62

VYHLÁŠKA
Národného bezpečnostného úradu

z 10. marca 2014,

ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 133/2009 Z. z. o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách a pravidlách na výkon certifikačných činností

Národný bezpečnostný úrad podľa § 14 ods. 1 písm. j) a ods. 2 zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov ustanovuje:

Čl. I

Vyhláška Národného bezpečnostného úradu č. 133/2009 Z. z. o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách a pravidlách na výkon certifikačných činností sa mení a dopĺňa takto:

1. V úvodnej vete sa slová „§ 14 ods. 1 písm. j)“ nahrádzajú slovami „§ 14 ods. 1 písm. j) a ods. 2“.

2. Slovo „žiadateľ“ v príslušnom gramatickom tvare sa v celom texte návrhu vyhlášky nahrádza slovami „žiadateľ o certifikát“ v príslušnom gramatickom tvare.

3. V § 9 ods. 3 sa za slová „produktu pre elektronický podpis“ vkladajú slová „alebo produktu pre elektronickú pečať“ a za slová „produkt pre elektronický podpis“ sa vkladajú slová „alebo produkt pre elektronickú pečať“.

4. V § 9 ods. 5 písm. f) sa za slovo „podpis“ vkladajú slová „alebo prostriedku pre elektronickú pečať“.

5. V § 9 ods. 5 písm. g), § 9 ods. 6 a § 12 ods. 1 sa za slovo „podpis“ vkladajú slová „alebo produktu pre elektronickú pečať“.

6. V § 12 ods. 2 písm. a) sa na konci pripájajú tieto slová: „alebo produktom pre elektronickú pečať“.

7. V § 12 ods. 2 písm. b) a § 14 ods. 2 písm. i) sa na konci pripájajú tieto slová: „alebo produktu pre elektronickú pečať“.

8. V § 14 ods. 2 písm. d) sa za slová „poruchách produktu pre elektronický podpis“ vkladajú slová „alebo produktu pre elektronickú pečať“ a za slová „činnosť produktu pre elektronický podpis“ sa vkladajú slová „alebo produktu pre elektronickú pečať“.

9. V § 14 ods. 2 písm. k) sa na konci pripájajú tieto slová: „alebo v produkte pre elektronickú pečať“.

10. V § 15 ods. 1 sa na konci pripája táto veta: „Pravidlá na výkon certifikačných činností vychádzajú z obsahu a štruktúry certifikačného poriadku.“.

11. Prílohy č. 1 a 2 vrátane nadpisov znejú:

„**Príloha č. 1**
k vyhláške č. 133/2009 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 tiež kontaktné informácie o certifikačnej autorite, najmä adresu elektronickej pošty, telefonický a faxový kontakt.

2. VŠEOBECNÉ USTANOVENIA
Základné východiská pre legislatívne vzťahy a procedúry poskytovania akreditovaných certifikačných služieb.

2.1. Povinnosti
Záväzky všetkých subjektov vstupujúcich do procesov súvisiacich s poskytovaním akreditovaných certifikačných služieb.
Definícia záväzkov všetkých subjektov vstupujúcich do procesov súvisiacich s certifikátmi a časovými pečiatkami
a) certifikačnej autority,
b) registračnej autority,
c) žiadateľa o certifikát 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
Opis zodpovednosti každého subjektu za
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 vrátane jej presného rozsahu.

2.4. Riešenie sporov
Určenie spôsobu interpretácie certifikačného poriadku a spôsobu riešenia sporov.

2.5. Poplatky
Špecifikácia poplatkov, ktoré si certifikačná autorita alebo registračná autorita účtuje za služby spojené s vydávaním certifikátov a ich správou.

2.6. Zverejňovanie informácií
Záväzky certifikačnej autority súvisiace so zverejňovaním informácií, a to
a) publikovanie informácií o vlastných postupoch a procedúrach, vlastných certifikátoch a stave týchto certifikátov,
b) periodicita publikovania informácií,
c) požiadavky na využívanie zverejňovaných informácií spravovaných certifikačnou autoritou treťou stranou, požiadavky na využívanie adresárov spravovaných certifikačnou autoritou treťou stranou.

2.7. Audit zhody
Informácie súvisiace s pravidelnými auditmi zhody s deklarovanými záväzkami, a to
a) frekvencia a periodicita auditu,
b) identita a kvalifikácia audítora, ako aj jeho vzťah k auditovanému subjektu,
c) zoznam oblastí, ktoré sú predmetom auditu zhody,
d) zoznam opatrení realizovaných na základe výsledkov auditu.

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 práv duševného vlastníctva
Opis vlastníckych práv k certifikátom, procedúram a kľúčom.

3. IDENTIFIKÁCIA A AUTENTIFIKÁCIA
Opis procedúr súvisiacich s autentifikáciou žiadateľa o certifikát pri prvom vydaní certifikátu, pri zrušení 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, ak bol existujúci certifikát zrušený.

3.4. Žiadosť o zrušenie certifikátu
Procesy súvisiace so spracovaním požiadaviek na identifikáciu subjektu pri žiadosti o zrušenie certifikátu.

4. PREVÁDZKOVÉ POŽIADAVKY
Opis procedúr súvisiacich s vydávaním certifikátov.

4.1. Žiadosť o vydanie certifikátu
Procesy súvisiace so zaregistrovaním žiadateľa o certifikát a s vystavením žiadosti o vydanie certifikátu.

4.2. Vydanie certifikátu
Procesy súvisiace s vydaním certifikátu a informovaním žiadateľa o certifikát 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 sú
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) určenie periodicity publikovania zoznamu zrušených certifikátov,
f) požiadavky na používateľov certifikátov na sledovanie zoznamu zrušených certifikátov,
g) opis 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, ak dôvodom zrušenia certifikátu je kompromitácia súkromného kľúča.

4.5. Procedúry pre audit bezpečnosti
Procesy súvisiace so zaznamenávaním prevádzkových udalostí a systému auditu sú
a) typy zaznamenávaných prevádzkových 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 záznamov so zameraním na
a) typy zaznamenávaných udalostí,
b) lehotu uchovávania archívnych záznamov,
c) prístupové práva a ochranu archívnych záznamov proti modifikácii a proti vymazaniu,
d) zálohovanie archívnych záznamov,
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 s riešením havarijných situácií. Každá z týchto oblastí sa rozpracúva samostatne a ide o procedúry
a) na obnovu činností, vrátane činností počas samotnej havárie, ak výpočtové zdroje, programové vybavenie alebo údaje certifikačnej autority sú poškodené alebo je podozrenie, že sú poškodené; procedúry opisujú spôsob obnovenia bezpečného prostredia, určenia, ktoré certifikáty sa zrušia, či možno ďalej používať súkromný kľúč certifikačnej autority, ako sa nový verejný kľúč zverejní,
b) obnovy, ak certifikát certifikačnej autority je zrušený; procedúry opisujú spôsob obnovy bezpečného prostredia a spôsob zverejnenia nového verejného kľúča,
c) obnovy, ak súkromný kľúč certifikačnej autority je skompromitovaný; procedúry opisujú spôsob obnovy bezpečného prostredia a spôsob zverejnenia nového verejného kľúča,
d) certifikačnej autority pre prevádzku a obnovu prevádzky v prípade havarijných situácií (napríklad katastrofy prírodnej alebo inej povahy) 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
Opis bezpečnostných opatrení certifikačnej autority na zabezpečenie bezpečnej prevádzky a činnosti. V rámci opisovaných opatrení je samostatná pozornosť venovaná certifikačnej autorite, adresárovým službám, registračnej autorite, ako aj používateľom.

5.1. Opatrenia na fyzickú bezpečnosť
Opis fyzických bezpečnostných opatrení súvisiacich s prevádzkovými priestormi certifikačnej autority. Opisované oblasti zahŕňajú

a) lokalizáciu a konštrukciu prevádzkových priestorov,
b) fyzický prístup,
c) elektrické napájanie a vzduchotechniku,
d) rozvody vody a kanalizácie,
e) opatrenia ochrany pred požiarmi,
f) uchovávanie technických nosičov dát,
g) nakladanie s odpadmi,
h) záložné prevádzkové priestory.

5.2. Procedurálne opatrenia
Opis 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 formulovať v tejto časti.

5.3. Personálne bezpečnostné opatrenia
Personálne bezpečnostné opatrenia obsahujú
a) požiadavky na 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 systémom,
f) bezpečnostné požiadavky na zmluvne zabezpečované činnosti,
g) požiadavky na dokumentáciu poskytovanú jednotlivým pracovníkom.

6. TECHNICKÉ BEZPEČNOSTNÉ OPATRENIA
Opis technických bezpečnostných opatrení certifikačnej autority na ochranu kryptografických kľúčov a aktivačných údajov, ako sú napríklad heslá, PIN čísla, kľúče. Táto časť môže definovať požiadavky na adresárové služby a ďalšie subjekty, napríklad registračné autority súvisiace s ochranou kryptografických kľúčov a kritických bezpečnostných parametrov. Opis 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 inštalácia páru kľúčov sa opisuje pre vydavateľa certifikátov, registračné autority, adresárové služby, držiteľov certifikátov a používateľov certifikátov. Rozpracúvajú sa oblasti, v ktorých sa identifikuje,
a) kto generuje pár súkromného a verejného kľúča pre daný subjekt,
b) spôsob bezpečného poskytnutia súkromného kľúča danému subjektu,
c) spôsob bezpečného poskytnutia súkromného kľúča daného subjektu vydavateľovi certifikátu,
d) spôsob bezpečného poskytnutia verejného kľúča certifikačnej autority používateľom certifikátu,
e) akú dĺžku majú kľúče,
f) kto generuje parametre verejného kľúča,
g) kontrola kvality parametrov v procese generovania kľúčov,
h) spôsob generovania kľúčov softvérovými alebo hardvérovými prostriedkami,
i) spôsob použitia, na ktorý sa kľúč generuje alebo na aké účely je jeho používanie obmedzené.

6.2. Ochrana súkromného kľúča
Analyzujú sa požiadavky na ochranu súkromného kľúča, a to
a) aké štandardy sa vyžadujú pre modul generujúci kľúče, napríklad 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, určuje sa, kto je vykonávateľom rekonštrukcie, akou formou sa príslušný kľúč rekonštruuje a aké sú bezpečnostné opatrenia v takomto systéme; rekonštrukciou súkromného kľúča sa rozumie metóda tzv. „key escrow“,
d) ak je súkromný kľúč zálohovaný, určuje sa, kto vykonáva zálohovanie, akým spôsobom sa zálohovanie vykonáva a ako sa záloha chráni,
e) ak je súkromný kľúč archivovaný, určuje sa, 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, napríklad prihlásenie používateľa, PIN číslo, token, automaticky; pri aktivácii 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
Opis ďalších aspektov manažmentu párových dát pre všetky subjekty obsahuje údaje,
a) či sa verejný kľúč archivuje, ak áno, kto vykonáva archiváciu a aké sú bezpečnostné opatrenia,
b) o časových intervaloch používania párových dát pre súkromné kľúče a verejné kľúče.

6.4. Aktivačné údaje
Opis 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
Opis počítačových bezpečnostných opatrení, napríklad používanie bezpečných systémov, riadenie prístupu, audit, testovanie bezpečnosti a penetračné testovanie. Môže byť popísaný aj spôsob získavania produktov, hodnotenie bezpečnosti počítačového systému, napríklad podľa technickej normy,[6]) požiadavky na vyhodnocovanie a testovanie produktov, ich certifikáciu a akreditáciu.

6.6. Bezpečnostné opatrenia na vývoj a riadenie bezpečnosti
Opis bezpečnostných opatrení na vývoj, napríklad 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 opisovať 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 bezpečnosť a softvérová bezpečnosť, zhoda so schválenými algoritmami, elektromagnetická kompatibilita a vnútorné testy. Požiadavky môžu byť definované referenciou používaného štandardu, napríklad FIPS 140-2.

7. PROFILY CERTIFIKÁTOV A ZOZNAMOV ZRUŠENÝCH CERTIFIKÁTOV
Opis 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 pre potrebu aktualizácie alebo zmeny certifikačného poriadku, ktoré obsahujú zoznam súčastí špecifikácií,
a) ktoré sa môžu zmeniť bez oznámenia a bez zmien identifikátora certifikačného poriadku,
b) ktoré sa môžu zmeniť po uplynutí oznamovacieho intervalu bez zmien identifikátora certifikačného poriadku; procedúry na oznamovanie zmien sa opisujú tiež vrátane termínov na pripomienkovanie a zapracovanie pripomienok, mechanizmov na záverečné zapracovanie zmien pred zavedením zmien,
c) ktorých zmena vyžaduje zmenu identifikátora certifikačného poriadku.

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

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

Príloha č. 2
k vyhláške č. 133/2009 Z. z.

ŠTRUKTÚRA PRAVIDIEL NA VÝKON CERTIFIKAČNÝCH ČINNOSTÍ

Štruktúra pravidiel na výkon certifikačných činností je zhodná so štruktúrou podľa prílohy č. 1 a obsahuje informácie, ako certifikačná autorita plní požiadavky podľa certifikačného poriadku identifikovaného objektovým identifikátorom.

Dokument pravidiel na výkon certifikačných činností obsahuje najmenej jeden objektový identifikátor certifikačného poriadku a odkaz na adresu webového sídla, na ktorom sa nachádza certifikačný poriadok definujúci požiadavky identifikované objektovým identifikátorom.“.

Poznámka pod čiarou k odkazu 6 znie:

„[6]) Súbor ISO/IEC 15408 Information technology. Security techniques. Evaluation criteria for IT security (Informačné technológie. Bezpečnostné techniky. Kritériá na hodnotenie bezpečnosti IT).“.

Čl. II

Táto vyhláška nadobúda účinnosť 15. marca 2014.

Jozef Magala v. r.