Posúdenie bezpečnosti chráneného dátového úložiska (CHDÚ) systému eKasa od firmy CHDÚ, s.r.o.

O spoločnosti Nethemba

Nethemba je slovenská IT bezpečnostná spoločnosť založená v roku 2007, špecializujúca sa primárne na bezpečnosť webových a mobilných aplikácií a penetračné testy. Tvoria ju špecialisti s dlhoročnými skúsenosťami v oblasti IT bezpečnosti a svetovými bezpečnostnými certifikátmi (OSCE, OSCP, CISSP). Sme experti na tvorbu komplexných bezpečnostných auditov podľa OSSTMM metodológie ako aj detailných bezpečnostných auditov webových aplikácií podľa testovacej príručky OWASP, tiež sme spoluautori aktuálnej testovacej príručky OWASP v4. Okrem našej špecializácie na bezpečnosť webových a mobilných technológií sa špecializujeme aj na externé, intranetové a lokálne systémové audity, digitálne forenzné analýzy, audity bezdrôtových sietí, návrh ultra-bezpečných, vysoko-dostupných a škálovateľných systémov, cloud computing či školenia v oblasti bezpečnosti pre vývojárov a IT administrátorov.
Medzi naše špeciality patrí bezpečnosť RFID/NFC technológií, hĺbková analýza a tvorba exploitov, bezpečnostné audity SAP systémov či bezpečnosť TETRA a GSM sietí. Venujeme sa tiež bezpečnostnému výskumu v rôznych oblastiach, ktorý aj finančne podporujeme.
Ako prví na svete sme zverejnili „offline“ Mifare Classic cracker, ktorý umožňuje prelomiť viac ako miliardu používaných čipových kariet Mifare Classic.
Súčasne sme odhalili vážne zraniteľnosti v SMS lístkoch používaných vo veľkých stredoeurópskych mestách (Praha, Bratislava, Viedeň, Varšava, Košice), ako aj v mobilnom SMS parkovaní.
Začiatkom roka 2015 sme realizovali tiež rozsiahlu analýzu bezpečnosti platobných NFC kariet.
Aktívne sa venujeme aj ochrane digitálne súkromie (viac informácií na www.chrantesvojesukromie.sk a www.chrantesvesoukromi.cz).

Bezpečnosti sa aktívne venujeme pravidelnými príspevkami na rôznych svetových konferenciách.
Od roku 2014 každoročne organizujeme so spoločnosťou ESET vlastnú IT bezpečnostnú konferenciu Cypherconf.

Ako firma pôsobíme tiež na nemeckom (Nethemba GmbH) a španielskom trhu (Nethemba SA).

Aktuálne informácie zo sveta bezpečnosti reflektujeme na našich sociálnych sieťach:
https://facebook.com/nethemba
https://twitter.com/nethemba
https://www.linkedin.com/company/nethemba

Čo je eKasa

eKasa predstavuje systém on-line zasielania pokladničných dokladov vystavených na registračných pokladniach (ktoré používajú podnikatelia na evidenciu hotovosti) na server Finančnej správy SR. Každý vystavený doklad na pokladni sa ešte pred samotnou tlačou zašle na server eKasa – zasielajú sa základné údaje bločku (hlavička) a aj jednotlivé položky. Tým získava finančná správa prehľad o každom vystavenom doklade v reálnom čase.

eKasu na strane podnikateľa tvorí **pokladničný program eKasa klient (PPEKK)** – tým je myslený firmvér pokladnice, prípadne samostatný softvér vo forme napr. DLL knižnice. Podlieha certifikácii – na FS sú odovzdané kompletné zdrojové kódy programu PPEKK, elektronicky sa podpisuje (podpis slúži na overenie, či sa v pokladni používa softvér, ktorý bol certifikovaný). Ďalej eKasu pokladňu z pohľadu zákona tvorí **chránené dátové úložisko (CHDÚ)** – ide o pamäť, do ktorej sa dáta môžu len zapisovať, v žiadnom prípade sa nesmie dať čokoľvek už zapísané pozmeniť, prípadne odstrániť. Túto požiadavku musí spĺňovať aj samotný výrobca CHDÚ – nesmie existovať nástroj, pomocou ktorého by sa dalo niečo pozmeniť alebo vymazať. PPEKK a CHDÚ z hľadiska certifikácie vždy predstavujú jeden celok, ktorý sa certifikuje spoločne.

Do CHDÚ sa zapisujú všetky vystavené doklady (dátové správy zaslané na server FS), ako aj všetky dáta, ktoré sú zaslané na tlačiareň a následne vytlačené. V prípade výpadku internetu (keď nie je server eKasa dostupný) sa pokladničný doklad vo forme dátovej správy (XML) uloží do CHDÚ (tzv. off-line doklad). Po odstránení problémov s pripojením k serveru FS ich následne pokladňa automaticky odošle, prípadne ich odošle na pokyn obsluhy pokladne. CHDÚ primárne slúži na ochranu ešte neodoslaných dokladov na server eKasa – zabraňuje ich dodatočnej úprave, prípadne úplného vymazania ešte pred odoslaním. Pri vystavení dokladu sa do CHDÚ najskôr ukladá dátová správa (zhodná s tou, ktorá sa posiela na server FS), následne sa ukladá aj tlačová úloha – vygenerovaný pokladničný doklad aj s QR kódom.

Špecifikáciu CHDÚ vydala Finančná správa SR a je uvedená v nasledovnom dokumente:
https://www.financnasprava.sk/_img/pfsedit/dokumenty_PFS/Podnikatelia/eKasa/2019/2019.01.11_e_kasa_certif.pdf

Pokladňu eKasa môže predstavovať:

- klasická pokladňa, napr. na Slovensku najčastejšie používaná firmy ELCOM – firmvér pokladne predstavuje PPEKK, vo vnútri pokladne je CHDÚ
- eKasa tlačiareň (pôvodné fiškálne tlačiarne) – PPEKK, CHDÚ a tlačiareň tvoria jeden celok
- softvérové PPEKK a hardvérové CHDÚ – PPEKK tvorí softvér, ktorí je spustený na počítači, najčastejšie vo forme DLL knižnice, ovladača, spusteného programu na pozadí a podobne. CHDÚ sa v tomto prípade pripája spravidla k počítaču, napr. cez RS-232 alebo ethernet rozhrania. Tlačiareň musí byť pripojená k CHDÚ, aby bola splnená požiadavka „všetko, čo sa tlačí na tlačiarni, musí byť v CHDÚ“. Tu sa na predaj používa akýkoľvek pokladničný softvér, ktorý sa nemusí sa certifikovať – certifikuje sa len

PPEKK.

Hlavným cieľom zavedenia eKasy je zlepšenie výberu daní, znižovanie čiernych tržieb, obmedzenie vystavovania falošných dokladov.

Chránené dátové úložisko firmy CHDU, s.r.o.

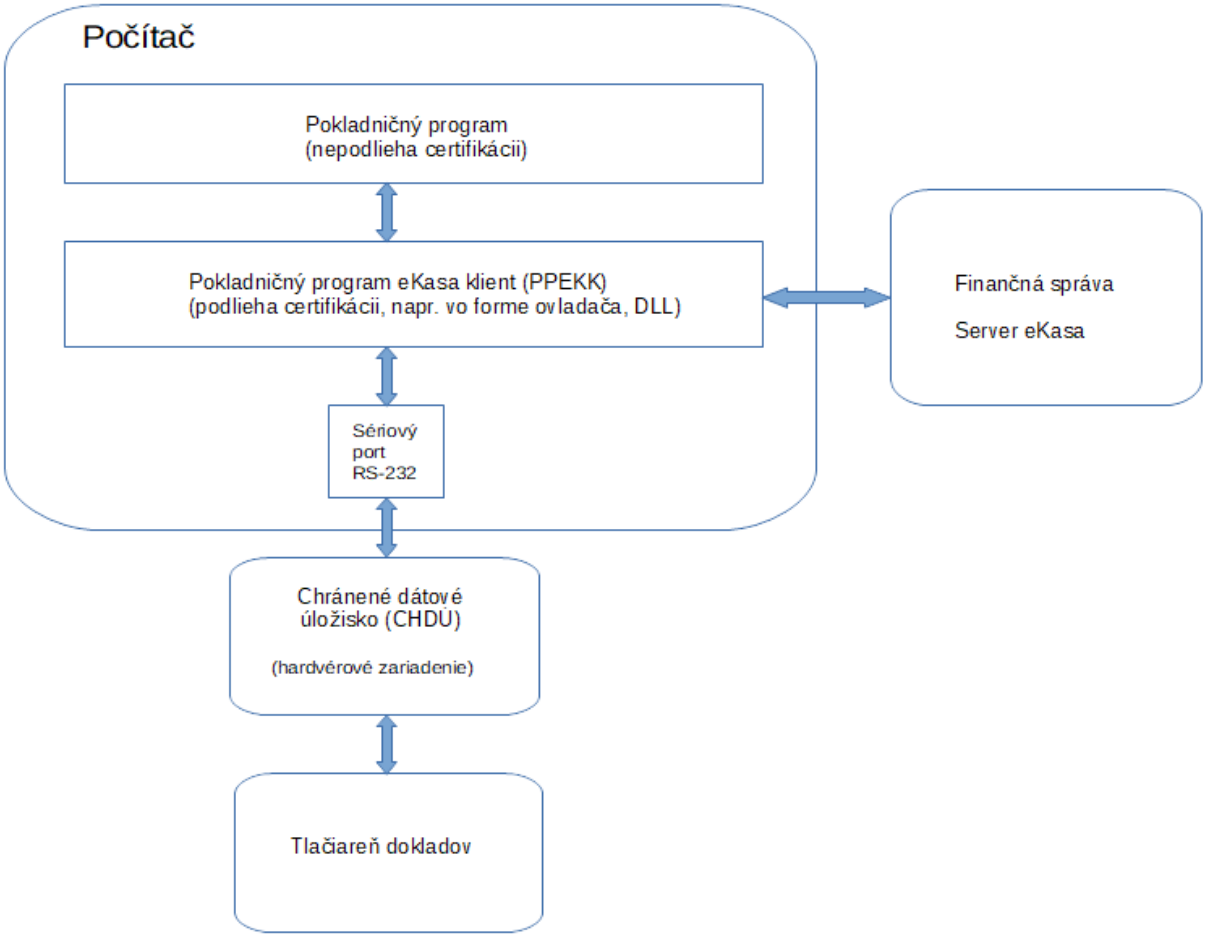
Firma CHDÚ s.r.o. dodáva CHDÚ vlastnej výroby veľkej časti certifikovaných riešení. Mnohí dodávatelia si naprogramovali vlastné PPEKK a použili CHDÚ tohto výrobcu (toto ako jeden celok certifikovali). Niektorí výrobcovia pokladničných riešení mali (prípadne ešte majú) problémy pri certifikácii vlastných riešení a použití svojho vlastného CHDÚ. Podľa ich oficiálnych (niekorých neoficiálnych) vyjadrení to nesúvisí s ich technickým riešením, ale s ochotou (neochotou) pracovníkov finančnej správy certifikovať ich riešenie. Jednoducho povedané, ak použijete CHDÚ od firmy CHDÚ, s.r.o., certifikácia riešenia je rýchla a bezproblémová, v opačnom prípade je vydanie certifikátu veľmi otázne. Niektorí výrobcovia prišli na certifikáciu s vlastným CHDÚ - ak chceli mať certifikát v dohľadnej dobe, museli použiť a aj použili CHDÚ tejto firmy.

Niektorí výrobcovia zároveň napádajú a spochybňujú technické riešenie firmy CHDU, s.r.o. Ide hlavne o komunikáciu medzi PPEKK a CHDÚ, ktorá podľa špecifikácie finančnej správy má byť šifrovaná (musí byť použitá asymetrická šifra). Samotná finančná správa však CHDÚ firmy CHDÚ s.r.o. neoficiálne udelila výnimku (nemusí používať šifrovanie) a iným dodávateľom certifikovala riešenia s týmto CHDÚ aj bez použitia šifrovania. V priebehu leta 2019 sa finančná správa pokúsila dodatočne „zlegalizovať“ výnimku šifrovania – úpravou špecifikácie a to tak, pri tomto type CHDÚ už nie je potrebné šifrovanie (pri iných typoch podmienka šifrovania zostala zachovaná).

Je dôležité šifrovanie komunikácie medzi PPEKK a CHDÚ ?

Podľa špecifikácie sa majú do CHDÚ ukladať nekomprimované a nešifrované údaje (pokladničné doklady). CHDÚ si môžete predstaviť ako obyčajnú pamäťovú kartu, na ktorej sú uložené údaje. Ak nie sú údaje na nej zašifrované a zároveň komunikácia medzi PPEKK a CHDÚ nie je šifrovaná, potencionálny útočník sa môže „postaviť do cesty“ medzi PPEKK a CHDÚ – tu môže dané dáta upravovať, prípadne ich do skutočného CHDÚ ani nezapisovať. Keďže toto technické riešenie je veľmi jednoduché (obsahuje jednoduchý komunikačný protokol bez šifrovania), veľmi jednoducho je možné naprogramovať softvérový emulátor CHDÚ – bude sa tváriť ako skutočné (fyzické) CHDÚ, avšak vystavené off-line doklady nikdy nebudú na finančnú správu zaslané – prevzatá tržba podnikateľom a vystavený off-line doklad akoby nikdy neexistoval.

Obrázok č. 1 – štandardné pripojenie CHDÚ k počítaču

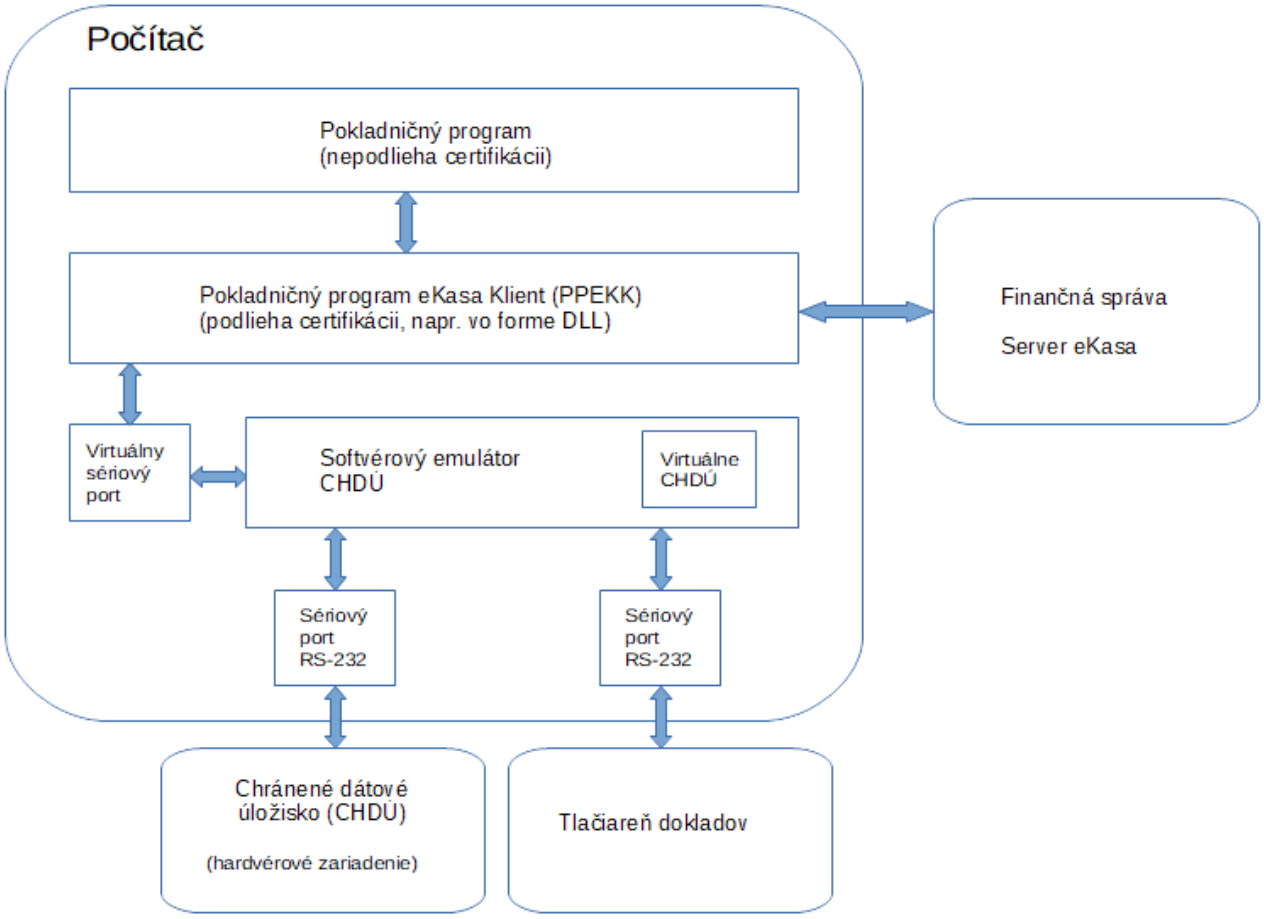


Na počítači je nainštalovaný pokladničný program ľubovolného dodávateľa, ktorý podporuje konkrétne certifikované riešenie eKasa s vydaným certifikátom (PPEKK). K počítaču je pripojené CHDÚ (od CHDÚ s.r.o. pomocou štandardného sériového portu RS-232. Tlačiareň je pripojená k CHDÚ. Doklady na finančnú správu zasiela certifikovaná časť PPEKK.

Emulátor CHDÚ

Emulátor CHDÚ emuluje fyzické CHDÚ firmy CHDÚ, s.r.o. - emuláciou sa rozumie to, že sa pre pokladničnú aplikáciu (PPEKK) „tvári“ ako hardvérové chránené dátové úložisko. Reaguje na príkazy PPEKK, jednotlivé dátové správy ukladá do svojho chráneného úložiska (súbor na disku počítača), pričom prijímané dáta typu tlačovej úlohy preposiela na skutočnú tlačiareň. Pre svoj beh nepotrebuje fyzické CHDÚ – to sa používa len na okopírovanie inicializačných a autentifikačných údajov podnikateľa, t.j. na vytvorenie klonu CHDÚ pre emulátor.

Obrázok č. 2 – pripojenie CHDÚ k počítaču s použitím emulátora



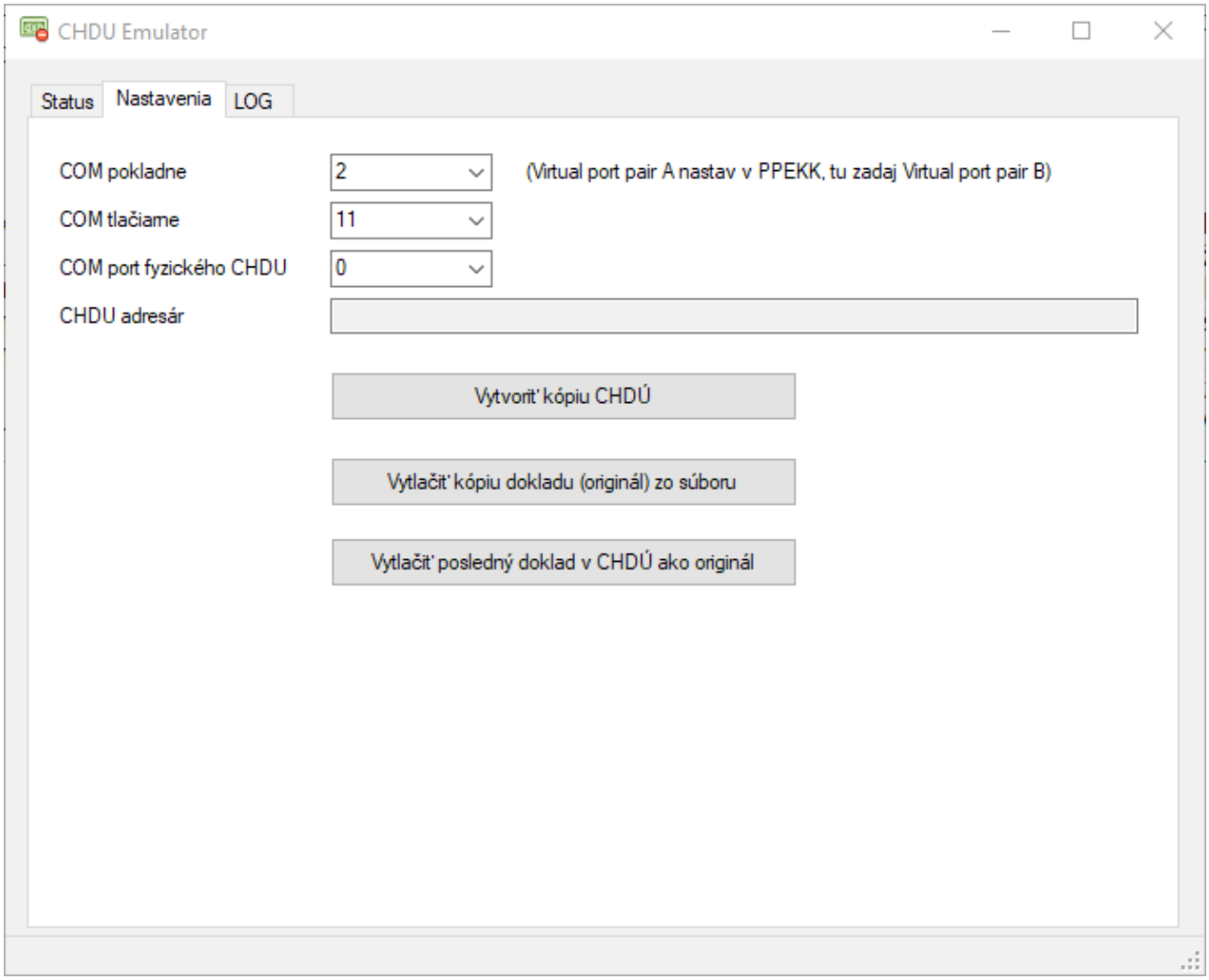
V certifikovanom programe PPEKK sa nenastavuje skutočný fyzický port CHDÚ, ale len virtuálny sériový port. Ten tvorí tzv. null-modem emulator – sofvérová dvojica portov. Tu je možné použiť niektorý z voľne dostupných, napr. com0com, alebo sa dá zakúpiť ľubovolný komerčný, napr. od firmy Eltima). V PPEKK sa nastaví prvý z dvojice, v emulátore CHDÚ druhý port. Tým sa zabezpečí, že pri odoslaní dát z PPEKK sa nebudú preposielať na fyzický CHDÚ, ale len do emulátora. Ten sa tvári ako skutočné fyzické CHDÚ, zapisuje do svojho virtuálneho CHDÚ (súbor na disku počítača) jednotlivé dátové pakety. V prípade operácie čítania vie späť do PPEKK zaslať už uložené dáta. Tlač dokladu neprebieha cez fyzické CHDÚ, ale priamo emulátor zasiela dáta do tlačiarne, ktorá je pripojená k počítaču formou RS-232.

Doklady vystavené v PPEKK s použitím emulátora nesmú byť v žiadnom prípade zaslané na finančnú správu. To by sa dalo zabezpečiť odpojením počítačovej pokladne od internetu. V praxi je však toto riešenie drastické, preto zakázať server finančnej správy je možné urobiť aj elegantnejším spôsobom, napr. sieťovou infraštruktúrou (pravidlom v rootri), prípadne ako v emulátore nastavením výnimky pre odchádzajúce pakety vo Windows firewall-i. Server finančnej správy eKasa je prístupný na adrese ekasa.financnasprava.sk – emulátor si zistí IP adresu a tú zapíše ako pravidlo pre blokovanie IP.

Nastavenie emulátora CHDÚ

Emulátor CHDÚ je možné použiť s ľubovolným pokladničným riešením v kombinácii s ľubovolným dodávateľom PPEKK, ktorí používajú chránené dátové úložisko od firmy CHDU, s.r.o. Samozrejme platí to len v prípade, ak PPEKK beží na počítači. Ak je CHDÚ vložené do zariadenia a komunikácia medzi pokladničným riešením a CHDÚ prebieha iným protokolom, tento emulátor nie je možné použiť.

Obrázok č. 3 – nastavenie emulátora CHDÚ



Po nastavení emulátora je najskôr potrebné vytvoriť virtuáne CHDÚ. V emulátore je to vyriešené vytvorením kópie skutočného fyzického CHDÚ, ktoré môže byť aj úplne nové a prázdne. Dôvodom vytvorenia kópie je obídenie ochrany samotného dodávateľa PPEKK, ktorý si spravidla „svoje“ CHDÚ chráni zapísaním určitých výrobných nastavení do CHDÚ, napr. do prvého dátového bloku si zapíše (zašifruje, zahašuje) výrobné číslo fyzického CHDÚ). Zámerne v emulátore neuvádzame už inicializované CHDÚ niektorých dodávateľov eKasa riešení,

pretože ich necheme poškodiť. Momentálne môže emulátor použiť len ten, kto má už zakúpené PPEKK a fyzické CHDÚ.

Po skopírovaní CHDÚ pre použitie emulátora už fyzické CHDÚ nie je potrebné, môže byť od počítača odpojené. Ak chce však podnikateľ používať hybridný režim (vystavovať on-line legálne doklady) a niektoré nelegálne off-line, musí byť fyzické CHDÚ samozrejme pripojené.

Tlač dokladu s použitím emulátora CHDÚ

Pri vyhotovení dokladu pokladníkom na počítačovej pokladni a funkcii „Uzatvor doklad“ alebo „Vytlač doklad“ a pod. pokladničný systém preposiela doklad do PPEKK. Ten následne zasiela doklad na server finančnej správy (ak je internet a server eKasa dostupný). Keďže emulátor po spustení vždy zakáže server eKasa, PPEKK vyhotoví off-line doklad. Ten následne PPEKK ukladá do CHDÚ v očakávaní, že ho na finančnú správu odošle neskôr – k tomu však nikdy nedôjde. Následne sa doklad vytlačí na tlačiarni a odovzdá sa zákazníkovi.

Dôležité !!! Každý doklad vyhotovený pokladňou je elektronicky podpísaný samotným podnikateľom (jeho autentifikačnými údajmi). Z podpisu je možné dokázať, že daný doklad skutočne vyhotovil konkrétny podnikateľ na konkrétnom certifikovanom pokladničnom riešení. Toto je aj zásadný rozdiel medzi pôvodnými pokladničnými riešeniami a riešeniami eKasa. Emulátor pri tlači dokladu nahrádza pravý podpis falošným (je to zmes náhodných znakov), pričom je upravený aj samotný QR kód. Vyhotovenie off-line dokladu s falošným podpisom znemožňuje finančnej správe dokázať podnikateľovi, že daný doklad vyhotovil skutočne on (samozrejme pokiaľ nie je prichytený priamo pri predaji).

Ďalšie funkcie emulátora CHDÚ

Okrem vyhotovovanie falošných off-line dokladov je možné emulátor použiť aj na opätovnú tlač originálnych dokladov (v tejto verzii je možné tlačiť originál posledného dokladu). Stačí pripojiť CHDÚ akéhokoľvek dodávateľa PPEKK, ktorý používa CHDÚ od firmy CHDÚ, s.r.o. Len s malým úsilím je možné doprogramovať tlač akéhokoľvek dokladu (originálu). Týmto si môžu podnikatelia napr. po skončení mesiaca navzájom zapožičať CHDÚ a vytlačiť si do nákladov toľko dokladov, koľko len potrebujú. Z takýchto dokladov si môžu uplatniť aj odpočet DPH – kontrolný výkaz sa podrobne (dokladovo) nezaoberá drobným predajom, ale len faktúrami.

Záver

Ak nie je komunikácia medzi PPEKK a CHDÚ šifrovaná, je chránené dátové úložisko veľmi ľahko zraniteľné. **Závažnosť vyhotovovania falošných dokladov podčiarkuje fakt, že tieto doklady je možné vytvárať na neupravených pokladničných systémoch a certifikovaných eKasa riešeniach**. Výrobca pokladničného systému ako aj výrobca PPEKK nebudú ani len tušiť, že na ich softvéri sa vyhotovujú falošné pokladničné doklady. Vyhotovovať falošné doklady bolo doposiaľ možné len na upravených pokladničných riešeniach, ktoré bolo možné v prípade zabavenia pokladne dôslednou analýzou aj dokázať. Tu je možné emulátor umiestniť na vytvorený RAM disk operačného systému (RAM drive) – pri prípadnom zabavení počítača a jeho vypnutí sa emulátor CHDÚ z počítača stratí a tak dokazovanie môže byť značne náročné.