



Finančné riaditeľstvo Slovenskej republiky

Certifikácia chráneného dátového úložiska a pokladničného programu e-kasa klienta - on-line registračnej pokladnice

Obsah

História zmien a ich popis	3
Pojmy	3
Skratky	3
1. Postup konania o certifikácii.....	4
2. Požiadavky na funkčnosť a konštrukciu PPEKK a CHDÚ.....	5
A. Požiadavky na PPEKK	5
B. Požiadavky CHDÚ	7
3. Odporúčania pre certifikáciu a konštrukcia CHDÚ a PPEKK	10

História zmien a ich popis

Verzia dokumentu	Dátum zmeny	Popis zmeny
1.0	14.12.2018	Vytvorenie prvej finálnej verzie dokumentu
1.1	09.01.2019	Odstránenie povinnosti tlače slovného spojenia „úhrada poukazom“ a čísla JÚP na tlačovom výstupe NEODOSLANÉ DÁTOVÉ SPRÁVY v časti A bod 4
1.2	09.05.2019	Úprava časti A bod 4
1.3	19.06.2019	Úprava textácie výnimky v bode 3 podbod 6 a doplnenie výkladu k výnimke uvedenej v bode 3 podbod 6 za účelom jednoznačného výkladu tohto bodu
1.4	11.07.2019	Odstránenie podbodu 2 z bodu 3

Pojmy

Pojem	Význam
System e-kasa	Prostredie zriadené finančným riaditeľstvom, ktoré slúži na evidenciu dátových správ zasielaných prostredníctvom pokladnice e-kasa klient
On-line registračná pokladnica	Súbor pokladničného programu, chráneného dátového úložiska, hardverových prostriedkov, ktoré zabezpečujú komunikáciu so systémom e-kasa prostredníctvom integračného rozhrania, ktoré zverejní Finančné riaditeľstvo Slovenskej republiky na svojom webovom sídle a ďalších prostriedkov, ktoré zabezpečujú plnenie povinností podľa tohto zákona
Pokladničný program	Program on-line registračnej pokladnice, ktorý zabezpečuje splnenie požiadaviek podľa § 4a ods. 2
Chránené dátové úložisko	Zabezpečené technické zariadenie, ktoré zabezpečuje jednorazový a trvalý nešifrovaný zápis dátových správ a ostatných údajov vytlačených alebo odoslaných on-line registračnou pokladnicou; ďalšie požiadavky na chránené dátové úložisko určí finančné riaditeľstvo na svojom webovom sídle
Identifikačné údaje	Súbor údajov potrebných na vyhotovenie pokladničného dokladu, dokladu označeného slovami „NEPLATNÝ DOKLAD“, „VKLAD“ alebo „VÝBER“, ktoré jednoznačne identifikujú on-line registračnú pokladnicu podnikateľa
Autentifikačné údaje	Údaje, ktoré umožňujú overiť identitu on-line registračnej pokladnice pri komunikácii so systémom e-kasa.

Skratky

Skratka	Význam
PPEKK	Pokladničný program e-kasa klienta - online registračnej pokladnice
CHDÚ	Chránené dátové úložisko
FW CHDÚ	Programové vybavenie chráneného dátového úložiska (firmvér)
SW	Aplikačný/nadstavbový program
PRN	Tlačiareň
FRSR	Finančné riaditeľstvo Slovenskej republiky
KPEKK	Kód pokladnice e-kasa klient – online registračnej pokladnice
PD	Pokladničný doklad
JÚP	Jednouúčelový poukaz

1. Postup konania o certifikácii

V zmysle § 4c pripravovanej novely zákona č. 289/2008 Z. z. o používaní elektronickej registračnej pokladnice a o zmene a doplnení zákona Slovenskej národnej rady č. 511/1992 Zb. o správe daní a poplatkov a o zmenách v sústave územných finančných orgánov v znení neskorších predpisov v znení neskorších predpisov (*d'alej len „zákon č. 289/2008 Z. z.“*) vykonáva konanie o certifikácii PPEKK a CHDÚ FRSR.

Konanie o certifikácii začína na základe žiadosti výrobcu, dovozcu alebo distribútora PPEKK a CHDÚ. **Prílohou žiadosti sú doklady a podklady uvedené v § 4c ods. 2 a ods. 4 a doklady a podklady, ktoré zverejní FRSR na svojom webovom sídle (§ 4c ods. 3).**

FRSR po doručení žiadosti vykoná kontrolu doručených príloh. Výrobca, dovozca alebo distribútor PPEKK a CHDÚ po doručení žiadosti a kontrole zaslaných príloh **vykoná na FRSR kompiláciu zdrojových kódov PPEKK a FW CHDÚ (ak CHDÚ obsahuje riadiaci FW). Predmetom certifikácie budú len výsledky kompilácie.**

FRSR overí splnenie požiadaviek na PPEKK a CHDÚ podľa § 4a ods. 2 zákona č. 289/2008 Z. z. a v prípade splnenia požiadaviek vydá rozhodnutie o certifikácii PPEKK a CHDÚ. V rozhodnutí o certifikácii sa uvedie názov, verzia a jedinečný identifikátor PPEKK a CHDÚ. Rozhodnutie o certifikácii je platné najviac päť rokov odo dňa nadobudnutia právoplatnosti.

Ak PPEKK a CHDÚ nespĺňa niektorú z požiadaviek podľa § 4a ods. 2 zákona č. 289/2008 Z. z. alebo ak výrobca, dovozca alebo distribútor PPEKK a CHDÚ nepredloží všetky doklady alebo veci uvedené v § 4c ods. 2 a ods. 4 zákona č. 289/2008 Z. z. a ktoré zverejní FRSR na svojom webovom sídle (§ 4c ods. 3), FRSR vydá rozhodnutie o zamietnutí certifikácie.

FRSR je povinné o žiadosti rozhodnúť do 90 dní od začatia konania o certifikácii.

Výrobca, dovozca alebo distribútor PPEKK a CHDÚ je povinný oznámiť FRSR každú aktualizáciu PPEKK spolu s popisom vykonaných zmien. Súčasťou oznámenia je aj aktualizovaná dokumentácia vrátane zdrojových kódov PPEKK spolu so skompilovanou aktualizovanou verziou **zdrojových kódov PPEKK a FW CHDÚ (ak CHDÚ obsahuje riadiaci FW)**. FRSR posúdi vykonané zmeny a ak tieto majú vplyv na požiadavky na PPEKK podľa § 4a ods. 2 zákona č. 289/2008 Z. z. alebo na výsledky testovacích scenárov podľa § 4c ods. 2 písm. c) zákona č. 289/2008 Z. z., vyzve výrobcu, dovozcu alebo distribútora PPEKK a CHDÚ, aby postupoval primerane podľa § 4c ods. 2 zákona č. 289/2008 Z. z. Pri zmene alebo pri úprave CHDÚ sa primerane postupuje podľa vyššie uvedeného.

Výrobca, dovozca alebo distribútor PPEKK a CHDÚ je povinný predať podnikateľovi len taký PPEKK a CHDÚ, na ktoré FRSR vydalo rozhodnutie o certifikácii.

PPEKK a CHDÚ podliehajú certifikácii spoločne a nie je možné ich certifikovať, predávať a ani používať samostatne.

2. Požiadavky na funkčnosť a konštrukciu PPEKK a CHDÚ

A. Požiadavky na PPEKK

1. Kompilácia zdrojových kódov, ktoré boli odovzdané ako príloha k žiadosti o certifikáciu, sa vykoná na FRSSR. Výstupný PPEKK sa podpíše certifikátom podľa písmena A bodu 2 na FRSSR.
2. Výstupný PPEKK musí výrobca, dovozca alebo distribútor podpísať certifikátom, ktorý spĺňa nasledovné podmienky:
 - i. certifikát musí byť od certifikačnej authority, musí byť štandardne dostupnými nástrojmi overiteľný a musí obsahovať funkcionality časovej pečiatky (*expirácia certifikátu nemôže mať vplyv na činnosť PPEKK alebo on-line registračnej pokladnice ako celku*),
 - ii. výrobca, dovozca alebo distribútor musí zabezpečiť certifikát použitý na podpísanie PPEKK voči krádeži alebo zneužitiu a to, že certifikát nebude použitý na iné účely, o čom vydá výrobca, dovozca alebo distribútor písomné prehlásenie,
 - iii. stratu, krádež alebo zneužitie certifikátu použitého na podpis PPEKK bezodkladne oznámi FRSSR,
 - iv. výrobca, dovozca alebo distribútor je povinný použiť certifikát, ktorý je v čase podania žiadosti o certifikáciu považovaný za bezpečný.
3. Použitie účinných a v čase podania žiadosti o certifikáciu neprelomených anti-reverse engineering ochrán, pričom ich popis výrobca, dovozca alebo distribútor predloží v konaní o certifikácii (*predpokladá sa použitie napríklad packer-ov, obfuscator-ov, TPM modul a podobne*).
4. PPEKK resp. FW CHDÚ musí obsahovať jednoduchú a ľahko prístupnú funkcionality na vytvorenie binárneho obrazu podľa písmena B bod 9 a na vytlačenie všetkých neodoslaných dátových správ v nižšie definovanej štruktúre. Funkcionality na vytlačenie neodoslaných dátových správ musí umožňovať vytlačenie všetkých aktuálne neodoslaných dátových správ ako aj filtrovanie podľa dátumu, času a čísla dokladu (výberom od-do). Spôsob konštrukcie a umiestnenie tejto funkcionality v PPEKK resp. FW CHDÚ si určí výrobca, dovozca alebo distribútor. Aj tlač neodoslaných dátových správ sa ukladá do CHDÚ v zmysle písmena B bod 6 ii. Výrobca, dovozca alebo distribútor nie je povinný vytvoriť prístupnú funkcionality na vytvorenie binárneho obrazu a na vytlačenie všetkých neodoslaných dátových správ v prípade, ak to nie je technicky realizovateľné (*technická realizovateľnosť bude posúdená v konaní o certifikácii v závislosti od konštrukcie PPEKK a CHDÚ, pričom však samotná funkcionality musí byť v PPEKK alebo CHDÚ vytvorená za účelom jej integrovania do aplikačného SW*). Výsledný tlačový výstup neodoslaných dátových správ obsahuje nasledovnú štruktúru údajov (*tlačí sa len pravá časť so zvýrazneným písmom, popisné údaje v ľavej časti sa netlačia, štruktúra a obsah údajov v pravej časti je ilustračný*):

Názov tlačového výstupu

KPEKK

jedinečný identifikátor PPEKK a CHDÚ

Dátum a čas tlače neodoslaných dátových správ

Zvolený filter

NEODOSLANÉ DÁTOVÉ SPRÁVY

8882012345678001

6a7bc8d786e4f523f490e8r1a7ab683a1e3e5f7f

26.11.2018;13:26:51

dátum, čas, číslo dokladu

GPS/adresa/EČV (platí pri prenosnej pokladnici)

48.742435;19.139584;Lazovna 63,Banska Bystrica;BB111AA

///Pokladničný doklad///

poradové číslo PD

00001

dátum a čas vyhotovenia PD

22.11.2018;14:52:23

označenie/množstvo/sadzba/cena

chlieb;1x;1,50;20;1,50

označenie/množstvo/sadzba/cena

šunka;200g;6,79;20;1,36

základ dane/sadzba/daň

1,49;20;0,37

celková suma platenej ceny 1,86
identifikátor PD (vrátenie/oprava) O-C01070A9201448C99070A920141
unikátny identifikátor kupujúceho (ak bol zadany) 44112244
QR kód QR kód

///Pokladničný doklad - úhrada faktúry///

poradové číslo 00011
dátum a čas vyhotovenia PD 22.11.2018;18:42:23
číslo faktúry DF25/2018
celková suma platenej ceny 1200,00
unikátny identifikátor kupujúceho (ak bol zadany) 44112244
QR kód QR kód

///Pokladničný doklad - výmena JÚP///

poradové číslo 00058
dátum a čas vyhotovenia PD 22.11.2018;21:50:30
označenie/množstvo/sadzba/cena pobyt;1x;189,00;20;189,00
celková suma platenej ceny 189,00
unikátny identifikátor kupujúceho (ak bol zadany) 44112244
QR kód QR kód

GPS/adresa/EČV (platí pri prenosnej pokladnici) 48.732329;19.141847;Miletičova 42,Bratislava;BB333AA

///Pokladničný doklad - úhrada faktúry - výmena JUP///

poradové číslo 00059
dátum a čas vyhotovenia PD 22.11.2018;21:52:23
číslo faktúry DF15/2018
celková suma platenej ceny 180,00
unikátny identifikátor kupujúceho (ak bol zadany) SK2211111111
QR kód QR kód

///Neplatný doklad///

poradové číslo 00060
slová "NEPLATNÝ DOKLAD" NEPLATNÝ DOKLAD
dátum a čas vyhotovenia PD 22.11.2018;22:12:23
označenie/množstvo/sadzba/cena espresso;1x;1,50;20;1,50
označenie/množstvo/sadzba/cena croissant;1x;2,00;20;2,00
základ dane/sadzba/daň 2,80;20;0,70
celková suma platenej ceny 3,50

///Vklad///

poradové číslo 00061
dátum a čas vyhotovenia PD 22.11.2018;22:20:00
slovo "VKLAD" VKLAD
suma vkladu 200,00

///Výber///

poradové číslo 00071
dátum a čas vyhotovenia PD 22.11.2018;22:44:00
slovo "VÝBER" VÝBER
suma výberu 650,00

///Zaevidovanie údajov z paragónu///

poradové číslo 00178
označenie/množstvo/sadzba/cena presso;1x;1,50;20;1,50
označenie/množstvo/sadzba/cena bábovka;1x;3,00;20;3,00

základ dane/sadzba/daň	3,60;20;0,90
celková suma platenej ceny	4,50
identifikátor PD (vrátenie/oprava)	O-C01070A9201448C99070A920141
unikátny identifikátor kupujúceho (ak bol zadany)	44112244
poradové číslo paragónu	00001
dátum a čas vyhotovenia paragónu	22.11.2018;22:58
dátum zaevidovania paragónu v PPEKK	22.11.2018
QR kód	QR kód

- Po odoslaní dátovej správy, prípadne opätovného on-line spojenia, sa PPEKK pokúsi o automatické (nezávisle od používateľa PPEKK) odoslanie všetkých predtým neodoslaných dátových správ (v prípade ak existujú). PPEKK musí mať funkcionality na manuálne odoslanie neodoslaných dátových správ.
- PPEKK musí spĺňať ostatné požiadavky uvedené v § 4a zákona č. 289/2008 Z. z.

B. Požiadavky CHDÚ

- Kompilácia zdrojových kódov, ktoré boli odovzdané ako príloha k žiadosti o certifikáciu sa vykoná na FRSSR. Výstupný FW CHDÚ sa podpíše certifikátom podľa písmena A bodu 2 na FRSSR (v prípade, ak konštrukcia CHDÚ neumožní nahrať FW CHDÚ do CHDÚ zo strany FRSSR, vykoná toto nahrať výrobca, dovozca alebo distribútor na FRSSR).
- CHDÚ musí umožniť nahrať len takého FW CHDÚ, ktorý je podpísaný platným certifikátom, to neplatí, ak je nahrať FW do CHDU možné len jednorázovo pri výrobe.
- CHDÚ musí byť zariadenie typu WORM (*Write Once Read Many*) tzn. žiadny už raz zapísaný bit nesmie byť možné prepísať, funkcionality čítania je však zachovaná bez obmedzenia. Kapacita CHDÚ pre ukladanie údajov podľa písmena B bod 6 i, ii, iii je minimálne 4 GB (*odporúča sa 8 GB*). Ak výrobca, dovozca alebo distribútor ukladá iné údaje (*písmeno B bod 6 iv*), zaplnenie časti CHDÚ vyhradenej pre tieto údaje nemôže spôsobiť nefunkčnosť/zablokovanie CHDÚ.
- Výrobca, dovozca alebo distribútor je povinný použiť vhodnú metódu na zabezpečenie jednorazového a trvalého zápisu údajov do pamäte CHDÚ. V prípade hardvérového riešenia musia byť kontakty súčiastok, ktoré tvoria CHDÚ (*s výnimkou komunikačného portu*) používateľsky neprístupné. Je nutné použiť vhodnú neodstrániteľnú hmotu, ktorou budú jednotlivé súčiastky zaliate (*výrobca, dovozca alebo distribútor môže navrhnúť alebo použiť aj iný vhodný a bezpečný spôsob ochrany – napríklad technológiu tretej strany, kde je WORM zariadenie zabezpečené štandardným výrobným procesom (napr. špecializované priemyselné SD karty)*). V prípade softvérového riešenia jednorazového a trvalého zápisu do pamäte CHDÚ môže byť tento bod zabezpečený použitím na to vhodnej technológie (v tomto prípade nie je nutné chrániť kontakty súčiastok).
- Údaje podľa bodu 6 uložené na CHDÚ nesmú byť šifrované ani komprimované.
- Ukladanie údajov do CHDÚ:
 - dátové správy (*Popis integračného rozhrania systému e-kasa (2018.07.23_Integr_rozhranie.pdf)*) – aj neúspešne odoslaná dátová správa sa ukladá do CHDÚ (*bez ohľadu na počet pokusov o odoslanie*),
 - formát 1:1 sekvencií, ktoré boli použité na tlač celého tlačového výstupu, resp. komunikácia s PRN pri tlači daného celého tlačového výstupu (*platí pre všetky tlačové výstupy, t.j. pokladničné doklady, vklady, výbery, neplatné doklady, objednávky, cenovky, uzávierky, dodacie listy, faktúry a pod.*). Ukladajú sa tu všetky doklady, ktoré boli vytlačené bez ohľadu na to, či boli odoslané do e-kasa systému,

- iii. pre pokladničné doklady zaslané v elektronickej podobe postačuje uloženie dátovej správy (*bod 6 ii sa tu nevyžaduje*),
 - iv. iné údaje môžu byť ukladané do CHDÚ avšak rovnako sa na ne vzťahuje podmienka jednorazového a trvalého zápisu. Tieto údaje musia byť súčasťou binárneho obrazu uvedeného v bode 9 avšak nemusia byť súčasťou exportu dát v zmysle bodu 9 i.
7. CHDÚ obsahuje miesto na uloženie minimálne 20 autentifikačných a identifikačných údajov, pričom aktuálne platná môže byť len jedna verzia týchto údajov. Pre účely evidencie tržieb sa používa vždy len posledná platná zostava autentifikačných a identifikačných údajov. Nahratie autentifikačných a identifikačných údajov musí byť štandardne používateľský prístupné.
8. Podpisový certifikát podnikateľa (súčasť autentifikačných údajov) musí byť pri podpisovaní dátových správ vyžiadaný len z CHDÚ, ak CHDÚ nebude prístupné, PPEKK nesmie podpísať dátovú správu. Na podpisovanie dátových správ sa použije vždy posledný platný podpisový certifikát podnikateľa. V prípade zaplnenia CHDÚ nie je možné vyhotovovať, odosielať a tlačiť pokladničné doklady a ostatné doklady, ktoré sa ukladajú do CHDÚ (*odporúča sa vhodne informovať používateľa PPEKK a CHDÚ o dochádzajúcej kapacite CHDÚ*).
9. Výrobca, dovozca alebo distribútor odovzdá softvérové resp. hardvérové prostriedky (*vrátane ich zdrojových kódov – nie je nutná kompilácia na FRSR*) na vytvorenie binárneho obrazu v pomere 1:1 zo všetkých údajov uložených v CHDÚ:
- i. zároveň dodá softvérový prostriedok(y) na vyexportovanie dát z daného obrazu:
 - 1. export všetkých odoslaných dátových správ, v adresárovej štruktúre *Odoslané/YYYYMMDDhhmmss_PORADOVECISLODOKLADU.xml*.
Všetky dátové správy prislúchajúce k tomuto dokladu sa nachádzajú chronologicky usporiadané v tom istom .xml súbore (*posledná správa je odpoveď z e-kasa systému*). Rovnaký postup sa aplikuje aj v prípade odoslanej chybnéj dátovej správy,
 - 2. export všetkých neodoslaných dátových správ, v adresárovej štruktúre *Neodoslané/YYYYMMDDhhmmss_PORADOVECISLODOKLADU.xml*.
Všetky dátové správy prislúchajúce k tomuto dokladu sa nachádzajú chronologicky usporiadané v tom istom .xml súbore,
 - 3. export všetkých ostatných dokladov v binárnom formáte do súboru *Ostatne.bin*,
 - 4. export všetkých dátových správ (§ 8a ods. 6 zákona č. 289/2008 Z. z.) v jednom súbore *GPS.xml* zoradené v chronologickom poradí (*vrátane odpovedí z e-kasa systému*).
10. Komunikácia medzi PPEKK a CHDÚ (*FW CHDÚ*) musí byť zabezpečená použitím asymetrického šifrovania, pričom verejný kľúč musí byť uložený v PPEKK a súkromný kľúč musí byť uložený v CHDÚ (*zmena týchto kľúčov podlieha novému konaniu o certifikácii*), táto časť neplatí pre výnimky uvedené v bode 3 podbod 5 tohto materiálu:
- i. kľúče na komunikáciu medzi PPEKK a CHDÚ (*FW CHDÚ*) si môže výrobca, dovozca alebo distribútor vygenerovať. Na komunikáciu medzi PPEKK a CHDÚ (*FW CHDÚ*) nie je možné použiť kľúče, ktoré sú súčasťou certifikátu, ktorý bol použitý na podpis PPEKK resp. *FW CHDÚ (písmeno A bod 1 a písmeno B bod 1)*,
 - ii. výrobca, dovozca alebo distribútor musí zabezpečiť kľúče použité na komunikáciu medzi PPEKK a CHDÚ (*FW CHDÚ*) voči krádeži alebo zneužitiu a to, že kľúče nebudú použité na iné účely, o čom vydá výrobca, dovozca alebo distribútor písomné prehlásenie,
 - iii. výrobca, dovozca alebo distribútor stratu, krádež alebo zneužitie kľúčov použitých na komunikáciu medzi PPEKK a CHDÚ (*FW CHDÚ*) bezodkladne oznámi FRSR,

- iv. kľúče použité na komunikáciu medzi PPEKK a CHDÚ (*FW CHDÚ*) nesmú byť v nešifrovanej forme súčasťou exportu údajov podľa písmena A bod 4 a písmena B bod 9. V prípade, že kľúče použité na komunikáciu medzi PPEKK a CHDÚ (*FW CHDÚ*) v šifrovanej forme budú súčasťou tohto exportu, výrobca, dovozca alebo distribútor je povinný zabezpečiť použitie dostatočne silného šifrovania, aby nedošlo k ich zneužitiu,
 - v. výrobca, dovozca alebo distribútor je povinný použiť šifrovacie metódy, ktoré sú v čase podania žiadosti o certifikáciu považované za bezpečné.
11. Je nepripustné nefunkčnosť/zablokovanie CHDÚ z dôvodu servisných prehliadok alebo iných vynútených servisných zásahov (okrem zaplnenia minimálnej kapacity alebo poruchy CHDÚ).
 12. Postupnosť krokov ukladania dát a komunikácie v rámci PPEKK, CHDÚ a servera e-kasa musí byť navrhnutá tak, aby nebolo možno modifikovať ukladané, odosielané a tlačené údaje.
 13. CHDÚ musí spĺňať ostatné požiadavky uvedené v § 4a zákona č. 289/2008 Z. z.

3. Odporúčania pre certifikáciu a konštrukcia CHDÚ a PPEKK

1. Pokladničný program

Pre účely certifikácie sa odporúča predkladať PPEKK vo forme „middleware“ (stredná vrstva, napríklad vo forme „tlačového manažéra“) z dôvodu, aby nebolo potrebné certifikovať kompletný aplikačný SW (napr. účtovný, skladový a iný obdobný SW) a zároveň, aby výrobca, dovozca alebo distribútor PPEKK a CHDÚ nemusel každú zmenu aplikačného SW oznamovať v zmysle § 4c ods. 10 zákona č. 289/2008 Z. z.

2. Tlačový výstup

Výrobca, dovozca a distribútor PPEKK a CHDÚ je povinný zabezpečiť, aby všetky tlačové výstupy, ktoré boli vytlačené cez PRN (ktorá je súčasťou on-line registračnej pokladnice), boli uložené v CHDÚ (§ 4a ods. 2 písm. m) zákona č. 289/2008 Z. z.).

3. Export všetkých ostatných dokladov v binárnom formáte do súboru Ostatne.bin (písmeno B, bod 9 i, bod 3)

Export údajov musí byť v chronologickej forme a v prípade, že pri použitej PRN nie je text tlačových výstupov štandardne čitateľný (čitateľný znamená tlačiiteľné ASCII znaky odpovedajúce vytlačeným znakom na tlačových výstupoch), tak konverzia do čitateľnej formy musí byť súčasťou predloženého softvérového nástroja (k certifikácii sa predkladá aj dokumentácia konverzie).

4. Odporúčanie pre šifrovacie metódy

Asymetrické šifrovanie je povinné len pri počiatočnej výmene kľúčov (ako pri TLS), následne sa môžu používať symetrické algoritmy.

Bezpečnosť algoritmov sa posudzuje na základe verejne publikovaných odporúčaní (napríklad NIST Special Publication 800-131A Revision 1, November 2015). Z uvedeného vyplýva, že za bezpečné symetrické šifry sú považované „AES-128, AES-192, AES-256 and three-key TDEA“. Dané šifry sa akceptujú v ľubovoľnom móde operácie okrem ECB (Electronic Codebook). Z daného dokumentu taktiež vyplývajú minimálne dĺžky digitálnych podpisových kľúčov:

„DSA: $\text{len}(p) \geq 2048$ AND $\text{len}(q) \geq 224$

RSA: $\text{len}(n) \geq 2048$

ECDSA: $\text{len}(n) \geq 224$ “

V prípade Hash funkcií je povolené používať iba „SHA-2 family (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256)“ alebo „SHA-3 family (SHA3-224, SHA3-256, SHA3-384, and SHA3-512)“. **SHA1 nie je akceptovateľná pre podpisové resp. bezpečnostné použitia.**

Vzhľadom na potencionálnu limitáciu embedded zariadení pri používaní symetrického šifrovania, sa umožňuje výrobcovi pre účely symetrického šifrovania používať aj algoritmus ChaCha20 (implementovaného podľa RFC8439). Daný algoritmus je minimálne 3 krát rýchlejší ako AES bez použitia špeciálnych inštrukcií a preto môže byť z hľadiska HW nárokov vhodnejší.

Pre všetky ďalšie otázky ohľadom akceptovateľnosti zabezpečenia odporúčame prečítať NIST Special Publication 800-131A Revision 1, November 2015.

5. PPEKK a CHDÚ tvoria/netvoria jeden celok

Pokiaľ PPEKK a CHDÚ tvoria jeden neoddeliteľný celok, tak nie je nutné používať šifrovanie medzi PPEKK a CHDÚ, avšak vyžaduje sa, aby PPEKK a CHDÚ boli zaliate hmotou resp. inak vhodne chránené (viď písmeno B bod 4). Ak

CHDÚ ako samostatný funkčný celok bez ohľadu na periférne obvody zabezpečení, že všetky tlačové výstupy sú v ňom uložené, tak nemusí byť šifrovaná komunikácia medzi ním a PPEKK.

V prípade, že PPEKK a CHDÚ netvorí jeden celok alebo CHDÚ ako samostatný funkčný celok nezabezpečí uloženie všetkých tlačových výstupov, tak sa postupuje v zmysle tohto dokumentu.

Výklad výnimky:

Výnimky uvedené v bode 3 podbod 6 sa aplikujú nasledovne:

1. Zariadenie, kde PPEKK a CHDÚ tvoria jeden funkčný celok (nie je povinnosť šifrovania)
2. Zariadenie, kde PPEKK a CHDÚ netvorí jeden funkčný celok, avšak CHDÚ ako samostatný funkčný celok bez ohľadu na periférne obvody zabezpečí, že všetky tlačové výstupy sú v ňom uložené (nie je povinnosť šifrovania, ide prevažne o CHDÚ typu „odchytávač“ tlačí)
3. Zariadenie, kde PPEKK a CHDÚ netvorí jeden funkčný celok, avšak komunikácia medzi PPEKK a CHDÚ prebieha cez ďalšie zariadenie (spravidla pôvodný fiskálny modul) – šifrovanie je povinné
4. Zariadenia, kde PPEKK a CHDÚ netvorí jeden funkčný celok, avšak zariadenie je jednoúčelové a dodatočne zabezpečené, túto podmienku spĺňajú výhradne platobné terminály – šifrovanie nie je povinné
5. Iné zariadenie neuvedené v bodoch 1-4 – vždy sa posudzuje predložené zariadenie a následne sa určí či je alebo nie je povinnosť šifrovať komunikáciu medzi PPEKK a CHDÚ.

6. Kópia pokladničného dokladu

Pre účely splnenia požiadavky uvedenej v § 4a ods. 2 písm. g) zákona č. 289/2008 Z. z. sa kópia pokladničného dokladu rekonštruje z dátovej správy uloženej v CHDÚ. Kópia pokladničného dokladu musí obsahovať všetky náležitosti podľa § 8 zákona č. 289/2008 Z. z. a nesmie obsahovať údaje uvedené v § 4 ods. 2 písm. g) zákona č. 289/2008 Z. z. (v prípade, ak pokladničný doklad obsahoval iné nepovinné texty, tieto musia byť vytlačené na kópii pokladničného dokladu).

7. Kapacita CHDÚ

Odporúčame, aby výrobca, dovozca alebo distribútor pri tvorbe CHDÚ zvolil takú kapacitu, ktorá podľa jeho prepočtov umožní ukladanie údajov v priemere aspoň 3 roky resp. aspoň 300 000 ks pokladničných dokladov.

Vypracovalo: Finančné riaditeľstvo SR