# PCS1e

## OCHRANA PRACOVNÍ STANICE

S.ICZ, DCEŘINÁ SPOLEČNOST ICZ, PROVĚŘENÁ NÁRODNÍM BEZPEČNOSTNÍM ÚŘADEM ČR (NBÚ) PRO STYK S UTAJOVANÝMI INFORMACEMI AŽ DO STUPNĚ UTAJENÍ „PŘÍSNĚ TAJNÉ“, NABÍZÍ KOMPLEXNÍ SLUŽBY V OBLASTI OCHRANY UTAJOVANÝCH INFORMACÍ.

Kryptografický prostředek PCS1e představuje komplexní řešení problému ochrany citlivých dat umisťovaných na lokálním nebo vzdáleném datovém úložišti pracovní stanice. Technologie tohoto řešení je založena na trvalém ukládání citlivých dat výhradně v šifrované podobě a to bez ohledu na konkrétní technické řešení použitých datových úložišť či periferních zařízení. Pro dosažení maximální úrovně zabezpečení je šifrování a dešifrování těchto dat prováděno v odděleném kryptografickém hardware, který nelze z prostředí stanice negativně ovlivnit. Přístup k šifrovacím funkcím a chráněným klíčům je reálně možný teprve poté, co je uživatel tímto nezávislým kryptografickým systémem úspěšně autorizován. Uvedené mechanismy tak zajišťují, že i přístup k datům v nešifrované podobě je možné získat pouze poté, co je oprávněný uživatel po přihlášení ke stanici ještě následně ověřen přímo šifrovacím systémem. Řešení PCS1e tak poskytuje komplexní hardwarové zabezpečení pracovní stanice určené pro zpracování utajovaných informací až do stupně „TAJNÉ“ včetně.

Základem spolehlivého šifrování je hardwarové kompaktní zařízení s vlastním operačním systémem, které je fyzicky instalováno v hostitelském počítači, avšak zde pracuje zcela nezávisle na jeho procesoru, paměti a datových úložištích. Hlavním rysem uvedeného zařízení je aktivní a trvalá ochrana šifrovacích klíčů a veškerých s jimi prováděných operací. Nasazením národního certifikovaného kryptografického prostředku PCS1e do pracovních stanic vašeho zabezpečeného informačního systému zajistíte nejenom certifikovanou kryptografickou ochranu utajovaných informací, ale především získáte bezpečnostní technologii, která vám reálně umožní snížit požadavky na fyzickou a administrativní bezpečnost provozu IS.

### CERTIFIKACE

Certifikát NBÚ, evidenční číslo K20165, je platný do 22. 1. 2019 a potvrzuje způsobilost kryptografického prostředku pro ochranu utajovaných informací, včetně stupně utajení:

- TAJNÉ pro národní utajované informace
- CONFIDENTIEL UE/EU CONFIDENTIAL
- NATO CONFIDENTIAL


### Provedení

- Základní hardwarový adaptér v podobě rozšiřující karty pro sběrnici PCI Express počítače kompatibilního s IBM PC zajišťující veškeré bezpečnostní a kryptografické funkce zcela odděleně od hostitelského počítače
- Rozšiřující software do hostitelského počítače s operačním systémem Microsoft Windows zajišťující integraci bezpečnostních a kryptografických funkcí do uživatelského prostředí a aplikací

### Základní funkcionalita

- On-line kryptografická ochrana souborů (s utajovanými informacemi) zpracovávaných v hostitelském počítači prováděná formou transparentního šifrování ukládaných souborů s řízením kryptografických funkcí na úrovni adresářů, logických disků, výměnných médií a vzdálených síťových úložišť
- Off-line kryptografická ochrana souborů (s utajovanými informacemi) zpracovávaných v hostitelském počítači, realizovaná formou bezpečných šifrovaných souborových archivů určených primárně pro ukládání a přenos dat, překračující perimetr zabezpečeného IS (např. e-mailem přes veřejné sítě jako je Internet)

### Uživatelská přívětivost

- PCS1e je určen pro standardní počítače kompatibilní s IBM PC s operačním systémem Microsoft Windows
- PCS1e je uživatelsky přátelské řešení, kde šifrování probíhá zcela transparentně a automaticky. Od uživatele se nevyžadují žádné speciální úkony, kromě vložení čipové karty a zadání PINu
- Instalací PCS1e lze reálně snížit nároky na fyzickou bezpečnost a bezpečnost komunikačních systémů

## Zabezpečení komplexní ochrany

- Řízení přístupu uživatelů k operačnímu systému hostitelského počítače na základě bezpečnostního předmětu (čipové karty)
- Přístup k datům v šifrovaných souborech ukládaných na lokálních, síťových a výměnných datových úložištích hostitelského počítače na základě bezpečnostního předmětu (čipové karty)
- Systémové zabezpečení realizované šifrováním uživatelského profilu, částí systémových datových oblastí, dočasných a zbytkových informací na disku a konfigurace systému
- Nezávislý audit bezpečnostně významných událostí vytvářený na interním paměťovém modulu hardwarového adaptéru PCS1e se zajištěním trvalé ochrany proti jeho neoprávněné modifikaci

## Klíčové vlastnosti hardwarového šifrovacího řešení PCS1e

- Transparentní šifrování souborů obsahujících utajované informace při jejich ukládání do úložišť
- Nezávislá vrstva funkcí pro řízení přístupu k šifrovaným i nešifrovaným souborům doplňující mechanismy standardního řízení přístupu k datům v operačním systému
- Integrační rozhraní (zákaznické aplikace se silnými bezpečnostními funkcemi, integrace kryptografické ochrany do standardních aplikací)
- Silná ochrana kryptografických klíčů - klíče nikdy neopouští PCS1e a nejsou tak dostupné pro hostitelský počítač
- Bezpečná realizace kryptografických algoritmů - algoritmy nejsou přístupné pro procesy běžící na počítači (dostupnost pouze prostřednictvím aplikačního API)
- Bezpečné uložení a trvalá ochrana klíčů – klíče jsou v prostředku aktivně chráněny i ve vypnutém stavu

## Klíčové možnosti řešení PCS1e

- Realizace trvalé ochrany souborů v certifikovaném IS (utajované informace se vůbec nemusí vyskytovat na žádném lokálním, síťovém a výměnném datovém úložišti v otevřeném tvaru)
- Vybudování komplexní zabezpečené pracovní stanice (silná identifikace a autentizace uživatele, trvalá ochrana souborů obsahujících utajované informace, ochrana systémových dat a konfigurace)
- Nezávislé řízení přístupu a ochrana souborů obsahujících utajované informace – silná záruka (oddělení informačních kategorií, více nezávislých úrovní zabezpečení, povolení/zakázání exportu utajovaných informací v otevřeném tvaru na výměnná média, omezení přístupu správce k uloženým datům)
- Široká správa šifrovacích klíčů, flexibilní klíčové hospodářství (více možností pro architekta IS), možnost automatizace úkonů správy

## Reference

Implementací kryptografického prostředku PCS1e doplněnou o další bezpečnostními produkty S.ICZ je možné vybudovat reálné certifikované informační systémy určené pro zpracování citlivých a utajovaných informací s vysokým uživatelským komfortem a vysokou přidanou bezpečnostní hodnotou. Příkladem takového informačního systému je IS MZV-KR, který obsahuje uzly různých stupňů utajení a umožňuje zpracování a výměnu utajovaných informací mezi ústředím Ministerstva zahraničních věcí ČR a zastupitelskými úřady ČR.

■ Základní parametry PCS1e

**Požadavky na počítač:**
- PCI Express rozhraní (volný PCI Express slot pro standardní kartu s délkou 168mm)

**Technické parametry:**
- rozměry (D x V x Š): 168 x 111 x 14,7 (mm)
- fyzické rozhraní: PCI Express 1.1 x1
- čtečka ČK: ISO 7816 &EMV 2000 level 1 připojena na interní USB konektor PCS1e
- provozní teplota: 0-45 st. C (vnitřní teplota PC)
- relativní vlhkost: 5-95% (nekondenzující)

**Podporované OS:**
- MS Windows 7, MS Windows server 2008 R2 (on-line a off-line šifrování souborů s podporou 32 i 64 bitové OS)
- MS Windows XP (pouze pro off-line šifrování souborů)

**Ověření uživatele:**
- fyzická čipová karta přímo obsluhovaná hardwarovým adaptérem PCS1e
- metody následné I/A do OS: tajné heslo, certifikát (Smart Card Logon)

**Aplikační rozhraní:**
- PKCS#11
- MS Crypto API

**Implementace šifrování do OS:**
- transparentní on-line šifrování: soubory, adresáře, logické disky, výměnná média, vzdálená síťová úložiště
- off-line šifrování souborů
- asymetrie (podepisování, šifrování)

**Algoritmy:**
- šifrovací algoritmy: národní algoritmus (rychlost 3,2 MB/s), AES 256 (rychlost 12 MB/s), RSA 2048
- hashovací algoritmus SHA 256

**Bezpečné úložiště klíčů:**
- deaktivace / destrukce s možností napojení na vnější kontakt
- víceúrovňový klíčový systém
- max. počet úložišť: 30
- max. počet klíčů v úložišti: 400
- max. počet klíčů: 12000 (30 x400)

**Ostatní bezpečnostní funkce:**
- fyzikální generátor náhody
- nezávislý čas
- nezávislý audit
- dohledový procesor

**Systémová bezpečnost:**
- možnost šifrování profilu uživatele
- možnost šifrování systémových dat (spooler, temp, ...)
- možnost řízení exportu dat v otevřené podobě

**Třída kryptografického prostředku:**
- CCI

**Fyzická bezpečnost:**
- parametr S1=7

**Míry záruk podle Common Criteria:**
- vývoj a návrh řešení byl proveden v souladu s požadavky na záruky EAL4+

**OBCHODNÍ 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:** sec-sales@i.cz