

Bezpečné chránené dátové úložisko CHDU5000

V poslednej dobe sa na nás začali obracať servisné organizácie s otázkou bezpečnosti chránených dátových úložisk /CHDÚ/. Už sama podstata pojmu v zákone „chránené dátové úložisko“ navodzuje dojem, že by sa malo jednať o technicky vyspelé zariadenie s bezpečnostnými prvkami. Ak má byť CHDÚ prínosom pre výber daní a má ochrániť majiteľa eKasy pred neoprávneným zásahom tretích strán, tak by mala jeho bezpečnosť zodpovedať ochranným prvkom súčasnej doby.

Pôvodné fiskálne pamäte boli chránené len administratívne preto by ministerstvo financií malo vyžadovať zaviesť vyššiu formu ochrany pri ktorej sú CHDÚ chránené vypodpisovanou chránenou komunikáciou. Ak ochranné prvky CHDÚ nesplnia môžeme konštatovať, že sa jedná len o fiskálnu pamäť bez akékoľvek ochrany.

Bezpečná výmena údajov medzi CHDÚ a programom eKasa

- jednoznačná identifikácia na základe privátneho bezpečného kľúča
- nadviazanie komunikácie na základe kľúčov privátny – verejný
- vypodpisovaná bezpečná komunikácia
- kryptovaná výmena údajov
- jednorázový WORM zápis údajov do CHDÚ
- jednoznačná identifikácia CHDÚ na základe nemenného sériového čísla

Tieto všetky podmienky CHDU5000 vyrábané firmou Varos Trade, s.r.o. spĺňa.

Pokiaľ CHDÚ neobsahuje vymenované ochranné prvky, je to to isté ako vlastniť platobnú kartu, ktorú použije ktokoľvek kto má k nej prístup. Alebo zneužitie bankového účtu len preto, lebo niekto vie jeho číslo. V tomto prípade je jediná ochrana zamknúť kartu do trezoru, ďalej nepoužívať a nikomu neposkytnúť číslo účtu.

Uvedomujeme si, že pri nesplnení podmienok na bezpečnosť, by bol význam CHDÚ takmer bezpredmetný dokonca si myslíme, že nezabezpečené riešenie CHDÚ by bolo nebezpečné pre jeho majiteľa. Do CHDÚ bez ochranných prvkov sa dajú jednoducho dopisovať akékoľvek kompromitujúce údaje, čo by v konečnom dôsledku mohlo ohrozovať podnikateľa a degradovať dôkazový proces preukázania úniku daní na minimum.

V súčasnej modernej dobe bezpečnostných prvkov je jediná ochrana komunikácie CHDÚ / pokiaľ CHDÚ nie je pevne zaliaty s PPEKK / **vypodpisovaná komunikácia a kryptovanie dátového prenosu.**

Iba pri splnení týchto podmienok sa:

- spraví z CHDÚ bezpečné sofistikované zariadenie, ktoré ochráni podnikateľa pred neoprávneným zásahom a zápisom údajov do CHDÚ necertifikovaným SW tretích strán nepovolanou osobou,
- spraví z CHDÚ jednoznačný kontrolný prvok v prípade daňovej kontroly,
- spraví z CHDÚ jednoznačný dôkazový predmet v prípade spáchania trestnej činnosti krátenia daní.

Je na zvážení, či by sa tieto bezpečné ochranné prvky nemali vyžadovať v procese certifikácie.

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

CHDU5000

bezpečné chránené dátové úložisko

Stupne viacnásobnej ochrany CHDU5000

CHDU5000 je zariadenie typu WORM
jednorazový zápis údajov s viacnásobným čítaním

Ochrana I. stupňa

* uloženie CHDU5000 do zariadenie - tlačiarne

Ochrana II. stupňa

* celá komunikácia z nadradenou aplikáciou je zakrytovaná
symetrickou blokovou šifrou AES-256

Ochrana III. stupňa

* výmena údajov z nadradenou aplikáciou
prebieha bezpečným kanálom s bezpečným protokolom

Ochrana IV. stupňa

* každé CHDU5000 obsahuje privátny kľúč ktorý slúži
na bezpečnú komunikáciu

Ochrana V. stupňa

* CHDU5000 má jednoznačné hardvérové
výrobné číslo, ktoré je nemenné

Ochrana VI. stupňa

* každé CHDU5000 má jedinečný identifikátor



Fiskálna pamäť FMEM do 1.7.2019

Stupne viacnásobnej ochrany fiskálnej pamäte

Fiskálna pamäť je zariadenie typu WORM
jednorazový zápis údajov s viacnásobným čítaním

Ochrana I. stupňa

- * uloženie FMEM do zariadenie - tlačiarne

Ochrana II. stupňa

- * prístup k FMEM chránený daňovou plombou

Ochrana III. stupňa

- * manipulácia s FMEM umožnená iba evidovaným servisným organizáciám

Ochrana IV. stupňa

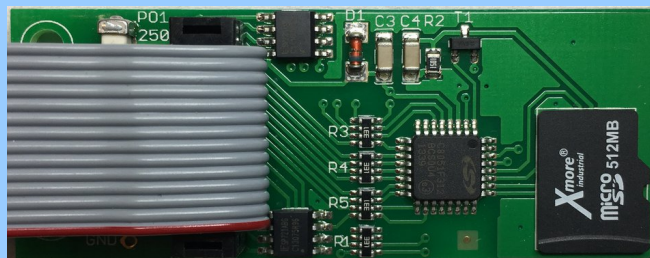
- * výmena FMEM - požadovaný zápis v knihe ERP

Ochrana V. stupňa

- * zápis a čítanie údajov s FMEM vykonáva špeciálna riadiaca doska s nezverejneným komunikačným protokolom

Ochrana VI. stupňa

- * každá FMEM má jedinečný identifikátor



NECHRÁNENÉ dátové úložisko CHDÚ / typu pôvodná fiskálna pamäť /

Stupne bezpečnej ochrany CHDÚ

CHDÚ je zariadenie typu WORM
jednorazový zápis údajov s viacnásobným čítaním

Ochrana I. stupňa

* ~~uloženie CHDÚ do zariadenie – tlačiarne~~

Ochrana II. stupňa

* ~~celá komunikácia z nadradenou aplikáciou je zakryptovaná
symetrickou blokovou šifrou AES-256~~

Ochrana III. stupňa

* ~~výmena údajov z nadradenou aplikáciou
prebieha bezpečným kanálom~~

Ochrana IV. stupňa

* ~~každé CHDÚ obsahuje privátny kľúč ktorý slúži
na bezpečnú komunikáciu~~

Ochrana V. stupňa

* CHDÚ by malo mať jednoznačné hardvérové
výrobné číslo, ktoré je nemenné

Nechránené dátové úložisko je bezvýznamný prvok v procese kontroly a preukázania úniku daní. Bezpečnosť zariadenia nie je ani na úrovni pôvodnej fiskálnej pamäte, ktorá sa chránila aspoň administratívne viacnásobnou ochranou. Ktokoľvek neoprávnený môže vykonať zápis do CHDÚ a preto je tento dôkazový materiál

NEPOUŽITEĽNÝ.