



Finančné riaditeľstvo Slovenskej republiky

Certifikácia chráneného dátového úložiska a pokladničného programu e-kasa klienta pre on-line registračnú pokladnicu aj softvérovú on-line registračnú pokladnicu

Obsah

História zmien a ich popis	3
Pojmy	3
Skratky	4
1. Postup konania o certifikácii.....	5
2. Požiadavky na funkčnosť a konštrukciu PPPEK a CHDÚ podľa § 2 písm. j) bod 1 zákona č. 384/2025 Z. z.	6
A. Požiadavky na PPPEK	6
B. Požiadavky CHDÚ podľa § 2 písm. j) bod 1 zákona č. 384/2025 Z. z.	6
C. Požiadavky na OS Android	9
3. Požiadavky na funkčnosť a konštrukciu PPPEK a CHDÚ podľa § 2 písm. j) bod 2 zákona č. 384/2025 Z. z., požiadavky na vzdialené prostredie	10
A. CHDÚ, ktoré nie je umiestnené vo vzdialenom prostredí	10
B. CHDÚ, ktoré je umiestnené vo vzdialenom prostredí	14
C. Vzdialené prostredie	16
4. Odporúčania pre certifikáciu a konštrukciu CHDÚ a PPPEK	17

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
1.5	31.12.2021	Zrušenie povinnosti testovania unikátneho identifikátor kupujúceho v zmysle nálezů Ústavného súdu č. č. k. PL. ÚS 25/2019-117 z 10. novembra 2021
1.6	10.11.2023	Aktualizácia a doplnenie dokumentu (bod 2 písmeno A podbod 4; bod 2 písmeno B podbod 9 a 10; bod 2 písmeno C). Úprava bodu 3 primerane k zmenám z bodu 2, pridanie bodu 3 podbod 7 a 8.
1.6.1	13.03.2024	Oprava bodu 2 písmeno A podbod 4. Doplnenie výkladu k bod 2 písmeno B podbod 9 písmeno i bod 3.
1.7	22.11.2024	Úprava a doplnenie dokumentu (bod 2 písmeno A podbod 4; bod 2 písmeno B podbod 9; bod 3 podbod 5, 7 a 8
1.8	08.12.2025	Zpracovanie požiadaviek pre softvérovú on-line registračnú pokladnicu a vzdialené prostredie. Odstránenie „Neodoslaných dátových správ“ z bodu 2 písmeno A podbod 4, úprava minimálnej kapacity CHDÚ v bode 2 písmeno B podbod 3

Pojmy

Pojem	Význam
Systém pre pokladnice eKasa	Prostredie zriadené finančným riaditeľstvom, ktoré slúži na evidenciu dátových správ zasielaných prostredníctvom pokladnice eKasa
Pokladnica eKasa	1.on-line registračná pokladnica 2.softvérová on-line registračná pokladnica alebo 3.virtuálna registračná pokladnica
On-line registračná pokladnica	Súbor pokladničného programu, chráneného dátového úložiska podľa písmena j) prvého bodu, hardvérových prostriedkov, ktoré zabezpečujú komunikáciu so systémom pre pokladnice eKasa prostredníctvom integračného rozhrania a ďalších prostriedkov, ktoré zabezpečujú plnenie povinností podľa tohto zákona; integračné rozhranie určí Finančné riaditeľstvo Slovenskej republiky (ďalej len „finančné riaditeľstvo“) a uverejní ho na svojom webovom sídle
Softvérová on-line registračná pokladnica	Súbor pokladničného programu, chráneného dátového úložiska podľa písmena j) druhého bodu, ktoré sú spustené na hardvérových prostriedkoch, ktoré zabezpečujú komunikáciu so systémom pre pokladnice eKasa prostredníctvom integračného rozhrania, pričom súbor pokladničného programu a chráneného dátového úložiska podľa písmena j) druhého bodu môže byť umiestnený na vzdialenom prostredí, a ďalších prostriedkov, ktoré zabezpečujú plnenie povinností podľa tohto zákona; integračné rozhranie určí finančné riaditeľstvo a uverejní ho na svojom webovom sídle
Pokladničný program	Program on-line registračnej pokladnice alebo softvérovej on-line registračnej pokladnice, ktorý zabezpečuje splnenie požiadaviek podľa § 5 ods. 3 a 4
Chránené dátové úložisko	1. 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 a uverejní ich na svojom webovom sídle, 2. súbor softvérových prostriedkov, ktoré sú spustené na hardvérových prostriedkoch, a ktoré zabezpečujú integritu do nich ukladaných dátových správ a ostatných údajov vytlačených alebo odoslaných softvérovou on-line registračnou pokladnicou; ďalšie požiadavky na chránené dátové úložisko určí finančné riaditeľstvo a uverejní ich na svojom webovom sídle

Vzdialené prostredie	Server, ktorý používa výrobca, dovozca alebo distribútor pokladničného programu a chráneného dátového úložiska podľa písmena j) druhého bodu; ďalšie požiadavky na vzdialené prostredie určí finančné riaditeľstvo a uverejní ich na svojom webovom sídle
Identifikačné údaje	Súbor údajov potrebných na vyhotovenie pokladničného dokladu, ktoré jednoznačne identifikujú on-line registračnú pokladnicu alebo softvérovú on-line registračnú pokladnicu predávajúceho
Autentifikačné údaje	Údaje, ktoré umožňujú overiť identitu on-line registračnej pokladnice alebo softvérovej on-line registračnej pokladnice pri komunikácii so systémom pre pokladnicu eKasa
Uvedenie pokladnice eKasa do prevádzky	Prvé zaslanie údajov podľa písmen r) až t) do systému pre pokladnicu eKasa alebo ich uloženie v chránenom dátovom úložisku pri prekročení hraničnej doby odozvy
NOP	NOP "Notifikátor okamžitých platieb" - notifikačný systém v správe FRSR pre podporu okamžitých platieb, vrátane platieb QR kódom

Skratky

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

1. Postup konania o certifikácii

V zmysle § 6 zákona č. 384/2025 Z. z. o evidencii tržieb a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 384/2025 Z. z.“) vykonáva konanie o certifikácii PPPEK a CHDÚ FRSR.

Konanie o certifikácii PPPEK a CHDÚ začína na základe žiadosti výrobcu, dovozcu alebo distribútora PPPEK a CHDÚ. Predmetom konania o certifikácii PPPEK a CHDÚ podľa § 2 písm. j) druhého bodu zákona č. 384/2025 Z. z. môže byť aj vzdialené prostredie. **Prílohou žiadosti sú doklady a podklady uvedené v § 6 ods. 2 zákona č. 384/2025 Z. z. (aj zverejnené na webovom sídle FRSR) a uvedené v § 6 ods. 4 zákona č. 384/2025 Z. z.**

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

FRSR overí splnenie požiadaviek na PPPEK a CHDÚ podľa § 5 ods. 3 alebo § 5 ods. 4 zákona č. 384/2025 Z. z. a v prípade splnenia požiadaviek vydá rozhodnutie o certifikácii PPPEK a CHDÚ. V rozhodnutí o certifikácii sa uvedie názov, verzia a jedinečný identifikátor PPPEK a CHDÚ prípadne vzdialeného prostredia, ak bolo súčasťou konania o certifikácii. Rozhodnutie o certifikácii je platné najviac päť rokov odo dňa nadobudnutia právoplatnosti.

Ak PPPEK a CHDÚ (prípadne vzdialené prostredie ak je súčasťou konania o certifikácii) nespĺňa niektorú z požiadaviek podľa § 5 ods. 3 alebo § 5 ods. 4 zákona č. 384/2025 Z. z. alebo ak výrobca, dovozca alebo distribútor PPPEK a CHDÚ nepredloží všetky doklady alebo veci uvedené v § 6 ods. 2 zákona č. 384/2025 Z. z. (aj zverejnené na webovom sídle FRSR) a uvedené v § 6 ods. 4 zákona č. 384/2025 Z. z. FRSR vydá rozhodnutie o zamietnutí certifikácie.

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

Výrobca, dovozca alebo distribútor PPPEK a CHDÚ je povinný oznámiť FRSR každú aktualizáciu PPPEK spolu s popisom vykonaných zmien. Súčasťou oznámenia je aj aktualizovaná dokumentácia vrátane zdrojových kódov PPPEK spolu so skompilovanou aktualizovanou verziou **zdrojových kódov PPPEK a FW CHDÚ (ak CHDÚ obsahuje riadiaci FW)**. FRSR posúdi vykonané zmeny a ak tieto majú vplyv na požiadavky na PPPEK podľa § 5 ods. 3 alebo § 5 ods. 4 zákona č. 384/2025 Z. z. alebo na výsledky testovacích scenárov podľa § 6 ods. 2 písm. c) zákona č. 384/2025 Z. z., vyzve výrobcu, dovozcu alebo distribútora PPPEK a CHDÚ, aby postupoval primerane podľa § 6 ods. 2 zákona č. 384/2025 Z. z. Pri zmene alebo pri úprave CHDÚ alebo pri zmene alebo úprave vzdialeného prostredia sa primerane postupuje podľa vyššie uvedeného.

Výrobca, dovozca alebo distribútor PPPEK a CHDÚ je povinný predať predávajúcemu len taký PPPEK a CHDÚ a poskytnúť len také vzdialené prostredie, na ktoré FRSR vydalo rozhodnutie o certifikácii.

PPPEK a CHDÚ podliehajú certifikácii spoločne a nie je možné ich certifikovať samostatne.

PPPEK, CHDÚ a vzdialené prostredie podliehajú certifikácii spoločne a nie je možné ich certifikovať samostatne.

2. Požiadavky na funkčnosť a konštrukciu PPPEK a CHDÚ podľa § 2 písm. j) bod 1 zákona č. 384/2025 Z. z.

A. Požiadavky na PPPEK

1. Kompilácia zdrojových kódov, ktoré boli odovzdané ako príloha k žiadosti o certifikáciu, sa vykoná na FRSR. Výstupný PPPEK sa podpíše certifikátom podľa písmena A bodu 2 na FRSR.
2. Výstupný PPPEK 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 funkčnosť časovej pečiatky (*expirácia certifikátu nemôže mať vplyv na činnosť PPPEK alebo on-line registračnej pokladnice ako celku*),
 - ii. výrobca, dovozca alebo distribútor musí zabezpečiť certifikát použitý na podpísanie PPPEK 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 PPPEK bezodkladne oznámi FRSR,
 - 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. PPPEK resp. FW CHDÚ musí obsahovať jednoduchú a ľahko prístupnú funkčnosť na vytvorenie binárneho obrazu podľa písmena B bod 9.
5. Po odoslaní dátovej správy, prípadne opätovného on-line spojenia, sa PPPEK pokúsi o automatické (*nezavisle od používateľa PPPEK*) odoslanie všetkých predtým neodoslaných dátových správ (*v prípade ak existujú*). PPPEK musí mať funkčnosť na manuálne odoslanie neodoslaných dátových správ.
6. PPPEK musí spĺňať ostatné požiadavky uvedené v § 5 ods. 3 zákona č. 384/2025 Z. z.

B. Požiadavky CHDÚ podľa § 2 písm. j) bod 1 zákona č. 384/2025 Z. z.

1. Kompilácia zdrojových kódov, ktoré boli odovzdané ako príloha k žiadosti o certifikáciu sa vykoná na FRSR. Výstupný FW CHDÚ sa podpíše certifikátom podľa písmena A bodu 2 na FRSR (*v prípade, ak konštrukcia CHDÚ neumožní nahratie FW CHDÚ do CHDÚ zo strany FRSR, vykoná toto nahratie výrobca, dovozca alebo distribútor na FRSR*).
2. CHDÚ musí umožniť nahratie len takého FW CHDÚ, ktorý je podpísaný platným certifikátom, to neplatí, ak je nahratie FW do CHDU možné len jednorazovo pri výrobe.
3. CHDÚ musí byť zariadenie typu WORM (*Write Once Read Many*) tzn. žiadny už raz zapísaný bit nesmie byť možné prepísať, funkčnosť čítania je však zachovaná bez obmedzenia. Kapacita CHDÚ pre ukladanie údajov podľa písmena B bod 6 i, ii, iii je minimálne 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.
4. 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*) používateľský 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).

5. Údaje podľa bodu 6 uložené na CHDÚ nesmú byť šifrované ani komprimované.
6. Ukladanie údajov do CHDÚ:
 - i. dátové správy (*Popis integračného rozhrania systému e-kasa*) – aj neúspešne odoslaná dátová správa sa ukladá do CHDÚ (*bez ohľadu na počet pokusov o odoslanie*),
 - ii. 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.
 - v. JSON pre komunikáciu s NOP (len v prípade, ak je proces QR platby súčasťou PPEKK alebo CHDÚ) – odporúča sa, aby boli identifikátori QR platby priradené NOP naviazané na konkrétnu dátovú správu pokladničného dokladu.
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 prístupný.
8. Podpisový certifikát predávajúceho (súčasť autentifikačných údajov) musí byť pri podpisovaní dátových správ vyžiadaný len z CHDÚ, ak CHDÚ nebude prístupné, PPPEK nesmie podpísať dátovú správu. Na podpisovanie dátových správ sa použije vždy posledný platný podpisový certifikát predávajúceho. 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 PPPEK 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. Softvérové resp. hardvérové prostriedky na vytvorenie binárneho obrazu v pomere 1:1 k CHDÚ musia byť skompilované pre OS Windows. Predkladané softvérové alebo hardvérové prostriedky na tvorbu binárneho obrazu chráneného dátového úložiska v pomere 1:1 (ako aj následné aktualizácie týchto prostriedkov) musia byť spätne kompatibilné so všetkými verziami a typmi chráneného dátového úložiska daného výrobcu, dovozcu alebo distribútora, pričom musia byť schopné automaticky identifikovať pripojené/spracovávané chránené dátové úložisko a správne vytvoriť binárny obraz v pomere 1:1.
 - i. zároveň dodá softvérový prostriedok(y) (skompilované pre OS Windows) na vyexportovanie dát z binárneho obrazu chráneného dátového úložiska, ktorý musí spĺňať rovnakú podmienku spätnej kompatibility ako softvérový/hardvérový nástroj na tvorbu binárneho obrazu chráneného dátového úložiska:

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 aktuálne 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 vytlačených pokladničných dokladov a iných dokladov chronologicky zoradených podľa dátumu vytlačenia v binárnom formáte do súboru Ostatne.bin (neobsahuje identifikačné a autentifikačné údaje a dátové správy),
 4. export všetkých dátových správ (§ 9 ods. 4 zákona č. 384/2025 Z. z.) v jednom súbore GPS.xml zoradené v chronologickom poradí (*vrátane odpovedí z e-kasa systému*),
 5. export všetkých JSON správ v rámci komunikácie s NOP v jednom súbore JSON.BIN.
10. Komunikácia medzi PPPEK a CHDÚ (*FW CHDÚ*) musí byť pri zariadení, kde PPPEK a CHDÚ netvorí jeden funkčný celok a komunikácia medzi PPPEK a CHDÚ prebieha cez ďalšie zariadenie, zabezpečená použitím asymetrického šifrovania, pričom verejný kľúč musí byť uložený v PPPEK a súkromný kľúč musí byť uložený v CHDÚ (*zmena týchto kľúčov podlieha novému konaniu o certifikácii*), táto časť neplatí pre nasledovné konštrukcie zariadenia:
- zariadenie, kde PPPEK a CHDÚ tvoria jeden funkčný celok,
 - zariadenie, kde PPPEK 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 (prevažne o CHDÚ typu „odchytač“ tlače),
 - zariadenia, kde PPPEK a CHDÚ netvorí jeden funkčný celok, avšak zariadenie je jednocelové a dodatočne zabezpečené, túto podmienku spĺňajú výhradne platobné terminály,
- Iné zariadenie vyššie neuvedené sa vždy posudzuje a následne sa určí či je alebo nie je povinnosť šifrovať komunikáciu medzi PPPEK a CHDÚ.
- Zásady asymetrického šifrovania komunikácie medzi PPPEK a CHDÚ:
- i. kľúče na komunikáciu medzi PPPEK a CHDÚ (*FW CHDÚ*) si môže výrobca, dovozca alebo distribútor vygenerovať. Na komunikáciu medzi PPPEK a CHDÚ (*FW CHDÚ*) nie je možné použiť kľúče, ktoré sú súčasťou certifikátu, ktorý bol použitý na podpis PPPEK resp. FW CHDÚ (*písmeno A bod 1 a písmeno B bod 1*),
 - ii. výrobca, dovozca alebo distribútor musí zabezpečiť kľúče použité na komunikáciu medzi PPPEK 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 PPPEK a CHDÚ (*FW CHDÚ*) bezodkladne oznámi FRSR,
 - iv. kľúče použité na komunikáciu medzi PPPEK 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 PPPEK 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 neprípustné 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 predkladaného vzájomného prepojenia PPPEK a 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 § 5 ods. 3 zákona č. 384/2025 Z. z.

C. Požiadavky na OS Android

1. Nie je možná inštalácia výrobcom digitálne nepodpísaných aplikácií v zariadení.
2. Nemožnosť externej modifikácie pamäte OS Android.
3. Ladenie cez USB/ADB musí byť zablokované.
4. Bootloader musí byť zamknutý a fastboot zablokovaný.
5. Nie je možné modifikovať a ani čítať obsah partícií na SD/EMMC na úrovni recovery.
6. Výrobca, dovozca alebo distribútor musí popísať akým spôsobom a či je možné OS Android update/upgrade.
7. Výrobca, dovozca alebo distribútor musí predložiť binárny obraz v pomere 1:1 OS Android používaný v zariadení.
8. Výrobca, dovozca alebo distribútor musí predložiť všetky heslá do nastavení zariadenia prípadne iné heslá vyžadované zariadením.
9. V prípade resetu (obnovenia zariadenia do továrenských nastavení) musí ostať, prípadne sa obnoviť (napríklad pri úspešnom pripojení na internet) PPPEK v zariadení. Všetky údaje (napr. identifikačné a autentifikačné údaje, neodoslané dátové správy a pod.) musia byť opätovne načítavané z CHDÚ.

3. Požiadavky na funkčnosť a konštrukciu PPPEK a CHDÚ podľa § 2 písm. j) bod 2 zákona č. 384/2025 Z. z., požiadavky na vzdialené prostredie

V zmysle § 2 písm. j) bod 2 a v zmysle § 2 písm. an) zákona č. 384/2025 Z. z. určuje FRSR tieto požiadavky:

- A. Pre CHDÚ, ktoré nie je umiestnené vo vzdialenom prostredí (je umiestnené lokálne na predajnom mieste)
- B. Pre CHDÚ, ktoré je umiestnené vo vzdialenom prostredí (nie je umiestnené lokálne na predajnom mieste)
- C. Vzdialené prostredie

A. CHDÚ, ktoré nie je umiestnené vo vzdialenom prostredí

Rozsah, štruktúra a miesto ukladania údajov

1. Všetky dátové správy a ostatné vytvorené, vytlačené alebo odoslané údaje/dáta sa ukladajú v CHDÚ softvérovej on-line registračnej pokladnice (ďalej len „SORP“) nešifrované a v spoločnom adresári (ďalej len „root“).
2. root musí byť prístupný minimálne na čítanie štandardnou programovou výbavou zariadenia (prehliadačom súborov/súborovým manažérom napr. Windows Explorer, Android File Manager, Apple Files a podobne), na ktorom je CHDÚ resp. SORP inštalovaná;
3. Umiestnenie root je spravidla štandardný adresár, kde aplikácie v rámci zvoleného systému ukladajú dáta, (napr. pre Windows systémy adresár „C:\ProgramData“, pre Linux systémy adresár „/srv/“, pre ostatné operačné systémy umiestnenie, ktoré sa v rámci štandardov vývoja pre danú platformu používa na ukladanie aplikačných dát, avšak zároveň je prístupná cez štandardný prehliadač súborov na danej platforme).
4. root musí byť pomenovaný rovnako ako výrobca, dovozca alebo distribútor PPPEK a CHDÚ, názov je doplnený o suffix PPPEK - napr. „C:\ProgramData\Príklad s.r.o PPPEK“ (znaky, ktoré nie sú akceptovateľné súborovým systémom daného operačného systému sú nahradené ekvivalentom bez diakritiky resp. medzerou).
5. V root sa nachádzajú adresáre, ktoré budú predstavovať jednotlivé transakcie (ďalej len „transakcia“). Transakciou sa rozumie kompletný úkon v aplikovateľnom rozsahu od odoslania/prijatia údajov a tlače, druhy transakcii:
 - i. nahratie kompletného inicializačného balíčku (identifikačných a autentifikačných údajov);
 - ii. zaevidovanie pokladničného dokladu (všetky dátové správy, tlačový výstup)
 - iii. zaevidovanie polohy (dátové správy)
 - iv. tlač ostatných údajov (tlačový výstup)
6. Transakcia má označenie/meno svojho adresára vo forme: YYMMDD-III-III-III, kde YY je 2-ciferný rok, MM je 2-ciferný mesiac, DD je 2-ciferný deň a III-III-III je 12-ciferné sekvenčné číslo začínajúce od 1 (delené na tri 4-číselné skupiny). Príklad: 250917-0000-0000-0002.
7. Transakcie sú logicky členené podľa roku a mesiaca vo forme YYMM kde YY je 2-ciferný rok a MM je 2-ciferný mesiac (napríklad celá cesta k transakcii bude: „C:\ProgramData\Príklad s.r.o PPPEK\25\09\250917-0000-0000-0002“;
8. V rámci adresára transakcie sa nachádzajú súbory prislúchajúce k danej transakcii, ktorých názov je tvorený z názvu adresára transakcie doplnený o 4-cifernú skupinu čísiel číslovaných sekvenčne od 1

pre danú transakciu identifikujúcu jednotlivé časti v chronologickom poradí s príponou podľa typu súboru:

- i. JSON pre komunikáciu s NOP (len v prípade, ak je proces QR platby súčasťou PPEKK alebo CHDÚ),
 - ii. XML pre dátové správy,
 - iii. PRN pre tlačové výstupy k danej XML správe – pokladničné doklady (formát 1:1 bez sekvencií, ktoré boli použité na tlač pokladničného dokladu, resp. komunikácia s tlačiarňou pri tlači pokladničného dokladu),
 - iv. BIN pre ostatné tlačové výstupy (formát 1:1 sekvencií, ktoré boli použité na tlač celého tlačového výstupu, resp. komunikácia s tlačiarňou pri tlači daného celého tlačového výstupu),
 - v. AUTH pre autentifikačné údaje,
 - vi. IDENT pre identifikačné údaje.
9. Pre každý súbor v adresári transakcie sa bude nachádzať rovnako pomenovaný súbor s príponou 512, ktorý bude obsahovať kontrolný súčet príslušajúceho súboru transakcie vo formáte: SHA512 súčet (hexadecimálny formát 128 znakov, všetky malým písmom), dve medzery, názov súboru, ku ktorému patrí a nový riadok LF notácia (nie CRLF bez ohľadu na systém).
10. Pre každý súbor v adresári transakcie, okrem súborov s kontrolným súčtom, sa vytvoria súbory s príponou SYNC, ktoré obsahujú synchronizačný kontrolný kód (hexadecimálny formát 128 znakov, všetky malým písmom; plus LF notácia konca riadku).

Príklad obsahu adresára transakcie:

Názov transakcie - adresára	Názov súboru	Popis hodnoty
250917-0000-0000-0001	250917-0000-0000-0001-0001.AUTH	Autentifikačné údaje
	250917-0000-0000-0001-0001.512	Kontrolný súčet
	250917-0000-0000-0001-0001.SYNC	Synchronizačný kontrolný kód
	250917-0000-0000-0001-0002.IDENT	Identifikačné údaje
	250917-0000-0000-0001-0002.512	Kontrolný súčet
	250917-0000-0000-0001-0002.SYNC	Synchronizačný kontrolný kód
250917-0000-0000-0002	250917-0000-0000-0002-0001.XML	Dátová správa odoslaná na zaevidovanie
	250917-0000-0000-0002-0001.512	Kontrolný súčet
	250917-0000-0000-0002-0001.SYNC	Synchronizačný kontrolný kód
	250917-0000-0000-0002-0002.XML	Dátová správa – odpoveď servera
	250917-0000-0000-0002-0002.512	Kontrolný súčet
	250917-0000-0000-0002-0002.SYNC	Synchronizačný kontrolný kód
	250917-0000-0000-0002-0003.PRN	Binárna forma tlačového výstupu
	250903-0000-0000-0002-0003.512	Kontrolný súčet
	250917-0000-0000-0002-0003.SYNC	Synchronizačný kontrolný kód
250917-0000-0000-0003	250917-0000-0000-0003-0001.BIN	Ostatný tlačový výstup – NEPLATNÝ DOKLAD
	250917-0000-0000-0003-0001.512	Kontrolný súčet
	250917-0000-0000-0003-0001.SYNC	Synchronizačný kontrolný kód
250917-0000-0000-0004	250917-0000-0000-0004-0001.XML	Dátová správa odoslaná na zaevidovanie - poloha SORP
	250917-0000-0000-0004-0001.512	Kontrolný súčet
	250917-0000-0000-0004-0001.SYNC	Synchronizačný kontrolný kód
	250917-0000-0000-0004-0002.XML	Dátová správa – odpoveď servera
	250917-0000-0000-0004-0002.512	Kontrolný súčet
	250917-0000-0000-0004-0002.SYNC	Synchronizačný kontrolný kód

11. Synchronizačný kontrolný kód je počítaný ako zreťazený SHA512, do ktorého vstupuje ako prvý 128 bajtový náhodný nemenný reťazec, ktorý sa nachádza v PPPEK a je schválený počas konania o certifikácii PPPEK a CHDÚ SORP (je rovnaký aj v následných nahlásených a schválených aktualizáciách). Výrobca, dovozca alebo distribútor zabezpečí jeho obfuskovanie v rámci schváleného PPPEK resp. nadväzujúcej aktualizácii PPPEK a CHDÚ SORP. Synchronizačný kontrolný kód bude ďalej tvorený zo všetkých súborov prislúchajúcich ku všetkým dovtedy existujúcim transakciám v chronologickom poradí a to vrátane súborov 512 a SYNC.

Príklad:

1. SHA512 z 128 bajtového reťazca
 2. SHA512 z prvého súboru transakcií
 3. SHA512 z reťazcov kroku 1 a 2
 4. SHA512 z ďalšieho súboru transakcií
 5. SHA512 z reťazcov kroku 3 a 4
 6. a tak ďalej pre všetky zostávajúce transakcie.
12. root neobsahuje iné súbory ako uvedené v tomto dokumente.
 13. Autentifikačné a identifikačné údaje sa nahrávajú spolu v rámci jednej transakcie (uvedené platí aj v prípade aktualizácie identifikačných alebo autentifikačných údajov).
 14. Kapacita CHDÚ podľa § 2 písm. j) bod 2 zákona č. 384/2025 Z. z. je minimálne 8 GB.

Integrita ukladaných údajov

15. Kontrola integrity údajov uložených v CHDÚ SORP sa vykoná vždy pri štarte (reštarte) SORP. V rámci kontroly integrity údajov uložených v CHDÚ SORP sa zo všetkých prepočíta synchronizačný kontrolný kód a porovná sa s každým jedným synchronizačným kontrolným kódom v chronologickom poradí.
16. Ak tento kód nebude zhodný, používateľ SORP je informovaný, že zlyhala kontrola integrity údajov uložených v CHDÚ SORP s presnou identifikáciou SYNC súboru, pri ktorom došlo k zlyhaniu integrity. Ďalší zápis do CHDÚ SORP nie je možný. Rovnaký postup sa uplatní aj v prípade, ak nebude nájdený root (výrobca, dovozca alebo distribútor vzhľadom na použité technológie vytvorí vhodný spôsob rozlíšenia medzi zmazaním root a uvedením SORP do prevádzky podľa § 2 písm. al) zákona č. 384/2025 Z. z.).
17. Pri kontrole integrity údajov uložených v CHDÚ SORP sa vypočíta číslo nasledujúceho pokladničného dokladu, ktoré sa použije pre ďalšiu činnosť SORP v súlade s § 5 ods. 4 písm. g) zákona č. 384/2025 Z. z.
18. Po vypnutí PPPEK na spustenej (aktívnej) SORP nie je možné zapisovať do CHDÚ SORP (a to ani po opätovnom zapnutí PPPEK) a je nutné vykonať reštart systému SORP, čím sa vykoná kontrola integrity údajov uložených v CHDÚ SORP. Spustenie zápisu do CHDÚ SORP je možné len raz po štarte SORP. Ak bol zápis do CHDÚ SORP spustený, nie je možné ho spustiť opakovane a to až do reštartovania systému SORP.

Vyhotovenie pokladničného dokladu

V zmysle § 5 ods. 4 zákona č. 384/2025 Z. z. softvérová on-line registračná pokladnica musí spĺňať tieto požiadavky:

d) vytlačenie pokladničného dokladu,

e) vytlačenie kópie pokladničného dokladu tak, aby neobsahoval identifikátor dokladu, QR kód, overovací kód predávajúceho a podpisový kód predávajúceho,

j) uloženie dátových správ a ostatných údajov vytvorených, vytlačených alebo odoslaných v chránenom dátovom úložisku a prístup k nim.
l) vyhotovenie pokladničného dokladu, a to až po zaevidovaní dátovej správy v systéme pre pokladnice eKasa,
m) elektronické vytvorenie a zaslanie alebo sprístupnenie pokladničného dokladu kupujúcemu až po zaevidovaní dátovej správy v systéme pre pokladnice eKasa,
o) zasielanie údajov podľa § 9 do systému pre pokladnice eKasa,
s) zobrazenie slov „NEPLATNÝ DOKLAD“ v každom treťom riadku na všetkých dokladoch obsahujúcich údaje o cene tovaru alebo cene služby vytlačených na softvérovej on-line registračnej pokladnici okrem pokladničného dokladu.

19. Ak nie je možné vyhotoviť (vytlačiť, elektronicky odoslať) pokladničný doklad z dôvodu nezaevidovania dátovej správy v systéme pre pokladnice eKasa, zápis ďalších dát (transakcií), iných ako transakcia k neodoslanému pokladničnému dokladu, do CHDÚ SORP nie je možný.
20. Ak systém pre pokladnice eKasa odpovie SORP niektorou z chýb uvedených v bode 2.6 Integračného rozhrania alebo chybou -1 „Systém je momentálne vyťažený, skúste prosím neskôr“, transakcia sa považuje za ukončenú (odmietnutú) a ďalší zápis do CHDÚ SORP (tvorba ďalších nových transakcií) je možná (odmietnutá transakcia nezvyšuje číselný rad pokladničných dokladov).
21. Pre účely zabezpečenia ukladania dátových správ a ostatných údajov vytvorených, vytlačených alebo odoslaných SORP v CHDÚ SORP je výrobca, dovozca alebo distribútor povinný navrhnúť proces, ktorým bezpečne a spoľahlivo odchyti tlač z ostatných aplikácií tak, aby všetky tlačené dáta na aktívnej SORP boli uložené v CHDÚ SORP ako BIN s príslušným kontrolným súčtom (512) a synchronizačným kontrolným kódom (SYNC). Pre účely zamedzenia zápisu do CHDÚ SORP musí kontrola funkčnosti odchyty tlače prebiehať na aktívnej SORP nepretržite. Narušenie funkčnosti procesu odchyty tlače musí byť identifikovateľné s následným zablokovaním možnosti ukladania dát do CHDÚ SORP. Ďalší zápis do CHDÚ SORP je možný až po reštarte SORP, overení integrity údajov uložených v SORP a znovu spustení procesu odchyty tlače. Alternatívou k procesu odchyty tlače je absolútny zákaz tlače z iných aplikácií. Proces odchyty tlače určí výrobca, dovozca alebo distribútor na základe použitého operačného systému/zariadenia SORP.

Export údajov z CHDÚ SORP

V zmysle § 10 ods. 2 zákona č. 384/2025 Z. z. predávajúci je povinný chránené dátové úložisko uchovávať do uplynutia lehoty na zánik práva vyrubiť daň alebo rozdiel dane podľa § 69 Daňového poriadku. Na požiadanie daňového úradu alebo colného úradu je predávajúci povinný sprístupniť alebo predložiť údaje z chráneného dátového úložiska za požadované obdobie v elektronickej podobe ihneď na predajnom mieste alebo v lehote určenej daňovým úradom, colným úradom alebo Kriminálnym úradom finančnej správy; rozsah, štruktúru, náležitosti a spôsob poskytnutia údajov z chráneného dátového úložiska určí finančné riaditeľstvo a uverejní ich na svojom webovom sídle.

22. Výrobca, dovozca alebo distribútor v rámci SORP (CHDÚ SORP) implementuje automatizovaný export všetkých údajov z CHDÚ SORP (root) na pamäťové médium. Táto funkcia musí automaticky fungovať po zapnutí SORP (aj na zapnutej SORP) a to aj bez prihlásenia používateľa do systému, po pripojení správne naformátovaného pamäťového média (USB) SORP vykoná automatický export nešifrovaného ZIP archívu celého obsahu CHDÚ na toto pamäťové médium.
23. USB pamäťové médium musí byť naformátované ako exFAT a musí sa v jeho root adresári nachádzať súbor **FSSR_export** (bez prípony). Ak SORP detekuje prítomnosť tohto USB pamäťového média, automaticky vykoná export požadovaných údajov na toto pamäťové médium (názov exportného súboru je **kód pokladnice YYMMDD-hhmmss.zip**, kde **YY** je 2-ciferný rok, **MM** je 2-ciferný mesiac, **DD** je 2-

ciferný deň, hh je 2-ciferná hodina, mm je 2-ciferná minúta, ss je 2-ciferná sekunda času štartu procesu exportu údajov) a vykoná jeho softvérové bezpečné odpojenie.

24. Výrobca, dovozca alebo distribútor PPPEK a CHDÚ vytvorí a predloží v rámci konania o certifikácii nástroj na overenie integrity exportu z CHDÚ (overenie súborov 512 a SYNC súborov s presnou lokalizáciou narušenia integrity).

Odovzdanie zdrojových kódov

25. Výrobca, dovozca alebo distribútor PPPEK a CHDÚ postupuje rovnako ako je uvedené v bode 2 „požiadavky na funkčnosť a konštrukciu PPPEK a CHDÚ podľa § 2 písm. j) bod 1“ tohto dokumentu.

B. CHDÚ, ktoré je umiestnené vo vzdialenom prostredí

Rozsah, štruktúra a miesto ukladania údajov

1. Všetky dátové správy a ostatné vytvorené, vytlačené alebo odoslané údaje a dáta (napríklad najmä pokladničné doklady, neplatné doklady, vklady, výbery, objednávky, dodacie listy, faktúry, uzávierky a iné podobné interné alebo externé doklady vytvorené v rámci činnosti SORP) a identifikačné a autentifikačné údaje sa ukladajú v CHDÚ SORP, ktoré je umiestnené vo vzdialenom prostredí.
2. Štruktúru, spôsob a miesto ukladania vyššie uvedených údajov a dát v CHDÚ SORP umiestnenom vo vzdialenom prostredí určí výrobca, dovozca alebo distribútor PPPEK a CHDÚ podľa použitej technológie, pričom však musí zabezpečiť export údajov z CHDÚ SORP podľa bodu 3 písmeno A, podbod 4 (*Export údajov z CHDÚ SORP*) tohto dokumentu. Štruktúru, spôsob a miesto ukladania údajov a dát uvedených v bode 1 tejto časti dokumentu v CHDÚ SORP umiestnenom vo vzdialenom prostredí výrobca, dovozca alebo distribútor PPPEK a CHDÚ dokumentuje v konaní o certifikácii.

Integrita ukladaných údajov

3. Výrobca, dovozca alebo distribútor PPPEK a CHDÚ v konaní o certifikácii dokumentuje zabezpečenie integrity a kontrolu integrity údajov ukladaných do CHDÚ SORP umiestnenom vo vzdialenom prostredí. Súčasťou mechanizmu integrity údajov uložených v CHDÚ SORP vo vzdialenom prostredí je audit log.
4. Audit log je vo formáte .csv (kompatibilný s importom do MS Office, oddeľovač tabulátor) a obsahuje:
 - Dátum a čas záznamu
 - Identifikácia používateľa
 - Identifikácia SORP (kód pokladnice) a identifikácia softvéru (napr. nadradený)
 - Zdrojová IP adresa
 - Popis vykonanej činnosti (vykonaná transakcia, vykonané úkony).
5. Pri narušení integrity údajov uložených v CHDÚ SORP umiestnenom vo vzdialenom prostredí nie je možný zápis ďalších údajov podľa § 5 ods. 4 písm. j) a k) zákona č. 384/2025 Z. z. do CHDÚ. Výrobca, dovozca alebo distribútor PPPEK a CHDÚ v konaní o certifikácii dokumentuje postup v prípade narušenia integrity údajov uložených v CHDÚ SORP umiestnenom vo vzdialenom prostredí.
6. O narušení integrity údajov uložených v CHDÚ SORP umiestnenom vo vzdialenom prostredí musí byť používateľ SORP (predávajúci) informovaný.
7. Pri kontrole integrity údajov uložených v CHDÚ SORP umiestnenom vo vzdialenom prostredí sa vypočíta číslo nasledujúceho pokladničného dokladu, ktoré sa použije pre ďalšiu činnosť SORP v súlade s § 5 ods. 4 písm. g) zákona č. 384/2025 Z. z.

Vyhotovenie pokladničného dokladu

V zmysle § 5 ods. 4 zákona č. 384/2025 Z. z. softvérová on-line registračná pokladnica musí spĺňať tieto požiadavky:

- d) vytlačenie pokladničného dokladu,
- e) vytlačenie kópie pokladničného dokladu tak, aby neobsahoval identifikátor dokladu, QR kód, overovací kód predávajúceho a podpisový kód predávajúceho,
- j) uloženie dátových správ a ostatných údajov vytvorených, vytlačených alebo odoslaných v chránenom dátovom úložisku a prístup k nim.
- l) vyhotovenie pokladničného dokladu, a to až po zaevidovaní dátovej správy v systéme pre pokladnice eKasa,
- m) elektronické vytvorenie a zaslanie alebo sprístupnenie pokladničného dokladu kupujúcemu až po zaevidovaní dátovej správy v systéme pre pokladnice eKasa,
- o) zasielanie údajov podľa § 9 do systému pre pokladnice eKasa,
- s) zobrazenie slov „NEPLATNÝ DOKLAD“ v každom treťom riadku na všetkých dokladoch obsahujúcich údaje o cene tovaru alebo cene služby vytlačených na softvérovej on-line registračnej pokladnici okrem pokladničného dokladu.

- 8. Ak nie je možné vyhotoviť (vytlačiť, elektronicky odoslať) pokladničný doklad z dôvodu nezaevidovania dátovej správy v systéme pre pokladnice eKasa, zápis ďalších dát (transakcií), iných ako transakcia k neodoslanému pokladničnému dokladu, do CHDÚ SORP umiestnenom vo vzdialenom prostredí nie je možný.
- 9. Ak systém pre pokladnice eKasa odpovie SORP niektorou z chýb uvedených v bode 2.6 Integračného rozhrania alebo chybou -1 „Systém je momentálne vyťažенý, skúste prosím neskôr“, transakcia sa považuje za ukončenú (odmietnutú) a ďalší zápis do CHDÚ SORP umiestnenom vo vzdialenom prostredí (tvorba ďalších nových transakcií) je možná (odmietnutá transakcia nezvyšuje číselný rad pokladničných dokladov).

Tlač pokladničných dokladov a iných dokladov

- 10. Pre účely zabezpečenia ukladania dátových správ a ostatných údajov vytvorených, vytlačených alebo odoslaných SORP v CHDÚ umiestnenom na vzdialenom prostredí je výrobca, dovozca alebo distribútor PPPEK a CHDÚ povinný navrhnuť proces, ktorým bezpečne a spoľahlivo odchyť tlač z ostatných aplikácií (vrátane všetkých aplikácií, ktoré s nimi komunikujú), ktoré sú spustené vo vzdialenom prostredí, kde je umiestnený pokladničný program a/alebo CHDÚ SORP alebo ostatných aplikácií, ktoré so vzdialeným prostredím komunikujú a umožňujú vyhotovenie a vytlačenie pokladničného dokladu (zápis údajov do CHDÚ SORP umiestnenom vo vzdialenom prostredí).
- 11. Pre účely zamedzenia zápisu do CHDÚ SORP umiestnenom vo vzdialenom prostredí musí kontrola funkčnosti odchyty tlače prebiehať na aktívnej SORP nepretržite. Narušenie funkčnosti procesu odchyty tlače musí byť identifikovateľné s následným zablokovaním možnosti ukladania dát do CHDÚ SORP umiestnenom na vzdialenom prostredí. Ďalší zápis do CHDÚ SORP umiestnenom na vzdialenom prostredí je možný až po overení integrity údajov uložených v CHDÚ SORP a znovu spustení procesu odchyty tlače. Alternatívou k procesu odchyty tlače je absolútny zákaz tlače z iných aplikácií. Proces odchyty tlače určí výrobca, dovozca alebo distribútor PPPEK a CHDÚ na základe použitého operačného systému/zariadenia SORP.

Export údajov z CHDÚ SORP

- 12. Export údajov z CHDÚ SORP umiestneného vo vzdialenom prostredí musí byť v rovnakom rozsahu, štruktúre a forme aká je definovaná v bode 3 písmeno A podbod 22 a 23 tohto dokumentu (názov

exportného súboru je **kód pokladnice YYMMDD-hhmmss.zip**, kde YY je 2-ciferný rok, MM je 2-ciferný mesiac, DD je 2-ciferný deň, hh je 2-ciferná hodina, mm je 2-ciferná minúta, ss je 2-ciferná sekunda času štartu procesu exportu údajov). Súčasťou exportu údajov z CHDÚ SORP je audit log umiestnený v root-e ZIP súboru exportu (názov audit logu je **audit.csv**).

13. Výrobca, dovozca alebo distribútor PPPEK a CHDÚ vytvorí a predloží v rámci konania o certifikácii nástroj na overenie integrity exportu z CHDÚ (overenie súborov 512 a SYNC súborov s presnou lokalizáciou narušenia integrity).

Odobzanie zdrojových kódov

14. Výrobca, dovozca alebo distribútor PPPEK a CHDÚ postupuje rovnako ako je uvedené v bode 2 „požiadavky na funkčnosť a konštrukciu PPPEK a CHDÚ podľa § 2 písm. j) bod 1“ tohto dokumentu“.

C. Vzdialené prostredie

1. Zabezpečuje ukladanie všetkých údajov podľa § 5 ods. 4 písm. j) a k) zákona č. 384/2025 Z. z. do CHDÚ SORP umiestnenom vo vzdialenom prostredí (uvedené sa vzťahuje aj na ostatné SW (vrátane všetkých SW, ktoré s nimi komunikujú), ktoré sú spustené vo vzdialenom prostredí, kde je umiestnený pokladničný program a/alebo CHDÚ alebo ostatné SW, ktoré so vzdialeným prostredím komunikujú a umožňujú vyhotovenie a vytlačenie pokladničného dokladu).
2. Zabezpečuje integritu všetkých údajov podľa § 5 ods. 4 písm. j) a k) zákona č. 384/2025 Z. z. uložených v CHDÚ SORP umiestnenom vo vzdialenom prostredí prípadne ďalších údajov uložených do CHDÚ SORP umiestnenom vo vzdialenom prostredí.
3. Zabezpečuje export údajov z CHDÚ SORP umiestnenom vo vzdialenom prostredí v predpísanej štruktúre, forme a rozsahu (viď bod 3 písmeno B podbod 12 a 13 tohto dokumentu).
4. Primerane zabezpečuje povinnosti uvedené v § 10 ods. 5 zákona č. 384/2025 Z. z.

Podľa § 10 ods. 5 zákona č. 384/2025 Z. z. výrobca, dovozca alebo distribútor pokladničného programu a chráneného dátového úložiska podľa § 2 písm. j) druhého bodu, ktoré sú umiestnené na vzdialenom prostredí a na ktoré bolo vydané rozhodnutie o certifikácii pokladničného programu a chráneného dátového úložiska, je povinný

- a) zabezpečiť ochranu všetkých údajov uložených v chránenom dátovom úložisku podľa § 2 písm. j) druhého bodu umiestnenom na vzdialenom prostredí pred stratou, zničením, poškodením, zneužitím, neoprávneným zásahom do nich a neoprávneným prístupom k nim; rovnako je povinný zabezpečiť ochranu autentifikačných údajov k softvérovej on-line registračnej pokladnici proti ich zneužitiu, strate alebo odcudzeniu,
- b) umožniť predávajúcemu bezodkladne získať všetky údaje uložené v chránenom dátovom úložisku podľa § 2 písm. j) druhého bodu umiestnenom na vzdialenom prostredí na účely plnenia povinností podľa tohto zákona alebo podľa osobitných predpisov,¹⁵⁾
- c) na požiadanie daňového úradu, colného úradu alebo Kriminálneho úradu finančnej správy sprístupniť alebo predložiť údaje z chráneného dátového úložiska podľa § 2 písm. j) druhého bodu umiestneného na vzdialenom prostredí; rozsah, štruktúru, náležitosti a spôsob poskytnutia údajov z chráneného dátového úložiska určí finančné riaditeľstvo a uverejní ich na svojom webovom sídle,
- d) preukázateľne odovzdať predávajúcemu všetky údaje uložené v chránenom dátovom úložisku podľa § 2 písm. j) druhého bodu umiestnenom na vzdialenom prostredí, ak bolo zrušené rozhodnutie o certifikácii pokladničného programu a chráneného dátového úložiska podľa § 2 písm. j) druhého bodu, ktoré sú umiestnené na vzdialenom prostredí, alebo ak sa ukončí činnosť vzdialeného prostredia.

4. Odporúčania pre certifikáciu a konštrukciu CHDÚ a PPPEK

1. Pokladničný program

Pre účely certifikácie sa odporúča (avšak nevyžaduje) predkladať PPPEK 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 PPPEK a CHDÚ nemusel každú zmenu aplikačného SW oznamovať v zmysle § 6 ods. 10 zákona č. 384/2025 Z. z.

2. Tlačový výstup

Výrobca, dovozca a distribútor PPPEK a CHDÚ je povinný zabezpečiť, aby všetky tlačové výstupy, ktoré boli vytlačené cez PRN (*ktorá je súčasťou on-line registračnej pokladnice alebo softvérovej on-line registračnej pokladnice*), boli uložené v CHDÚ (§ 5 ods. 3 písm. k) a § 5 ods. 4 písm. j) zákona č. 384/2025 Z. z.).

3. Export všetkých ostatných dokladov v binárnom formáte do súboru Ostatne.bin (bod 2 písmeno B, bod 9 i, bod 3)

Export údajov musí byť v chronologickej forme a v prípade, že pri použití PRN nie je text tlačových výstupov štandardne čitateľný (*čitateľný znamená tlačiteľné 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. Kópia pokladničného dokladu

Pre účely splnenia požiadavky uvedenej v § 5 ods. 3 písm. e) a § 5 ods. 4 písm. e) zákona č. 384/2025 Z. z. sa kópia pokladničného dokladu rekonštruuje z dátovej správy uloženej v CHDÚ alebo z uloženej tlačovej kópie pokladničného dokladu v CHDÚ. Kópia pokladničného dokladu nesmie obsahovať údaje uvedené v § 5 ods. 3 písm. e) a § 5 ods. 4 písm.

e) zákona č. 384/2025 Z. z. (v prípade, ak pokladničný doklad obsahoval iné nepovinné texty, tieto nemusia byť vytlačené na kópii pokladničného dokladu).

6. 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.

7. Podmienky a príklady pri evidencii pokladničných dokladov

1. Pri vystavovaní pokladničných dokladov a evidencii zliav musia byť dodržané nasledovné podmienky:
 - i. zľava sa môže evidovať na pokladničný doklad len v prípade, že je na pokladničnom doklade evidovaná položka,
 - ii. zľava sa môže evidovať na pokladničný doklad len v sadzbe dane z pridanej hodnoty (ďalej len „DPH“), v ktorej je evidovaná položka,
 - iii. výška zľavy môže byť maximálne vo výške ceny za evidovanú položku.
2. Pri predaji vratných obalov sa použije typ položky „K“ (kladná), pričom v dátovej správe sa k tejto položke použije sadzba DPH 0% (tzv. „technická sadzba“). V rámci rekapitulácie DPH (keďže ide o vratný obal) nesmie byť táto sadzba ani suma vratných obalov obsiahnutá v rekapitulácii DPH. V rámci alfanumerického označovania predávanej položky sadzbou DPH nesmie byť na pokladničnom doklade položka „vratný obal“ označená týmto údajom. Pre interný matematický výpočet sa môže údaj o vratných obaloch uvádzať pod rekapituláciou ako samostatný údaj.
3. Pri vrátení vratného obalu sa použije typ položky „VO“ (vratné obaly) pričom platia rovnaké podmienky ako v predchádzajúcom bode pri predaji vratného obalu.
4. Pri prijatí zálohy za predávaný tovar/službu sa použije typ položky „K“ (kladná) s priradením príslušnej sadzby DPH v zmysle zákona č. 222/2004 Z. z. v znení neskorších predpisov (záloha v čase jej prijatia ešte nemusí podliehať zdaneniu DPH). Pri odpočítaní zálohy sa použije typ položky „OZ“ (odpočítaná záloha), pričom musia byť dodržané nasledovné podmienky:
 - i. odpočítaná záloha sa môže evidovať na pokladničný doklad len v prípade, že je na pokladničnom doklade evidovaná položka.
5. V prípade predaja jednorúčelového poukazu („JÚP“) platí, že už v čase jeho vystavenia je známe miesto dodania tovaru alebo miesto dodania služby, na ktoré sa poukaz vzťahuje a daň splatná z tohto tovaru alebo služby. Náležitosti pokladničného dokladu pri predaji a výmene JÚP sú obsiahnuté v § 8 ods. 3 zákona č. 384/2025 Z. z.
6. Pri výmene jednorúčelového poukazu „JÚP“ sa použije typ položky „VP“ (výmena poukazu) a musia byť dodržané nasledovné podmienky:
 - i. pri výmene JÚP je povolené (nie povinné) križovať sadzby DPH (napr. JÚP v sadzbe 20% DPH a tovar (doplatok) v sadzbe 23% DPH),
 - ii. pri výmene JÚP nie je povolené evidovať JÚP samostatne na pokladničný doklad bez evidencie položky.
 - iii. pri výmene JÚP, kde hodnota JÚP a hodnota položky (tovaru/služby) na ktorú je JÚP uplatnený sú rovnaké (celková suma pokladničného dokladu bude 0,00 Eur), pokladničný doklad nemôže obsahovať žiadne alfanumerické označenie sadzby DPH pri položke ani pri JÚP a nesmie byť zobrazená žiadna rekapitulácia DPH.
 - iv. pri výmene JÚP, kde hodnota JÚP je vyššia ako hodnota položky (tovaru/služby) na ktorú je JÚP uplatnený (celková suma pokladničného dokladu bude 0,00 Eur – aj napriek tomu, že

matematicky by mala byť suma záporná), pokladničný doklad nemôže obsahovať žiadne alfanumerické označenie sadzby DPH pri položke ani pri JÚP a nesmie byť zobrazená žiadna rekapitulácia DPH.

- v. pri výmene JÚP, kde hodnota JÚP je nižšia ako hodnota položky (tovaru/služby) na ktorú je JÚP uplatnený (celková suma dokladu je vyššia ako 0,00 Eur), pokladničný doklad bude obsahovať alfanumerické označenie sadzby DPH pri položke aj pri JÚP a na pokladničnom doklade musí byť zobrazená rekapitulácia DPH pre tú časť sumy, ktorá je vyššia ako hodnota JÚP (kladná suma rozdielu medzi sumou položky a sumou JÚP).

Podmienky týkajúce sa DPH v bode i, iii, iv, v sa vzťahujú pre platiteľa DPH.

Vypracovalo: Finančné riaditeľstvo SR