PCS1e

OCHRANA PRACOVNEJ STANICE

S.ICZ, DCÉRSKA SPOLOČNOSŤ ICZ, PREVERENÁ NÁRODNÝM BEZPEČNOSTNÝM ÚRADOM ČR (NBÚ) PRE STYK S UTAJOVANÝMI INFORMÁCIAMI AŽ DO STUPŇA UTAJENIA „PRÍSNE TAJNÉ“, PONÚKA KOMPLEXNÉ SLUŽBY V OBLASTI OCHRANY UTAJOVANÝCH INFORMÁCIÍ.

Kryptografický prostriedok PCS1e predstavuje komplexné riešenie problému ochrany citlivých údajov umiestňovaných na lokálnom alebo vzdialenom dátovom úložisku pracovnej stanice. Technológia tohto riešenia je založená na trvalom ukladaní citlivých údajov výhradne v šifrovanej podobe, a to bez ohľadu na konkrétne technické riešenie použitých dátových úložísk či periférnych zariadení. Na dosiahnutie maximálnej úrovne zabezpečenia prebieha šifrovanie a dešifrovanie týchto údajov v oddelenom kryptografickom hardvéri, ktorý nie je možné z prostredia stanice negatívne ovplyvniť. Prístup k šifrovacím funkciám a chráneným kľúčom je reálne možný až po tom, čo je používateľ týmto nezávislým kryptografickým systémom úspešne autorizovaný. Uvedené mechanizmy tak zaisťujú, že aj prístup k údajom v nešifrovanej podobe je možné získať iba po tom, čo je oprávnený používateľ po prihlásení do stanice ešte následne overený priamo šifrovacím systémom. Riešenie PCS1e tak poskytuje komplexné hardvérové zabezpečenie pracovnej stanice určenej na spracovanie utajovaných informácií až do stupňa „TAJNÉ“ vrátane.

**CERTIFIKÁCIA**

Certifikát NBÚ, evidenčné číslo K20165, je platný do 22. 1. 2019 a potvrdzuje spôsobilosť kryptografického prostriedku na ochranu utajovaných informácií do

a vrátane stupňa utajenia:

` TAJNÉ pre národné utajované informácie

` CONFIDENTIEL UE/EU CONFIDENTIAL

` NATO CONFIDENTIAL

Základom spoľahlivého šifrovania je hardvérové kompaktné zariadenie s vlastným operačným systémom, ktoré je fyzicky inštalované v hostiteľskom počítači, avšak tu pracuje úplne nezávisle od jeho procesoru, pamäte a dátových úložísk. Hlavným rysom uvedeného zariadenia je aktívna a trvalá ochrana šifrovacích kľúčov a všetkých s nimi vykonávaných operácií. Nasadením národného certifikovaného kryptografického prostriedku PCS1e do pracovných staníc vášho zabezpečeného informačného systému zaistíte nielen certifikovanú kryptografickú ochranu utajovaných informácií, ale predovšetkým získate bezpečnostnú technológiu, ktorá vám reálne umožní znížiť požiadavky na fyzickú a administratívnu bezpečnosť prevádzky IS.

# Vyhotovenie

` Základný hardvérový adaptér v podobe rozširujúcej karty pre zbernicu PCI Express počítača kompatibilného s IBM PC zaisťujúci všetky bezpečnostné a kryptografické funkcie úplne oddelene od hostiteľského počítača

` Rozširujúci softvér do hostiteľského počítača s operačným systémom Microsoft Windows zaisťujúci integráciu bezpečnostných a kryptografických funkcií do používateľského prostredia a aplikácií

# Základná funkcionalita

` On-line kryptografická ochrana súborov (s utajovanými informáciami) spracovávaných v hostiteľskom počítači vykonávaná formou transparentného šifrovania ukladaných súborov s riadením kryptografických funkcií na úrovni adresárov, logických diskov, výmenných médií a vzdialených sieťových úložísk

` Off-line kryptografická ochrana súborov (s utajovanými informáciami) spracovávaných v hostiteľskom počítači, realizovaná formou bezpečných šifrovaných súborových archívov určených primárne na ukladanie a prenos údajov, prekračujúca perimeter zabezpečeného IS (napr. e-mailom cez verejné siete, ako je internet)

# Používateľská prívetivosť

` PCS1e je určený pre štandardné počítače kompatibilné s IBM PC s operačným systémom Microsoft Windows

` PCS1e je používateľsky priateľské riešenie, kde šifrovanie prebieha úplne transparentne a automaticky. Od používateľa sa nevyžadujú žiadne špeciálne úkony okrem vloženia čipovej karty a zadania PIN-u

` Inštaláciou PCS1e je možné reálne znížiť nároky na fyzickú bezpečnosť a bezpečnosť komunikačných systémov

**[ PCS1e ]**

# Zabezpečenie komplexnej ochrany

` Riadenie prístupu používateľov do operačného systému hostiteľského počítača na základe bezpečnostného predmetu (čipovej karty)

` Prístup k údajom v šifrovaných súboroch ukladaných na lokálnych, sieťových a výmenných dátových úložiskách hostiteľského počítača na základe bezpečnostného predmetu (čipovej karty)

` Systémové zabezpečenie realizované šifrovaním používateľského profilu, častí systémových dátových oblastí, dočasných a zvyškových informácií na disku a konfigurácie systému

` Nezávislý audit bezpečnostne významných udalostí vytváraný na internom pamäťovom module hardvérového adaptéra PCS1e so zaistením trvalej ochrany proti jeho neoprávnenej modifikácii

# Kľúčové vlastnosti hardvérového šifrovacieho riešenia PCS1e

` Transparentné šifrovanie súborov obsahujúcich utajované informácie pri ich ukladaní do úložísk

` Nezávislá vrstva funkcií na riadenie prístupu k šifrovaným aj nešifrovaným súborom dopĺňajúca mechanizmy štandardného riadenia prístupu k údajom v operačnom systéme

` Integračné rozhranie (zákaznícke aplikácie so silnými bezpečnostnými funkciami, integrácia kryptografickej ochrany do štandardných aplikácií)

` Silná ochrana kryptografických kľúčov – kľúče nikdy neopúšťajú PCS1e a nie sú tak dostupné pre hostiteľský počítač

` Bezpečná realizácia kryptografických algoritmov – algoritmy nie sú prístupné pre procesy bežiace na počítači (dostupnosť iba prostredníctvom aplikačného API)

` Bezpečné uloženie a trvalá ochrana kľúčov – kľúče sú v prostriedku aktívne chránené aj vo vypnutom stave

# Kľúčové možnosti riešenia PCS1e

` Realizácia trvalej ochrany súborov v certifikovanom IS (utajované informácie sa vôbec nemusia vyskytovať na žiadnom lokálnom, sieťovom a výmennom dátovom úložisku v otvorenom tvare)

` Vybudovanie komplexnej zabezpečenej pracovnej stanice (silná identifikácia a autentizácia používateľa, trvalá ochrana súborov obsahujúcich utajované informácie, ochrana systémových údajov a konfigurácie)

` Nezávislé riadenie prístupu a ochrana súborov obsahujúcich utajované informácie – silná záruka (oddelenie informačných kategórií, viac nezávislých úrovní zabezpečenia, povolenie/zakázanie exportu utajovaných informácií v otvorenom tvare na výmenné médiá, obmedzenie prístupu správcu k uloženým údajom)

` Široká správa šifrovacích kľúčov, flexibilné kľúčové hospodárstvo (viac možností pre architekta IS), možnosť automatizácie úkonov správy

# Referencie

Implementáciou kryptografického prostriedku PCS1e doplnenou o ďalšie bezpečnostné produkty od spoločnosti S.ICZ je možné vybudovať reálne certifikované informačné systémy určené na spracovanie citlivých a utajovaných informácií s vysokým používateľským komfortom a vysokou pridanou bezpečnostnou hodnotou. Príkladom takého informačného systému je IS MZV-KR, ktorý obsahuje uzly rôznych stupňov utajenia a umožňuje spracovávať a vymieňať utajované informácie medzi ústredím Ministerstva zahraničných vecí ČR a zastupiteľskými úradmi ČR.

**OBCHODNÝ KONTAKT**

**S.ICZ a. s.** Na hřebenech II 1718/10 140 00 Praha 4

**TEL.:** +420 222 271 111

**FAX:** +420 222 271 112

**E-MAIL:** obchod-SICZ@iczgroup.com

* Základné parametre PCS1e

**Požiadavky na počítač:**

` rozhranie PCI Express (voľný slot PCI Express pre štandardnú kartu s dĺžkou 168 mm)

**Technické parametre:**

` rozmery (D × V × Š): 168 × 111 × 14,7 (mm)

` fyzické rozhranie: PCI Express 1.1 ×1

` čítačka ČK: ISO 7816 &EMV 2000 level 1 pripojená na interný USB konektor PCS1e

` prevádzková teplota: 0 – 45 st. C (vnútorná teplota PC)

` relatívna vlhkosť: 5 – 95 % (nekondenzujúca)

**Podporované OS:**

` MS Windows 7, MS Windows Server 2008 R2 (on-line

a off-line šifrovanie súborov s podporou 32- aj 64-bitového OS)

` MS Windows XP (iba pre off-line šifrovanie súborov)

**Overenie používateľa:**

` Fyzická čipová karta priamo obsluhovaná hardvérovým adaptérom PCS1e

` Metódy následnej I/A do OS: tajné heslo, certifikát (Smart Card Logon)

**Aplikačné rozhrania:**

` PKCS#11

` MS Crypto API

**Implementácia šifrovania do OS:**

` Transparentné on-line šifrovanie: súbory, adresáre, logické disky, výmenné médiá, vzdialené sieťové úložiská

` Off-line šifrovanie súborov

` Asymetria (podpisovanie, šifrovanie)

**Algoritmy:**

` Šifrovacie algoritmy: národný algoritmus (rýchlosť 3,2 MB/s), AES 256 (rýchlosť 12 MB/s), RSA 2048

` Hashovací algoritmus SHA 256

**Bezpečné úložisko kľúčov:**

` Deaktivácia/deštrukcia s možnosťou napojenia na vonkajší

Kontakt

` viacúrovňový kľúčový systém

` Max. počet úložísk: 30

` Max. počet kľúčov v úložisku: 400

` Max. počet kľúčov: 12000 (30 × 400)

**Ostatné bezpečnostné funkcie:**

` fyzikálny generátor náhody

` nezávislý čas

` nezávislý audit

` dohľadový procesor

**Systémová bezpečnosť:**

` Možnosť šifrovania profilu používateľa

` Možnosť šifrovania systémových údajov (spooler, temp, …)

` Možnosť riadenia exportu údajov v otvorenej podobe

**Trieda kryptografického prostriedku:**

` CCI

**Fyzická bezpečnosť:**

` Parameter S1=7

**Miery záruk podľa Common Criteria:**

` vývoj a návrh riešenia bol vykonaný v súlade s požiadavkami na záruky EAL4+