabela, Verdunská 1; **Praha 8**: JASIPA, Zenklova 60; **Praha 10**: Abonentní tiskový servis, Hájek 40, Uhříněves, BMSS START, areál VÚ JAWA, V Korytech 20; **Přerov**: Knihkupectví EM-ZET, Bartošova 9; **Šumperk**: Knihkupectví D-G, Hlavní tř. 23; **Teplice**: L + N knihkupectví, Kapelní 4; **Trutnov**: Galerie ALFA, Bulharská 58; **Ústí nad Labem**: 7 RX, s. r. o., Mírová 4, tel.: 047/44 249, 44 252, 44 253; **Zábřeh**: Knihkupectví PATKA, Žižkova 45; **Žatec**: Prodejna U Pivovaru, Žižkovo nám. 76. **Distribuční podmínky předplatného**: jednotlivé částky jsou expedovány neprodleně po dodání z tiskárny. Objednávky nového předplatného jsou vyřizovány do 15 dnů a pravidelné dodávky jsou zahajovány od nejbližší částky po ověření úhrady předplatného nebo jeho zálohy. Částky vyšlé v době od zaevidování předplatného do jeho úhrady jsou doposílány jednorázově. Změny adres a počtu odebíraných výtisků jsou prováděny do 15 dnů. **Reklamace**: informace na tel. čísle 0627/305 168. V písemném styku vždy uvádějte IČO (právnická osoba), rodné číslo (fyzická osoba). **Podávání novinových zásilek** povoleno Českou poštou, s. p., Odštěpný závod Jižní Morava Ředitelství v Brně č. j. P/2-4463/95 ze dne 8. 11. 1995.