LANPCSe-AES

OCHRANA LAN KOMUNIKÁCIE

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.

LANPCSe-AES realizuje vrstvu zaručenej ochrany sieťovej komunikácie pre pracovnú stanicu, na ktorej sa spracovávajú citlivé alebo utajované informácie. Základným rysom certifikovaného kryptografického prostriedku LANPCSe-AES je integrácia IPSec šifrátora do podoby internej šifrovacej sieťovej karty, ktorá sa umiestňuje do vnútrajšku pracovnej stanice. Nasadenie tohto kryptografického prostriedku tak umožní využiť súčasnú nezabezpečenú komunikačnú infraštruktúru (kabeláž, aktívne prvky) na pripojenie pracovných staníc, nachádzajúcich sa v bežných kanceláriách, do certifikovaného informačného systému určeného na spracovanie utajovaných informácií podľa zákona č. 412/2005 Zb.

**CERTIFIKÁCIA**

Certifikát NBÚ, evidenčné číslo K20158, je platný do 22. 01. 2019 a potvrdzuje spôsobilosť kryptografického prostriedku pre ochranu utajovaných informácií do a vrátane stupňa utajenia:

` VYHRADENÉ

` RESTRIENT UE/EU RESTRICTED

` NATO RESTRICTED

Pri návrhu a výstavbe informačných systémov s využitím LANPCSe-AES dochádza k zásadnému zníženiu nákladov na fyzické zabezpečenie prevádzkových priestorov IS a súčasne sa strácajú aj existujúce obmedzenia, ktoré bránia efektívnemu využívaniu a rozširovaniu systémov spracovávajúcich utajované informácie pre bežné pracoviská používateľov. Implementácia LANPCSe-AES vyčlení komunikačnú infraštruktúru za hranice certifikovaného informačného systému. Tým dôjde k eliminácii nákladov potrebných na zvýšenie ochrany všetkých komunikačných trás a na zabezpečenie priestorov dátových rozvádzačov. Súčasne aj odpadajú náklady na vybudovanie oddelenej duplicitnej a súbežne prevádzkovanej dátovej siete a zmiznú aj akékoľvek obmedzenia na geografické rozmiestnenie pracovných staníc používateľov. Svoj informačný systém tak môžete prevádzkovať tam, kde reálne potrebujete, a s minimálnymi nákladmi ho môžete prispôsobovať všetkým prevádzkovým a organizačným zmenám.


# Vyhotovenie

` Je to samostatný hardvérový kryptografický prostriedok (IPSec šifrátor) v podobe rozširujúcej sieťovej karty pre zbernicu PCI Express

` Na sprístupnenie hardvéru slúžia ovládače sieťového rozhrania a pre operačný systém neprináša žiadne obmedzenie

# Základná funkcionalita

` Kryptografický prostriedok sa stáva neoddeliteľnou súčasťou pracovnej stanice, ale kryptografické funkcie sú kompletne oddelené od operačného systému počítača

` Principiálna bezpečnosť – pracovnú stanicu môžu po sieti opustiť iba zašifrované údaje, operačný systém nemôže ovplyvniť funkciu prostriedku

` Eliminuje potrebu oddelenej duplicitnej a súbežne prevádzkovanej dátovej siete

` Nie je vyžadovaná prevádzková obsluha kryptografického prostriedku

` Umožňuje jedno pečatenie (jednu ochranu) – ochrana vnútrajška pracovnej stanice sa vzťahuje aj na ochranu zabudovaného IPSec šifrátora

# Efektivita implementácie

` LANPCSe-AES je určený pre štandardné počítače kompatibilné s IBM PC s OS MS Windows alebo Linux

` Inštalácia do OS počítača je realizovaná pomocou softvérových ovládačov, ktoré samy osebe nevyžadujú klasifikáciu HDD ako nosiča utajovaných informácií

` LANPCSe-AES sa v počítači javí ako štandardná sieťová karta a z pohľadu svojej obsluhy nekladie na používateľa žiadne ďalšie požiadavky (nie je vyžadovaná prevádzková obsluha kryptografického prostriedku)

` Výber priestoru pre umiestnenie počítača s LANPCSe-AES neovplyvňuje rozmiestnenie ďalších komponentov informačného systému

**[ LANPCSe-AES ]**

# Typické príklady nasadenia

` Ochrana komunikácie v prostredí LAN aj WAN (využitie štandardnej existujúcej nezabezpečenej aj verejnej komunikačnej infraštruktúry)

` Prepojenie súčasných geograficky a sieťovo izolovaných PC (samostatné stanice určené na spracovanie utajovaných informácií). Získanie možnosti on-line správy PC a on-line výmeny UI, obmedzenie nutnosti exportu UI na nosiče utajovaných informácií

` Presun súčasných pracovných staníc určených na spracovanie UI z oddelených zabezpečených priestorov priamo na pracovisko používateľa (predĺženie existujúceho certifikovaného IS na spracovanie UI)

` Tvorba nových IS určených na spracovanie UI s plným využitím štandardných produktov (napr. na tvorbu komunikačnej infraštruktúry, zaistenie sieťových služieb, zaistenie služieb AD domény vrátane správy)

` Bezpečná terminálová prevádzka určená na spracovanie UI (PC v podobe terminálu bez možnosti ukladať UI na lokálny disk)

# Kľúčové výhody HW šifrovaného spojenia s LANPCSe-AES

` Jednotná metóda – štandardizácia prenosu údajov on-line šifrovaním medzi počítačmi, ktoré je pre ostatné komponenty informačného systému úplne transparentné

` HW šifrovanie všetkých prenášaných údajov poskytuje tak fyzickú, ako logickú bariéru nezávislej ochrany, ktorá je postavená medzi pracovnú stanicu a komunikačnú sieť

` Umožňuje využitie súčasnej komunikačnej infraštruktúry (kabeláž, aktívne prvky) bez nutnosti robiť zmeny či obmedzovať jej funkcie

` Nevyžaduje žiadne špeciálne školenie pre koncového používateľa – používateľ nie je v role prevádzkovej obsluhy kryptografického prostriedku

` Prostriedok je pre chod operačného systému a aplikáciu pracovnej stanice úplne transparentný (nevyžaduje inštaláciu žiadneho aplikačného softvéru okrem ovládačov sieťovej karty)

` Kryptografické kľúče nikdy neopúšťajú LANPCSe-AES (nie sú dostupné pre pracovnú stanicu)

` Kryptografické algoritmy sú plne realizované vnútri LANPCSe-AES a nie sú ovplyvniteľné z pracovnej stanice

` Poskytuje funkcie bezpečného uloženia, správy a deštrukcie šifrovacích kľúčov, ktoré sú nezávislé od chodu operačného systému pracovnej stanice

` Umožňuje viacúrovňovú správu kryptografického prostriedku a vzdialený dohľad

` Umožňuje aj prevádzku v režime jednoduchej lokálnej správy (nevyžaduje centrum na riadenie a správu)

` Poskytuje nezávislý audit bezpečnostne významných udalostí vytváraný na pamäťovom module v kryptografickom prostriedku LANPCSe-AES zaisťujúcom trvalú ochranu proti neoprávnenej manipulácii

# Výkonný prostriedok pre centrá

Na budovanie rozsiahlych systémov, kde jednotlivé pracovné stanice vybavené kryptografickým prostriedkom LANPCSe-AES pristupujú do jedného alebo viacerých centier, sú na zaistenie dostatočného výkonu/priechodnosti týchto centier určené výkonné hraničné kryptografické prostriedky LANPCS-Rack. Tieto prostriedky sú plne kompatibilné s ostatnými kryptografickými prostriedkami rodiny LANPCS (LANPCSe-AES, LANPCS-AES). Podrobné informácie o výkonnom hraničnom kryptografickom prostriedku LANPCS-Rack sú uvedené v samostatnom produktovom liste.

**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

# Referencie

Implementáciou kryptografických prostriedkov LANPCSe-AES s ďalšími bezpečnostnými produktmi spoločnosti S.ICZ (napr. PCS1, AirGap 02) je možné vybudovať reálne certifikované informačné systémy určené na spracovanie citlivých a utajovaných informácií s vysokým používateľským komfortom a vysokou pridanou bezpečnostnou hodnotou. Používatelia tak môžu z prostredia svojej kancelárie využívať aplikácie na on-line spracovanie utajovaných informácií v rámci svojej organizácie a súčasne je možné z týchto systémov zaistiť aj trvalú výmenu informácií aj medzi organizáciami. Príkladom takého informačného systému je aktualizácia IS EU Extranet ČR, ktorý je určený na národnú distribúciu oficiálnych utajovaných dokumentov Rady EÚ.

* Základné parametre LANPCSe-AES

**Požiadavky na počítač:**

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

**Technické parametre:**

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

` fyzické PCI rozhranie: PCI Express 1.1 ×1

` fyzická sieťová vrstva: Ethernet 10/100 Mbps (konektor RJ 45)

` základná sieťová vrstva: IPv4

` bezpečnostné rozšírenie IP: IPsec (RFC 2406 – ESP)

` čítačka ČK: ISO 7816 &EMV 2000 level 1 pripojená na interný alebo externý USB konektor LANPCSe-AES

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

` relatívna vlhkosť: 5 – 95 % (nekondenzujúca)

**Podporované OS:**

` MS Windows

` Linux jadro 2.6 a novšie (preferencia linuxovej distribúcie Debian)

` podpora 32- aj 64-bitového OS

**Dátová priepustnosť:**

` 40 Mbps (fyzické maximum)

` 34 Mbps (reálna prevádzka)

**Prevádzkové režimy:**

` manuálny režim (prevádzková konfigurácia uložená na čipovej karte)

` autonómny režim (nemá prevádzkovú obsluhu kryptografického prostriedku, prevádzková konfigurácia uložená v LANPCSe-AES)

**Vzdialený dohľad:**

` ICMP

` SNMP

` prenos logov na FTP

**Kryptografia:**

` algoritmy: AES 256, HMAC SHA-256, Diffie-Hellman

**Interné bezpečnostné funkcie:**

` fyzikálny generátor náhody

` nezávislý čas

` nezávislý audit

` dohľadový procesor

**Trieda kryptografického prostriedku:**

` CCI

**Miery záruk podľa Common Criteria:**

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