541

VYHLÁŠKA
Národného bezpečnostného úradu

z 9. septembra 2002

o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách a pravidlách na výkon certifikačných činností

Národný bezpečnostný úrad (ďalej len „úrad“) podľa § 14 ods. 1 písm. j) a ods. 2 a § 26 ods. 1 písm. b) prvého bodu zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) ustanovuje:

§ 1

Predmet úpravy

Táto vyhláška upravuje
a) obsah a rozsah prevádzkovej dokumentácie certifikačnej autority,
b) bezpečnostné pravidlá a pravidlá na výkon certifikačných činností akreditovanej certifikačnej autority.

§ 2

Vymedzenie niektorých pojmov

Na účely tejto vyhlášky sa rozumie
a) párovými dátami dvojica tvorená verejným kľúčom a súkromným kľúčom patriacim k danému verejnému kľúču,
b) bezpečnostným opatrením technický, personálny alebo administratívny prvok ochrany, ktorého účelom je udržiavať bezpečný a spoľahlivý výkon certifikačných činností,
c) typom certifikátu a časovej pečiatky skupina atribútov charakterizujúcich vydaný certifikát a časovú pečiatku z hľadiska ceny a odporučeného využitia; certifikačná autorita môže vydávať certifikáty a časové pečiatky viacerých typov.

§ 3

Dokumentácia certifikačnej autority

(1) Certifikačná autorita vypracúva, vedie a aktualizuje dokumentáciu na výkon certifikačných činností.

(2) Dokumentácia certifikačnej autority obsahuje
a) prevádzkovú dokumentáciu,
b) bezpečnostné pravidlá,
c) pravidlá na výkon certifikačných činností.

§ 4

Prevádzková dokumentácia certifikačnej autority

Prevádzková dokumentácia certifikačnej autority obsahuje
a) certifikačný poriadok,
b) vzory zmlúv o vydaní a používaní certifikátu,
c) cenník poskytovaných certifikačných služieb,
d) prevádzkové záznamy,
e) iné záznamy, ktoré certifikačná autorita považuje za účelné.

§ 5

Certifikačný poriadok

(1) Certifikačný poriadok obsahuje
a) informácie pre koho a za akých podmienok poskytuje certifikačná autorita svoje služby,
b) obmedzenia pri poskytovaní svojich služieb, ak také obmedzenia existujú,
c) typy certifikátov a časových pečiatok, ktoré certifikačná autorita vydáva,
d) podpisové politiky a politiky časových pečiatok[1]),
e) práva a povinnosti používateľov služieb certifikačnej autority,
f) vzor žiadosti o poskytnutie certifikačnej služby,
g) pravidlá používania a zrušovania certifikátov.

(2) Certifikačný poriadok môže okrem informácií uvedených v odseku 1 obsahovať aj ďalšie informácie, ktorých zverejnenie certifikačná autorita považuje za účelné.

(3) Certifikačný poriadok akreditovanej certifikačnej autority popisuje úlohy jednotlivých subjektov a procesy súvisiace so správou certifikátov, a to
a) prvotnú registráciu žiadosti o vydanie certifikátu,
b) žiadosť o vydanie následného certifikátu,
c) vydanie certifikátu,
d) žiadosť o zrušenie certifikátu,
e) zrušenie certifikátu,
f) vydávanie zoznamu zrušených certifikátov.

(4) Certifikačný poriadok akreditovanej certifikačnej autority obsahuje klasifikáciu spracovávaných infor-

[1]) Vyhláška Národného bezpečnostného úradu č. 537/2002 Z. z. o formáte a spôsobe vyhotovenia zaručeného elektronického podpisu, spôsobe zverejňovania verejného kľúča úradu, postupe pri overovaní a podmienkach overovania zaručeného elektronického podpisu, formáte časovej pečiatky a spôsobe jej vyhotovenia, požiadavkách na zdroj časových údajov a požiadavkách na vedenie dokumentácie časových pečiatok (o vyhotovení a overovaní elektronického podpisu a časovej pečiatky).

mácií, spôsob ich ochrany a pravidlá na sprístupňovanie týchto informácií inému subjektu.

(5) Certifikačný poriadok akreditovanej certifikačnej autority ustanovuje pre každý ňou vydávaný typ certifikátu a časovej pečiatky náležitosti potrebné na vydanie certifikátu a časovej pečiatky, rozsah použiteľnosti certifikátov a časových pečiatok a záruky akreditovanej certifikačnej autority pre certifikát a časovú pečiatku daného typu.

(6) Certifikačný poriadok akreditovanej certifikačnej autority ustanovuje aj rozsah a spôsob zverejňovania informácií súvisiacich s poskytovaním certifikačných služieb, a to

a) kontaktných adries akreditovanej certifikačnej autority,
b) podporovaných štandardov a protokolov pre prístup k zverejňovaným informáciám,
c) vlastných certifikátov s riešením spôsobu ich nahradenia po skončení platnosti,
d) vydaných certifikátov, formátu ich zverejňovania a aktualizáciu zoznamu vydaných certifikátov,
e) zoznamov zrušených certifikátov, formátu ich zverejňovania a ich aktualizáciu; pre akreditovanú certifikačnú autoritu sa odporúča zabezpečiť zverejňovanie aspoň dvoma na sebe nezávislými spôsobmi.

(7) Certifikačný poriadok akreditovanej certifikačnej autority poskytuje informácie o vykonávaní auditu a zaznamenávaní prevádzkových udalostí.

(8) Akreditovaná certifikačná autorita môže mať viacero certifikačných poriadkov pre rôzne typy vydávaných certifikátov.

(9) Štruktúra certifikačného poriadku akreditovanej certifikačnej autority je uvedená v prílohe č. 1.

§ 6

Vzor zmluvy o vydaní a používaní certifikátu

(1) Vydanie certifikátu žiadateľovi o certifikát sa uskutočňuje na základe zmluvy o vydaní a používaní certifikátu.

(2) Obsahom zmluvy o vydaní a používaní certifikátu je definovanie vzťahu medzi žiadateľom o certifikát a certifikačnou autoritou v súvislosti s vydaním certifikátu.

(3) Certifikačná autorita môže mať vypracovaných viacero vzorov zmlúv o vydaní a používaní certifikátu pre rôzne typy vydávaných certifikátov.

(4) Vzor zmluvy o vydaní a používaní certifikátu obsahuje

a) postup na vydanie a prevzatie prvého certifikátu žiadateľovi o certifikát,
b) postup na vydanie a prevzatie následného certifikátu,
c) záväzky certifikačnej autority,
d) záväzky držiteľa certifikátu,
e) možné obmedzenie zodpovednosti certifikačnej autority v prípade porušenia pravidiel na vystavenie a prácu s certifikátmi zo strany žiadateľa,
f) potvrdenie o vydaní certifikátu a jeho odovzdaní žiadateľovi o certifikát.

§ 7

Cenník poskytovaných certifikačných služieb

Cenník poskytovaných certifikačných služieb obsahuje zoznam všetkých certifikačných služieb, ktoré certifikačná autorita poskytuje, spolu s uvedením aktuálnej ceny každej služby alebo informácie, že danú službu poskytuje certifikačná autorita bezplatne.

§ 8

Prevádzkové záznamy

(1) Prevádzkovými záznamami sú záznamy v písomnej alebo elektronickej forme vznikajúce pri certifikačnej činnosti.

(2) Certifikačná autorita zaznamenáva všetky prevádzkové udalosti pri

a) podávaní žiadosti o certifikát a vydávaní certifikátu,
b) spracúvaní a uchovávaní osobných údajov žiadateľa,
c) vydávaní certifikátu,
d) vydávaní krížového certifikátu,
e) skončení platnosti certifikátu,
f) požiadavke na zrušenie certifikátu,
g) zrušení certifikátu,
h) vytváraní a zverejňovaní zoznamu zrušených certifikátov,
i) manipulácii so súkromným kľúčom certifikačnej autority,
j) vydávaní časovej pečiatky.

(3) Záznamy o udalostiach podľa odseku 2 sa vytvárajú, uchovávajú a spracúvajú tak, aby sa zachovala preukázateľnosť pôvodu, dostupnosť, integrita, časová autenticita a dôvernosť týchto záznamov.

(4) Certifikačná autorita vytvára písomné záznamy o

a) prijatí žiadosti o vystavenie certifikátu,
b) odovzdaní certifikátu žiadateľovi o certifikát,
c) prijatí žiadosti a podnetov o zrušenie certifikátu,
d) oboznámení osôb určených na vykonávanie činností súvisiacich s poskytovaním certifikačných služieb s dokumentáciou a so smernicami certifikačnej autority,
e) preškolení osôb uvedených v písmene d) tak, aby ich kvalifikačné predpoklady zodpovedali vykonávaným činnostiam,
f) uvedení do prevádzky a zmene prevádzkového režimu nástroja na vytváranie elektronického podpisu certifikačnej autority, pričom sa vyžaduje, aby túto operáciu vykonali a písomne potvrdili aspoň dve fyzické osoby určené na túto činnosť,
g) technických zásahoch súvisiacich s prevádzkou a pravidelnou kontrolou technických zariadení a súčastí prevádzkovaného informačného systému.

(5) Certifikačná autorita môže za podmienok definovaných v jej certifikačnom poriadku vytvárať záznamy podľa odseku 4 písm. a) až c) v elektronickej forme.

§ 9

Bezpečnostné pravidlá

(1) Bezpečnostné pravidlá akreditovanej certifikačnej autority obsahujú
a) bezpečnostnú politiku,
b) bezpečnostný zámer,
c) bezpečnostný projekt,
d) havarijný plán,
e) bezpečnostné smernice.

(2) Na poskytovanie akreditovaných certifikačných služieb akreditovaná certifikačná autorita realizuje bezpečnostné opatrenia. Bezpečnostné opatrenia sú navrhnuté, zdokumentované a využívané podľa bezpečnostných pravidiel.

(3) Bezpečnostné opatrenia pozostávajú z mechanických a technických opatrení, z opatrení na ochranu produktu pre elektronický podpis a z opatrení na ochranu softvérových a hardvérových prvkov infraštruktúry, v ktorej sa produkt pre elektronický podpis prevádzkuje.

(4) Mechanické opatrenia sú všetky druhy bezpečnostných úschovných objektov, uzamykateľné kovové skrine, uzamykacie systémy, dvere, mreže, bezpečnostné fólie, okná a zasklenia.

(5) Technické opatrenia sú
a) elektromechanické zámkové zariadenia a systémy na kontrolu vstupov do objektov a chránených priestorov a systémy slúžiace na elektronické preukazovanie oprávnenosti a totožnosti osôb,
b) zariadenia poplachových systémov slúžiace na zisťovanie a vyhodnocovanie neoprávneného vstupu do objektu alebo chráneného priestoru,
c) kamerová zostava v rámci uzatvoreného televízneho okruhu,
d) zariadenia elektrickej požiarnej signalizácie,
e) zariadenia na fyzické ničenie nosičov informácií,
f) zariadenie na nepretržité vedenie kontrolného záznamu o činnosti prostriedku pre elektronický podpis a systémov evidencie poskytovaných certifikačných služieb s možnosťou sledovania a spätného preskúmavania záznamu, ako aj určenia zodpovednosti za vykonané činnosti,
g) iné technické prostriedky slúžiace na zabezpečenie objektu, chráneného priestoru, prevádzky produktu pre elektronický podpis, systémov evidencie poskytovaných certifikovaných služieb a médií so záložnými a archívnymi kópiami údajov týchto systémov.

(6) Opatrenia na ochranu produktu pre elektronický podpis sú opatrenia splňajúce požiadavky osobitného predpisu.[2])

(7) Bezpečnostné opatrenia prijaté akreditovanou certifikačnou autoritou musia spĺňať najmenej tieto podmienky:
a) pri poskytovaní certifikačných služieb v prenajatých priestoroch musí byť zmluvne obmedzený samostatný vstup majiteľa objektu do chránených priestorov len na nevyhnutné a okamžité riešenie havarijných stavov budov,
b) okrem prevádzkových priestorov musí akreditovaná certifikačná autorita zabezpečiť ďalšie chránené priestory na bezpečné skladovanie archívnych dokumentov a údajov a mesačných záložných kópií údajov systému certifikačnej autority; tieto priestory musia byť umiestnené v objekte, ktorý nie je fyzicky spojený s objektom, v ktorom sa poskytujú certifikačné služby,
c) poskytovanie certifikačných služieb musí byť podporené technickými a programovými prostriedkami vyhradenými výlučne na tento účel a dôsledne oddelenými od ostatných systémov pre bežnú administratívu certifikačnej autority,
d) technické a organizačné opatrenia musia zaistiť nepretržitú prevádzku akreditovanej certifikačnej autority aj v prípade zlyhania základnej technickej infraštruktúry najmenej na úrovni poskytovania služby registrácie požiadaviek na funkciu časovej pečiatky,
e) musí sa vypracovať a prevádzkovať vlastný systém priebežnej kontroly funkčnosti a bezpečnosti použitých bezpečnostných prostriedkov a opatrení,
f) musí sa vypracovať a prevádzkovať systém priebežného dokumentovania všetkých kľúčových aktivít v použitom systéme a pravidelného i náhodného vyhodnocovania takto vytvorených záznamov,
g) záznamy priebežného dokumentovania kľúčových aktivít použitého systému sa musia bezpečne uchovávať na médiách a v tvare použiteľnom na kontrolu najmenej počas troch rokov.

(8) Bezpečnostné pravidlá vypracúva akreditovaná certifikačná autorita sama alebo s pomocou externých fyzických osôb alebo právnických osôb. Bez ohľadu na spôsob vypracovania akreditovaná certifikačná autorita zabezpečí kvalifikovanú externú oponentúru bezpečnostných pravidiel. Na tento účel úradu predloží
a) údaje o zodpovednom riešiteľovi bezpečnostného projektu a jeho kvalifikácii pre oblasť informačnej bezpečnosti,
b) oponentský posudok predloženého bezpečnostného projektu od nezávislého externého špecialistu pre informačnú bezpečnosť odborne oprávneného na výkon auditu podľa osobitného predpisu,[3])
c) pri výhradách externého oponenta uvedených v oponentskom posudku aj vlastné vyjadrenie k oponentskému posudku.

(9) Akreditovaná certifikačná autorita pri zmenách v platných bezpečnostných pravidlách kvalifikovane posúdi ich dopad na bezpečnosť poskytovaných akre-

[2]) Vyhláška Národného bezpečnostného úradu č. 539/2002 Z. z., ktorou sa ustanovujú podrobnosti o požiadavkách na bezpečné zariadenia na vyhotovovanie časovej pečiatky a požiadavky na produkty pre elektronický podpis (o produktoch elektronického podpisu).
[3]) Vyhláška Národného bezpečnostného úradu č. 540/2002 Z. z. o podmienkach na poskytovanie akreditovaných certifikačných služieb a o požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov.

ditačných služieb a o navrhovaných zmenách a vyhodnotení ich dopadov na bezpečnosť bezodkladne informuje úrad.

§ 10

Bezpečnostná politika

(1) Bezpečnostná politika určuje základné požiadavky na ochranu citlivých informácií a záväzky jednotlivých subjektov vo vzťahu k bezpečnosti.

(2) Cieľom bezpečnostnej politiky je určenie cieľov a popisu spôsobu zabezpečenia celkovej bezpečnosti certifikačnej autority.

§ 11

Bezpečnostný zámer

(1) Bezpečnostný zámer určuje požiadavky na ochranu informácií zhromažďovaných, vytváraných, spracúvaných, prenášaných alebo ukladaných v súvislosti s poskytovaním certifikačných služieb.

(2) Bezpečnostný zámer obsahuje
a) určenie informácií, ktoré treba chrániť,
b) charakteristiku a popis použitia technických a programových prostriedkov, ktorých pomocou bude budúca akreditovaná certifikačná autorita vykonávať svoju činnosť,
c) predpokladanú organizačnú štruktúru budúcej akreditovanej certifikačnej autority s uvedením oprávnení pre každé pracovné zaradenie,
d) popis priestoru, v ktorom sú umiestnené prostriedky uvedené v písmene b),
e) požiadavky na celkovú bezpečnosť akreditovanej certifikačnej autority, ktorá sa skladá z personálnej bezpečnosti, objektovej bezpečnosti, administratívnej bezpečnosti a bezpečnosti technických a systémových prostriedkov.

§ 12

Bezpečnostný projekt

(1) Bezpečnostný projekt je predpis akreditovanej certifikačnej autority, ktorý určuje spôsob ochrany výkonu certifikačných činností a ochrany produktu pre elektronický podpis prostredníctvom bezpečnostných opatrení.

(2) Bezpečnostný projekt pozostáva z
a) analýzy rizík infraštruktúry, pomocou ktorej akreditovaná certifikačná autorita vykonáva certifikačné činnosti, s dôrazom na procedúry súvisiace s výkonom a evidenciou certifikačných činností a produktom pre elektronický podpis,
b) popisu bezpečnostných rizík súvisiacich s výkonom certifikačných činností a prevádzkou produktu pre elektronický podpis,
c) popisu bezpečnostných opatrení na obmedzenie identifikovaných bezpečnostných rizík,
d) popisu nasadenia, využívania a kontroly bezpečnostných opatrení.

(3) Súčasťou bezpečnostného projektu je určenie spôsobu ochrany osobných údajov pre certifikačné služby podľa osobitného zákona.[4])

§ 13

Havarijný plán

(1) Obsahom havarijného plánu je stanovenie postupov, ktoré sa budú aplikovať v prípade mimoriadnej udalosti. Pod mimoriadnou udalosťou sa na účely tejto vyhlášky rozumie udalosť, ktorá ohrozuje poskytovanie certifikačných služieb a ktorá nastáva v dôsledku zlyhania informačného systému pre certifikačné služby.

(2) Súčasťou havarijného plánu je plán obnovy. Plán obnovy ustanovuje postupy určené na obnovu riadnej funkčnosti informačného systému pre certifikačné služby po vzniku mimoriadnej udalosti.

§ 14

Bezpečnostné smernice

(1) Bezpečnostné smernice sú predpisy akreditovanej certifikačnej autority, ktoré rozpracúvajú ustanovenia bezpečnostného zámeru do procedúr a pracovných postupov záväzných pre všetkých zamestnancov certifikačnej autority.

(2) Bezpečnostné smernice upravujú najmenej tieto bezpečnostné opatrenia:
a) umiestnenie a používanie kryptografického zariadenia certifikačnej autority,
b) riadenie prístupu ku kryptografickému zariadeniu certifikačnej autority,
c) postup zálohovania dát a skladovania médií so záložnými kópiami údajov,
d) postupy pri haváriách a poruchách produktu pre elektronický podpis, haváriách a poruchách infraštruktúry ohrozujúcich činnosť produktu pre elektronický podpis, jeho bezpečnosť, ako aj bezpečnosť záložných kópií údajov, ako aj pri haváriách a poruchách ohrozujúcich autenticitu a integritu poskytovaných certifikačných služieb,
e) zabezpečenie prevádzky kryptografického zariadenia certifikačnej autority v núdzových alebo havarijných stavoch,
f) zásady práce s médiami,
g) tvorbu a vyhodnocovanie prevádzkových záznamov v písomnej alebo elektronickej forme,
h) správu bezpečnostných prostriedkov,
i) zásady bezpečného správania sa užívateľov a správcov produktu pre elektronický podpis,
j) zisťovanie bezpečnostných incidentov a ich riešenie,
k) monitorovanie a odhaľovanie nepovolených aktivít v produkte pre elektronický podpis,
l) bezpečnostné procedúry spojené s výkonom certifikačných činností.

[4]) Zákon č. 428/2002 Z. z. o ochrane osobných údajov.

§ 15

Pravidlá na výkon certifikačných činností

(1) Pravidlá na výkon certifikačných činností určujú postup, ktorý akreditovaná certifikačná autorita uplatňuje pri zabezpečovaní poskytovaných certifikačných služieb.

(2) Pravidlá na výkon certifikačných činností akreditovanej certifikačnej autority obsahujú procedúry a postupy súvisiace s

a) generovaním párových dát certifikačnej autority, so spôsobom ochrany súkromného kľúča certifikačnej autority a so spôsobom získania certifikátu certifikačnej autority,
b) generovaním párových dát žiadateľa o certifikát,
c) archiváciou certifikátov,
d) bezpečnosťou počítačového vybavenia,
e) kontrolou procedurálnej bezpečnosti, fyzickej bezpečnosti, bezpečnosti počítačovej siete, bezpečnosti informačného systému a bezpečnosti kryptografického modulu.

(3) Pravidlá na výkon certifikačných činností akreditovanej certifikačnej autority obsahujú aj technické špecifikácie

a) formátov údajov súvisiacich s poskytovaním certifikačných služieb,
b) odkazov na príslušné predpisy,
c) štandardov používaných pri výkone certifikačných služieb.

(4) Štruktúra pravidiel na výkon certifikačných činností je uvedená v prílohe č. 2.

§ 16

Účinnosť

Táto vyhláška nadobúda účinnosť 1. októbra 2002.

Ján Mojžiš v. r.

Príloha č. 1
k vyhláške č. 541/2002 Z. z.

ŠTRUKTÚRA CERTIFIKAČNÉHO PORIADKU AKREDITOVANEJ CERTIFIKAČNEJ AUTORITY

1. ÚVOD
   Základné informácie o účele dokumentu. Súčasťou certifikačného poriadku certifikačnej autority môže byť určenie rozsahu použiteľnosti certifikátov a časových pečiatok.
   Úvodné ustanovenia obsahujú aj kontaktné informácie o certifikačnej autorite, najmenej však adresu elektronickej pošty, telefonický a faxový kontakt.

2. VŠEOBECNÉ USTANOVENIA
   Základné východiská pre legislatívne vzťahy a procedúry poskytovania akreditovaných certifikačných služieb.
   2.1. Záväzky všetkých subjektov vstupujúcich do procesov súvisiacich s poskytovaním akreditovaných certifikačných služieb
      a) certifikačnej autority,
      b) registračnej autority,
      c) žiadateľa alebo držiteľa certifikátu,
      d) subjektu, ktorý koná na báze dôvery v daný certifikát a/alebo na základe elektronického podpisu overeného daným certifikátom (ďalej len „používateľ certifikátu“),
      e) správcov adresárov.
   2.2. Právne záruky
      Popis zodpovednosti každého subjektu
      a) záruky a obmedzenia poskytovaných záruk,
      b) typy krytých škôd,
      c) ohraničenie možných strát,
      d) ďalšie obmedzenia zodpovednosti.
   2.3. Finančná zodpovednosť
      Definovanie finančnej zodpovednosti certifikačnej autority a presné definovanie jej ohraničení.
   2.4. Rozhodcovské konanie a riešenie sporov
      Určenie spôsobu interpretácie certifikačného poriadku, napr. rozhodcovské konanie, spôsob riešenia sporov a pod.
   2.5. Poplatky
      Špecifikácia poplatkov, ktoré si certifikačná autorita alebo registračná autorita účtuje za služby spojené s vydávaním a so správou certifikátov.
   2.6. Zverejňovanie informácií
      Záväzky certifikačnej autority súvisiace so zverejňovaním informácií, a to
      a) publikovaním informácií o vlastných postupoch a procedúrach, vlastných certifikátoch a stave týchto certifikátov,
      b) periodicitou publikovania informácií,
      c) požiadavkami na využívanie zverejňovaných informácií spravovaných certifikačnou autoritou treťou stranou.
   2.7. Audit zhody
      Deklarácia certifikačnej autority v oblasti vykonávania auditov.
   2.8. Dôvernosť
      Záväzky certifikačnej autority súvisiace s ochranou informácií, a to
      a) typy informácií, ktoré má certifikačná autorita chrániť,
      b) typy informácií, ktoré nie sú klasifikované ako dôverné,
      c) kto bude oboznamovaný o zrušení certifikátu,
      d) politika poskytovania informácií vyžadovaných podľa zákona,
      e) prípady, v ktorých sa dôverná informácia môže zverejniť.
   2.9. Ochrana intelektuálnych práv
      Popis vlastníckych práv k certifikátom, procedúram a kľúčom.

3. IDENTIFIKÁCIA A AUTENTIFIKÁCIA
Popis procesov súvisiacich s autentifikáciou žiadateľov o certifikát pred vlastným vydaním certifikátu. Tieto procesy sa môžu čiastočne využiť aj pri žiadosti o zrušenie certifikátu a pri vydaní následného certifikátu.
3.1. Iniciálna registrácia
Základné vlastnosti procesov identifikácie a autentifikácie pri registrácii subjektu a vydávaní certifikátu. Medzi základné otázky riešené v tejto časti patria
a) typy mien, pravidlá na interpretáciu mien, požiadavky na jednoznačnosť a zmysluplnosť mien,
b) spôsob riešenia sporov týkajúcich sa mien,
c) či a akým spôsobom musí žiadateľ o certifikát preukázať vlastníctvo súkromného kľúča k verejnému kľúču v žiadosti o certifikát,
d) autentifikačné požiadavky pre organizácie a jej zástupcov.
3.2. Vydanie následného certifikátu
Procesy súvisiace s vydaním následného certifikátu po skončení alebo pred skončením platnosti existujúceho certifikátu, ak tento certifikát nebol zrušený.
3.3. Vydanie následného certifikátu po zrušení certifikátu
Procesy súvisiace s vydaním následného certifikátu v prípade, že existujúci certifikát bol zrušený.
3.4. Žiadosť o zrušenie certifikátu
Procesy súvisiace so spracovaním požiadaviek na identifikáciu subjektu pri žiadosti o zrušenie certifikátu.

4. PREVÁDZKOVÉ POŽIADAVKY
Popis procesov súvisiacich s vydávaním certifikátov.
4.1. Žiadosť o vydanie certifikátu
Procesy súvisiace so zaregistrovaním žiadateľa a s vystavením žiadosti o vydanie certifikátu.
4.2. Vydanie certifikátu
Procesy súvisiace s vydaním certifikátu a informovaním žiadateľa o vydaní certifikátu.
4.3. Prevzatie certifikátu
Procesy súvisiace s prevzatím certifikátu a následným publikovaním certifikátov.
4.4. Zrušenie certifikátu
Procesy súvisiace so zrušením certifikátu, a to
a) stanovenie okolností, za ktorých možno certifikát zrušiť,
b) stanovenie, kto môže o zrušenie certifikátu požiadať,
c) postup na vystavenie a spracovanie žiadosti o zrušenie certifikátu,
d) interval na zrušenie certifikátu na základe požiadavky,
e) stanovenie periodicity publikovania zoznamu zrušených certifikátov,
f) požiadavky na používateľov certifikátov na sledovanie zoznamu zrušených certifikátov,
g) popis možností on-line zisťovania stavu certifikátu a požiadavky na používateľov certifikátov na využívanie on-line mechanizmov na zisťovanie stavu certifikátu,
h) iné možnosti informovania o zrušení certifikátu a požiadavky na používateľov certifikátov na využívanie iných mechanizmov na zverejňovanie zrušenia certifikátu,
i) akákoľvek kombinácia predchádzajúcich mechanizmov pre prípad, že dôvodom zrušenia certifikátu je kompromitácia súkromného kľúča.
4.5. Audit bezpečnosti
Deklarácie certifikačnej autority o zaznamenávaní prevádzkových udalostí.
4.6. Archivácia záznamov
Deklarácie certifikačnej autority o archivácii záznamov.
4.7. Zmena kľúčov
Procesy súvisiace so zverejnením nového verejného kľúča certifikačnej autority.
4.8. Havarijný plán pre mimoriadne udalosti
Deklarácie certifikačnej autority o riešení havarijných situácií.
4.9. Skončenie činnosti certifikačnej autority
Informácia o spôsobe skončenia činnosti certifikačnej autority a zverejnení oznámenia o skončení činnosti vrátane archivácie podkladov.

5. FYZICKÉ, PROCEDURÁLNE A PERSONÁLNE BEZPEČNOSTNÉ OPATRENIA
Deklarácie certifikačnej autority o opatreniach na zaistenie bezpečnej prevádzky.

6. TECHNICKÉ BEZPEČNOSTNÉ OPATRENIA
Deklarácie certifikačnej autority o opatreniach na zabezpečenie bezpečnej prevádzky a tiež špecifikáciu kryptografických prostriedkov na generovanie kľúčov certifikačnej autority.

7. PROFILY CERTIFIKÁTOV A ZOZNAMOV ZRUŠENÝCH CERTIFIKÁTOV
   Popis profilov certifikátov a profilov zoznamov zrušených certifikátov.
   7.1. Profil certifikátu
   Formát, obsah a nastavenie typických hodnôt jednotlivých položiek vydávaných certifikátov.
   7.2. Profil zoznamu zrušených certifikátov
   Formát a obsah zoznamu zrušených certifikátov.

8. ADMINISTRÁCIA ŠPECIFIKÁCIÍ
   Popis spôsobu spravovania, aktualizácie a zverejňovania certifikačného poriadku, ako aj informácie o platnosti certifikačného poriadku.

Príloha č. 2
k vyhláške č. 541/2002 Z. z.

ŠTRUKTÚRA PRAVIDIEL NA VÝKON CERTIFIKAČNÝCH ČINNOSTÍ

1. ÚVOD
   Základné informácie o účele dokumentu. Úvodné ustanovenia obsahujú tiež kontaktné informácie o certifikačnej autorite, najmenej však adresu elektronickej pošty, telefonický a faxový kontakt.

2. VŠEOBECNÉ USTANOVENIA
   Základné východiská pre legislatívne vzťahy a procedúry poskytovania akreditovaných certifikačných služieb.
   2.1. Povinnosti
   Definícia záväzkov všetkých subjektov vstupujúcich do procesov súvisiacich s certifikátmi a časovými pečiatkami
   a) certifikačnej autority,
   b) registračnej autority,
   c) žiadateľa alebo držiteľa certifikátu,
   d) používateľa certifikátu,
   e) správcov adresárov.
   2.2. Právne záruky
   Popis zodpovednosti každého subjektu
   a) garancie a obmedzenia poskytovaných garancií,
   b) typy krytých škôd,
   c) ohraničenie možných strát,
   d) ďalšie obmedzenia zodpovednosti.
   2.3. Finančná zodpovednosť
   Definovanie finančnej zodpovednosti certifikačnej autority a presné definovanie jej ohraničení.
   2.4. Rozhodcovské konanie a riešenie sporov
   Určenie spôsobu interpretácie certifikačného poriadku, napr. rozhodcovské konanie, spôsob riešenia sporov a pod.
   2.5. Poplatky
   Špecifikácia poplatkov, ktoré si certifikačná autorita alebo registračná autorita účtuje za služby spojené s vydávaním a so správou certifikátov.
   2.6. Zverejňovanie informácií
   Záväzky certifikačnej autority súvisiace so zverejňovaním informácií
   a) publikovanie informácií o vlastných postupoch a procedúrach, vlastných certifikátoch a stave týchto certifikátov,
   b) periodicita publikovania informácií,
   c) požiadavky na využívanie adresárov spravovaných certifikačnou autoritou treťou stranou.
   2.7. Audit zhody
   Informácie súvisiace s pravidelnými auditmi zhody s deklarovanými záväzkami
   a) frekvencia a periodicita auditu,
   b) identita a kvalifikácia audítora, ako aj jeho vzťah k auditovanému subjektu,
   c) zoznam oblastí pokrývaných v audite zhody,
   d) zoznam opatrení realizovaných na základe výsledkov auditu.
   2.8. Dôvernosť
   Záväzky certifikačnej autority súvisiace s ochranou informácií
   a) typy informácií, ktoré má certifikačná autorita chrániť,
   b) typy informácií, ktoré nie sú klasifikované ako dôverné,
   c) kto bude oboznamovaný o zrušení certifikátu,
   d) politika poskytovania informácií vyžadovaných podľa zákona,
   e) prípady, v ktorých sa dôverná informácia môže zverejniť.
   2.9. Ochrana intelektuálnych práv
   Popis vlastníckych práv k certifikátom, procedúram a kľúčom.

3. IDENTIFIKÁCIA A AUTENTIFIKÁCIA
Popis procedúr súvisiacich s autentifikáciou žiadateľov o certifikát pred vlastným vydaním certifikátu. Tieto procedúry sa využívajú aj pri žiadosti o zrušenie certifikátu a o vydanie následného certifikátu.
3.1. Iniciálna registrácia
Základné vlastnosti procesov identifikácie a autentifikácie pri registrácii subjektu a vydávaní certifikátu. Medzi základné otázky riešené v tejto časti patria
a) typy mien, pravidlá na interpretáciu mien, požiadavky na jednoznačnosť a zmysluplnosť mien,
b) spôsob riešenia sporov týkajúcich sa mien,
c) či a akým spôsobom musí žiadateľ o certifikát preukázať vlastníctvo súkromného kľúča k verejnému kľúču v žiadosti o certifikát,
d) autentifikačné požiadavky pre organizácie a jej zástupcov.
3.2. Vydanie následného certifikátu
Procesy súvisiace s vydaním následného certifikátu po skončení alebo pred skončením platnosti existujúceho certifikátu, ak tento certifikát nebol zrušený.
3.3. Vydanie následného certifikátu po zrušení certifikátu
Procesy súvisiace s vydaním následného certifikátu v prípade, že existujúci certifikát bol zrušený.
3.4. Žiadosť o zrušenie certifikátu
Procesy súvisiace so spracovaním požiadaviek na identifikáciu subjektu pri žiadosti o zrušenie certifikátu.

4. PREVÁDZKOVÉ POŽIADAVKY
Popis procedúr súvisiacich s vydávaním certifikátov.
4.1. Žiadosť o vydanie certifikátu
Procesy súvisiace so zaregistrovaním žiadateľa a s vystavením žiadosti o vydanie certifikátu.
4.2. Vydanie certifikátu
Procesy súvisiace s vydaním certifikátu a informovaním žiadateľa o vydaní certifikátu.
4.3. Prevzatie certifikátu
Procesy súvisiace s prevzatím certifikátu a následným publikovaním certifikátov.
4.4. Zrušenie certifikátu
Procesy súvisiace so zrušením certifikátu, a to
a) určenie okolností, za ktorých možno certifikát zrušiť,
b) určenie, kto môže o zrušenie certifikátu požiadať,
c) postup na vystavenie a spracovanie žiadosti o zrušenie certifikátu,
d) interval na zrušenie certifikátu na základe požiadavky,
e) stanovenie periodicity publikovania zoznamu zrušených certifikátov,
f) požiadavky na používateľov certifikátov na sledovanie zoznamu zrušených certifikátov,
g) popis možností on-line zisťovania stavu certifikátu a požiadavky na používateľov certifikátov na využívanie on-line mechanizmov na zisťovanie stavu certifikátu,
h) iné možnosti informovania o zrušení certifikátu a požiadavky na používateľov certifikátov na využívanie iných mechanizmov na zverejňovanie zrušenia certifikátu,
i) akákoľvek kombinácia predchádzajúcich mechanizmov pre prípad, že dôvodom zrušenia certifikátu je kompromitácia súkromného kľúča.
4.5. Procedúry pre audit bezpečnosti
Procesy súvisiace so zaznamenávaním prevádzkových udalostí a systému auditu, a to
a) typy zaznamenávaných udalostí,
b) frekvencia spracovania a auditu prevádzkových záznamov,
c) perióda uchovávania prevádzkových záznamov,
d) ochrana prevádzkových záznamov so zameraním na prístupové práva, ochrana proti modifikácii a proti vymazaniu,
e) zálohovanie prevádzkových záznamov,
f) spôsob informovania subjektov o zaznamenávaní činnosti.
4.6. Archivácia záznamov
Procesy súvisiace s archiváciou so zameraním na
a) typy zaznamenávaných udalostí,
b) lehotu uchovávania archívov,
c) prístupové práva a ochranu archívnych záznamov proti modifikácii a proti vymazaniu,
d) zálohovanie archívov,
e) požiadavky na časové údaje v záznamoch,
f) procedúry na overovanie archívnych informácií.
4.7. Zmena kľúčov
Procesy súvisiace so zverejnením nového verejného kľúča certifikačnej autority.

4.8. Havarijný plán
Procesy súvisiace so zvládaním havarijných situácií. Každá z týchto oblastí sa rozpracúva samostatne:
a) procedúry na obnovu činností v prípade, že výpočtové zdroje, programové vybavenie alebo údaje certifikačnej autority sú poškodené, resp. je podozrenie, že sú poškodené. Procedúry popisujú spôsob obnovenia bezpečného prostredia, určenia, ktoré certifikáty sa zrušia, či možno ďalej používať súkromný kľúč certifikačnej autority, ako sa nový verejný kľúč zverejní.
b) procedúry obnovy pre prípad, že certifikát certifikačnej autority je zrušený. Procedúry popisujú spôsob obnovy bezpečného prostredia a spôsob zverejnenia nového verejného kľúča.
c) procedúry obnovy pre prípad, že súkromný kľúč certifikačnej autority je skompromitovaný. Procedúry popisujú spôsob obnovy bezpečného prostredia a spôsob zverejnenia nového verejného kľúča.
d) procedúry certifikačnej autority pre prevádzku a obnovu prevádzky v prípade prírodnej katastrofy a pred obnovou bezpečného prevádzkového prostredia v pôvodných alebo náhradných prevádzkových priestoroch.

4.9. Skončenie činnosti certifikačnej autority
Procesy súvisiace so skončením činnosti certifikačnej autority a zverejnením oznámenia o skončení činnosti vrátane archivácie podkladov.

5. FYZICKÉ, PROCEDURÁLNE A PERSONÁLNE BEZPEČNOSTNÉ OPATRENIA
Popis bezpečnostných opatrení certifikačnej autority na zabezpečenie bezpečnej prevádzky a činnosti. V rámci popisovaných opatrení je samostatná pozornosť venovaná certifikačnej autorite, adresárovým službám, registračnej autorite, ako aj používateľom.

5.1. Opatrenia na fyzickú bezpečnosť
Popis fyzických bezpečnostných opatraní súvisiacich s prevádzkovými priestormi certifikačnej autority. Popisované oblasti zahŕňajú
a) lokalizáciu a konštrukciu prevádzkových priestorov,
b) fyzický prístup,
c) napájanie a vzduchotechniku,
d) rozvody vody a kanalizácie,
e) protipožiarne opatrenia,
f) uchovávanie médií,
g) odpadové hospodárstvo,
h) záložné prevádzkové priestory.

5.2. Procedurálne opatrenia
Popis bezpečnostne kritických rolí a ich zodpovedností súvisiacich so zabezpečením prevádzky. Počet osôb požadovaných na splnenie každej úlohy. Požiadavky na identifikáciu a autentifikáciu definovaných rolí sa môžu tiež formulovať v tejto časti.

5.3. Personálne bezpečnostné opatrenia
Definovanie požiadaviek na
a) procedúry preverovania osôb súvisiacich s obsadzovaním bezpečnostne kritických rolí, ako aj ďalšieho personálu certifikačnej autority,
b) požiadavky na školenia a procedúry vykonávania školení pracovníkov,
c) požiadavky na interval preškoľovania personálu,
d) požiadavky na frekvenciu a rotáciu pracovníkov v rámci rolí v prevádzke,
e) sankcie za neautorizovanú činnosť, neautorizované využívanie pridelených práv a prístupu k systémov,
f) bezpečnostné požiadavky na zmluvne zabezpečované činnosti,
g) dokumentáciu poskytovanú jednotlivým pracovníkom.

6. TECHNICKÉ BEZPEČNOSTNÉ OPATRENIA
Popis technických bezpečnostných opatrení certifikačnej autority na ochranu kryptografických kľúčov a aktivačných údajov ako heslá, PIN-y, kľúče atď. Táto časť môže tiež definovať požiadavky na adresárové služby a ďalšie subjekty, napr. registračné autority súvisiace s ochranou kryptografických kľúčov a kritických bezpečnostných parametrov. Popis technických bezpečnostných opatrení využívaných na bezpečné generovanie párov kľúčov, autentifikáciu používateľov, vydávanie certifikátov, zrušenie certifikátov, audit a archiváciu.

6.1. Generovanie a inštalácia kľúčov
Generovanie a inštaláciu páru kľúčov treba popísať pre vydavateľa certifikátov, registračné autority, adresárové služby, držiteľov certifikátov a používateľov. Rozpracúvajú sa tieto oblasti:
a) kto generuje pár súkromného a verejného kľúča pre daný subjekt,
b) akým spôsobom sa súkromný kľúč bezpečne poskytne danému subjektu,
c) akým spôsobom sa verejný kľúč subjektu bezpečne poskytne vydavateľovi certifikátu,
d) ak je subjektom certifikačná autorita, akým spôsobom sa jej verejný kľúč bezpečne poskytne používateľom,
e) akú dĺžku majú kľúče,
f) kto generuje parametre verejného kľúča,
g) ako sa kvalita parametrov kontroluje v procese generovania kľúčov,

h) ako sa kľúče generujú softvérovými alebo hardvérovými prostriedkami,
i) na aké použitie sa kľúč generuje, resp. na aké účely je jeho používanie obmedzené.

6.2. Ochrana súkromného kľúča
Všetky subjekty musia analyzovať požiadavky na ochranu súkromného kľúča
a) aké štandardy sa vyžadujú pre modul generujúci kľúče, napr. FIPS 140-2,
b) ak je súkromný kľúč pod kontrolou N osôb z celkového počtu M osôb, treba stanoviť parametre; prípad zdvojenej kontroly je špeciálnym prípadom tohto princípu, kde N = 2, M = 2,
c) ak je možnosť rekonštrukcie súkromného kľúča, určiť, kto je vykonávateľom rekonštrukcie, akou formou sa príslušný kľúč rekonštruuje a aké sú bezpečnostné opatrenia v takomto systéme; pod rekonštrukciou súkromného kľúča sa chápe metóda tzv. „key escrow“,
d) ak je súkromný kľúč zálohovaný, určiť, kto vykonáva zálohovanie, akým spôsobom sa zálohovanie vykonáva a ako sa záloha chráni,
e) ak je súkromný kľúč archivovaný, určiť kto vykonáva archiváciu, akým spôsobom sa archivácia vykonáva a ako sa archivovaný kľúč chráni,
f) kto vkladá súkromný kľúč do kryptografického modulu, akým spôsobom sa kľúč vkladá a akým spôsobom sa súkromný kľúč v kryptografickom module uchováva,
g) kto môže aktivovať a používať súkromný kľúč, akým spôsobom sa aktivácia vykonáva, napr. prihlásenie používateľa, PIN číslo, token, automaticky. V prípade aktivácie kľúča, ako dlho je kľúč aktivovaný – jednorazovo, na určitý čas, neobmedzene.
h) kto a akým spôsobom môže deaktivovať súkromný kľúč,
i) kto a akým spôsobom môže zničiť súkromný kľúč.

6.3. Manažment párových dát
Popis ďalších aspektov manažmentu párových dát pre všetky subjekty
a) či sa verejný kľúč archivuje, ak áno, kto vykonáva archiváciu a aké sú bezpečnostné opatrenia,
b) aké sú časové intervaly používania pre súkromné a verejné kľúče.

6.4. Aktivačné údaje
Popis bezpečnostných opatrení na ochranu aktivačných údajov pre celý životný cyklus aktivačných údajov od ich generovania po používanie, archiváciu a zničenie. Pre aktivačné údaje treba riešiť analogické problémy ako pri ochrane kľúčov.

6.5. Počítačové bezpečnostné opatrenia
Popis počítačových bezpečnostných opatrení, napr. používanie bezpečných systémov, riadenie prístupu, audit, testovanie bezpečnosti a penetračné testovanie. Môže byť popísaný aj spôsob získavania produktov, hodnotenie bezpečnosti počítačového systému, napr. na báze medzinárodnej normy ISO IEC 15408, požiadavky na vyhodnocovanie a testovanie produktov, ich certifikáciu a akreditáciu.

6.6. Bezpečnostné opatrenia na vývoj a riadenie bezpečnosti
Popis bezpečnostných opatrení na vývoj, napr. bezpečnosť vývojového prostredia, bezpečnosť vývojového tímu, bezpečnosť systému riadenia konfigurácií a údržby, vývojové postupy, modularita, využívanie návrhu zabezpečujúceho odolnosť proti výpadkom a chybám.
Opatrenia na riadenie bezpečnosti môžu popisovať vykonávané testy zamerané na zistenie súladu systémov a sietí s definovanými štandardmi. Tieto prostriedky môžu byť zamerané na kontrolu integrity bezpečnostného softvéru, firmvéru a hardvéru na zabezpečenie ich správnej a kontrolovanej prevádzky.

6.7. Sieťové bezpečnostné opatrenia
Opatrenia na ochranu sieťovej infraštruktúry vrátane využívania firewallov.

6.8. Opatrenia pre kryptografické moduly
Opatrenia na ochranu návrh a využívanie kryptografických modulov, určenie rozhrania a okolia modulu, vstupy/výstupy, role a služby, stavový diagram, fyzická a softvérová bezpečnosť, zhoda so schválenými algoritmami, elektromagnetická kompatibilita a vnútorné testy. Požiadavky môžu byť definované referenciou používaného štandardu, napr. FIPS 140-2.

7. PROFILY CERTIFIKÁTOV A ZOZNAMOV ZRUŠENÝCH CERTIFIKÁTOV
Popis profilov certifikátov a zoznamu zrušených certifikátov.

7.1. Profil certifikátu
Formát, obsah a nastavenie typických hodnôt jednotlivých položiek vydávaných certifikátov.

7.2. Profil zoznamu zrušených certifikátov
Formát a obsah zoznamu zrušených certifikátov.

8. ADMINISTRÁCIA ŠPECIFIKÁCIÍ
Spôsob spravovania a aktualizácie certifikačného poriadku a pravidiel na výkon certifikačných činností.

8.1. Zmenové procedúry
Procedúry realizácie zmien v prípade potreby aktualizácie alebo zmeny certifikačného poriadku. Obsahuje
a) zoznam súčastí špecifikácií, ktoré sa môžu zmeniť bez oznámenia a bez zmien identifikátora certifikačného poriadku,

b) zoznam súčastí špecifikácie, ktoré sa môžu zmeniť po uplynutí oznamovacieho intervalu bez zmien identifikátora certifikačného poriadku. Procedúry na oznamovanie zmien sa popisujú tiež vrátane termínov na pripomienkovanie a zapracovanie pripomienok, mechanizmov na záverečné zapracovanie zmien pred zavedením zmien.
c) zoznam súčastí špecifikácie, ktorých zmena vyžaduje zmenu identifikátora certifikačného poriadku.

8.2. Procedúry na zverejňovania a upozornenie
a) zoznam dokumentov, informácií a procedúr, ktoré existujú, ale nezverejňujú sa,
b) mechanizmy na distribuovanie certifikačného poriadku vrátane riadenia prístupov v takejto distribúcii.

8.3. Procedúry na schvaľovanie
Spôsob určenia zhody prípadného špecifického certifikačného poriadku so všeobecným certifikačným poriadkom.