s.icz, dceřiná společnost icz, prověřená Národním bezpečnostním úřadem ČR pro styk s utajovanými informacemi až do stupně utajení „přísně tajné“, nabízí komplexní služby v oblasti ochrany utajovaných informací.

# LANPCS RG3


## Kryptografický prostředek pro ochranu utajovaných informací při síťové komunikaci

- Výkonný hardware poskytující nejvyšší úroveň bezpečnosti
- Certifikace pro CZ, EU, NATO
- Úplné oddělení kryptografických funkcí od počítače a jeho OS
- Centrální správa a vzdálený dohled
- Neobyčejné schopnosti ukryté v „běžné“ síťové kartě
- Nevyžaduje duplicitní lokální síťové rozvody
- Postačují běžné síťové prvky a pracovní stanice
- Umožňuje standardní správu a dohled celého informačního systému

LANPCS-RG3 je plnohodnotný výkonný certifikovaný šifrátor – dalo by se říci, že je dokonce určitým klonem pevnosti Fort Knox ve světě informačních technologií. Tento výjimečný produkt v sobě spojuje vlastnosti neúnavného ochránce a nepřemožitelné ozbrojené eskorty vašich odesílaných a přijímaných dat. Instalací LANPCS-RG3 do pracovní stanice získáte nejen unikátní bariéru před útoky z vnějšího světa počítačových sítí, ale i ochranu proti zlomyslnému malwaru a dalším hrozbám, o které v dnešním propojeném digitálním světě rozhodně není nouze.

Pořízením LANPCS-RG3 získáte šifrátor v podobě standardní síťové karty, která je použitelná ve většině pracovních stanic, a je připojitelná do běžné síťové infrastruktury. Produkt je vybudován na vlastní specializované hardwarové platformě, která je společností S.ICZ a. s. dlouhodobě vyvíjena pro bezpečnostně exponované aplikace. Jeho architektura je doslova „paranoidní”, uzavírá bezpečnostní služby šifrátoru uvnitř důvěryhodného hardwaru, a tím je zaručeně izoluje od vlivů okolního prostředí. Chrání tak přenosy dat proti vnějším útokům z nebezpečné džungle počítačových sítí a zcela eliminuje i možnost, že by vnější útočník mohl spoléhat na spolupráci s kompromitovaným hardwarem. Bezpečnostní funkce LANPCS-RG3 byly důsledně ověřeny NÚKIB při procesu certifikace podle zákona č. 412/2005 Sb. jako dostatečné pro ochranu utajovaných informací v rámci ČR, EU i NATO.

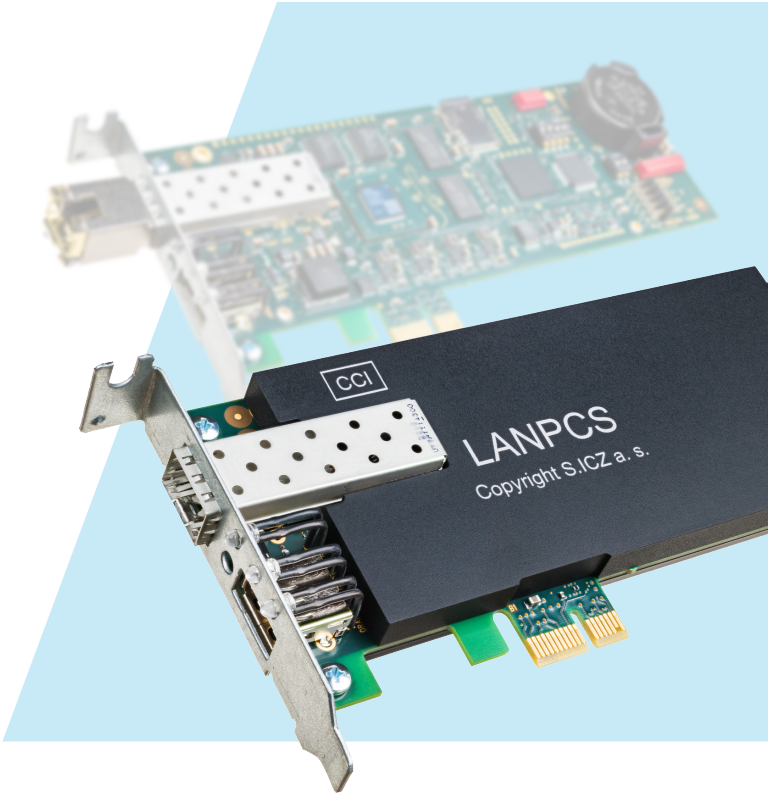
Zamkněte dveře a přiveďte síť – vše ostatní zajistím! Takto jednoduše by se dal popsat proces budování nebo rozšíření zabezpečeného informačního systému s použitím LANPCS-RG3. Provozovateli stačí zajistit fyzickou bezpečnost pouze v prostoru stanice, bez omezení pro okolní kanceláře. Z tohoto prostoru pak prostřednictvím stávajících sítí stanice bezpečně komunikuje s centrem. Nejsou potřeba žádné investice do komunikační infrastruktury a jen minimální do fyzického zabezpečení vybraných prostor. LANPCS-RG3 je moderní variantou zabezpečení umožňující dynamické budování rozsáhlých certifikovaných informačních systémů.

S.ICZ a. s. Na Hřebenech II 1718/10, 140 00 Praha 4 marketing@i.cz www.iczgroup.com +420 222 271 111

Dnešní svět je doba úžasných moderních technologií, kde každý nový tablet, počítač, server nebo aktivní síťový prvek je uváděn jako nejvýkonnější, nejspolehlivější a podporující nejnovější bezpečnostní standardy. Proč se ale každodenně setkáváme s bezpečnostními riziky při používání těchto moderních technologií? Proč selhávají implementované bezpečnostní standardy? Proč běžná ochrana komunikace pomocí šifrování na úrovni operačních systémů nebo specializovaných aplikací je tak často úspěšně prolomena při útocích hackerů?

Moderní technologie jsou vysoce komplexní, a proto značně složité. Dnešním trendem je integrace mnoha periferií do jednoho produktu s minimálními rozměry a maximálním výkonem. To vede k vysoké integraci a složitosti hardwaru a rozsáhlému a komplikovanému firmwaru (proprietární programový kód), který je stěžejní pro jeho správnou funkci. Výrobci jsou dnešním trhem tlačeni k velmi častým inovacím a nízkým cenám. To vede k produktům sice moderním a výkonným, ale často bezpečnostně zranitelným. Na prvním místě je rozsah funkcí, design, výkon, ale určitě ne bezpečnost. I renomovaný výrobce produktu se často spoléhá na čipy a firmware, které nikdo důkladně neposoudil z pohledu zranitelností a obvykle to není ani reálně možné. K aktuálně diskutované problematice důvěryhodnosti výrobců lze pouze konstatovat, že koncový uživatel je v případě nepoctivých úmyslů výrobce či jeho subdodavatelů zcela bezbranný.

**Svět a současné trendy nejsme schopni změnit! Co však změnit můžeme, je náš celkový přístup ke způsobu práce s citlivými a utajovanými informacemi. Základem je přijmout fakt, že ani sebelepší software na běžně dodávaných počítačích nemůže zajistit dostatečnou ochranu těchto informací při práci s nimi, jejich ukládání a přenosu.**




## Kryptografický prostředek
## LANPCS-RG3

Certifikovaný kryptografický prostředek LANPCS-RG3 (dále jen KP LANPCS-RG3) realizuje vrstvu zaručené a hodnocené ochrany síťové komunikace pro počítače, na kterých jsou zpracovávány citlivé nebo utajované informace. Jeho základním rysem je integrace plnohodnotného IPSec šifrátoru do podoby interní šifrovací síťové karty umístěné do skříně počítače. Nasazení tohoto kryptografického prostředku tak umožní využít stávající nezabezpečenou komunikační infrastrukturu (strukturovanou kabeláž, aktivní prvky) pro připojení počítačů nacházejících se v běžných kancelářích i do certifikovaného informačního systému (dále IS) určeného pro zpracování utajovaných informací podle zákona č. 412/2005 Sb.

Při návrhu a výstavbě IS s využitím KP LANPCS-RG3 dochází k zásadnímu snížení nákladů na fyzické zabezpečení provozních prostor IS a současně mizí mnohá omezení, která brání efektivnímu využívání a rozšiřování systémů zpracovávajících citlivé nebo utajované informace. Implementace KP LANPCS-RG3 vyčlení komunikační infrastrukturu za hranice certifikovaného IS. To vede k eliminaci nákladů, jinak potřebných, na zvýšení ochrany komunikačních tras a na zabezpečení prostor datových rozvaděčů. Navíc odpadají náklady na vybudování oddělené duplicitní a souběžně provozované datové sítě a zmizí i jakákoli omezení na geografické rozmístění počítačů. IS tak může být provozován tam, kde je reálná potřeba a s minimálními náklady je možné reagovat na provozní a organizační změny.

## Provedení

KP LANPCS-RG3 je postaven na speciálně vyvinutém hardwaru určeném pro bezpečnostně exponované aplikace (řešení s nejvyšší bezpečnostní úrovní). Fyzicky se jedná o rozšiřující kartu určenou pro počítače se sběrnicí PCIe, která zcela samostatně a odděleně realizuje funkci plnohodnotného šifrátoru. Karta navíc obsahuje specifické prvky, zajišťující nadstandardně vysokou a trvalou ochranu vnitřních operací a jejího obsahu před manipulací a vyčtením z vnějšího okolí. Díky tomu, že na kartě je umístěno i koncové fyzické síťové rozhraní, jeví se celý KP LANPCS-RG3 uživateli jako běžná síťová karta, která však současně poskytuje nejvyšší možnou úroveň nezávislosti a zabezpečení veškeré vnější komunikace počítače. Začlenění rozšiřující karty do počítače umožňují ovladače síťového rozhraní, které neplní žádné bezpečnostní funkce a pro operační systém a instalované aplikace nepřináší žádná omezení.

## Bezpečnostní záruky řešení

Jedinečná koncepce a architektura KP LANPCS-RG3 přináší velmi vysoké záruky zabezpečení veškeré vnější komunikace počítače zcela nezávisle na aktuálním:

- stavu a (ne)důvěře v hardware počítače,
- stavu a konfiguraci (ne)zabezpečení operačního systému a aplikací počítače,
- stavu a (ne)důvěře v síťové prvky lokální síťové infrastruktury,
- stavu a způsobu fyzického připojení počítače k lokální síti.

## Podpora správy počítačů

Výjimečná integrace šifrátoru do interní síťové karty, s úplným oddělením všech operací zajišťujících ochranu vnější komunikace (nejen vlastní kryptografie), umožňuje provozování počítače bez znatelných omezení, tedy včetně standardní:

- centrální správy a dohledu hardwaru počítačů,
- centrální správy a dohledu OS a aplikací počítačů,
- údržby a servisu hardwaru počítačů (bez LANPCS-RG3).

V případě, že počítač je provozován v režimu bezpečného terminálového klienta, který neumožňuje ukládání utajovaných informací na lokální disk, není nutné evidovat lokální disk jako nosič utajovaných informací.

## Lokální síťová infrastruktura

Unikátní koncepce a architektura KP LANPCS-RG3 (kdy počítač mohou po síti opustit pouze zašifrovaná data), umožňuje využít standardní lokální síťovou infrastrukturu pro certifikované IS zpracovávající citlivé nebo utajované informace, a to provozovateli přináší tyto jednoznačné výhody:

- není nutné budování oddělené duplicitní a souběžně provozované lokální síťové infrastruktury v jednotlivých objektech (značné finanční úspory),
- zjednodušení procesu pořízení a servisu síťových aktivních prvků (nejsou požadovány žádné nadstandardní bezpečnostní požadavky),
- jednotná centrální správa a vzdálený dohled všech síťových aktivních prvků (změna konfigurace aktivního prvku není bezpečnostně významná z pohledu zajištění důvěrnosti).

## Podpora správy KP LANPCS-RG3

Verze firmwaru 3.x přichází s podporou autentizace založené na principech mechanismů PKI a oddělení správy bezpečnostních funkcí od síťové konfigurace. Výsledkem je nová centrální správa umožňující efektivní nasazení KP LANPCS-RG3 v rámci:

- rozsáhlých a členitých počítačových sítí,
- postupně budovaných, rozšiřujících se nebo průběžně se měnících certifikovaných IS,
- geograficky rozšiřovaných certifikovaných IS do nových lokalit bez nutnosti navyšování počtu správců kryptografického prostředku.

Nová centrální správa umožňuje provozovateli efektivní správu KP LANPCS-RG3 v reálném čase, bez nutnosti součinnosti s jejím okolím.

## Dlouhodobá udržitelnost investice

KP LANPCS-RG3 je postaven na speciálně vyvinutém důvěryhodném hardwaru, který umožňuje dlouhodobou udržitelnost provozu i tak bezpečnostně exponované aplikace, jako je certifikovaný kryptografický prostředek. Základem zachování investice je architektura, kde všechny bezpečnostně významné prvky (obvody a rozhraní) jsou v hardwaru realizovány prostřednictvím programovatelného hradlového pole. Díky tomu je možné provádět úplný rozvoj prostředku, tedy nejenom jeho firmwarové části.

KP LANPCS-RG3 proto umožňuje dlouhodobý rozvoj jak z pohledu vlastní funkcionality, tak z pohledu nutných reakcí na nové bezpečnostní hrozby, a to bez potřeby jakýchkoli kompromisů. Použitelnost KP LANPCS-RG3 pro budoucí OS je dlouhodobě zajištěna i možností zpřístupnění zdrojových kódů ovladačů síťového rozhraní.

Provozovatel certifikovaného IS tak v podobě KP LANPCS-RG3 získává dlouhodobě udržitelnou investici s minimální životností plánovanou na dobu 8 let od prodeje nebo ukončení výroby.

## Příklady nasazení

**Povýšení stávajícího IS na certifikovaný IS**
KP LANPCS-RG3 umožňuje ochranu komunikace ve standardním prostředí LAN i WAN s využitím existující nezabezpečené lokální a veřejné komunikační infrastruktury.

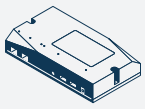
**Propojení izolovaných počítačů**
KP LANPCS-RG3 umožní bezpečně propojit již existující samostatné počítače, určené pro zpracování citlivých nebo utajovaných informací, umístěné v různých lokalitách. Přínosem je pak efektivní centrální správa a možnost online výměny informací. Tím dojde i k omezení exportu citlivých dat na nosiče utajovaných informací a potřeby jejich transportu.

**Nové rozsáhlé certifikované IS**
KP LANPCS-RG3 umožní jejich budování bez nutnosti vytvářet oddělené duplicitní a souběžně provozované lokální sítě a bez potřeby instalace standardních šifrátorů na hranice vzdálených objektů. To, mimo fi nančních úspor, přináší i značné časové úspory, což umožní zahájit budování certifikovaného IS bez zbytečných prodlev. Integrace KP LANPCS-RG3 přímo do počítačů uživatelů zajišťuje ideální distribuci šifrovacího výkonu při dosažení vysoké propustnosti certifikovaně chráněné komunikace. Ve spojení s technologií vzdáleného přístupu není nutné ve vzdálených lokalitách budovat a provozovat zabezpečené lokální serverovny.

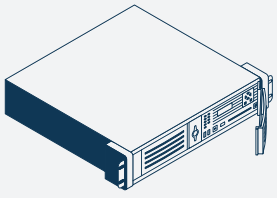
**Přesun stávajících počítačů**
Počítače určené pro zpracování citlivých nebo utajovaných informací, které jsou součástí již existujícího certifikovaného IS, je možné ze vzdálených zabezpečených prostor přesunout přímo na pracoviště uživatelů a tím umožnit významné zefektivnění jejich práce. Na tato pracoviště nejsou kladeny žádné nadstandardní požadavky z oblasti fyzické bezpečnosti. KP LANPCS-RG3 je sám o sobě bezpečným trezorem a uživateli zpřístupňuje pouze chráněné síťové rozhraní.

**Bezpečný terminál**
V dnešní době vzdálených ploch, terminálových řešení a virtualizace stanic se nabízí možnost zavést operační systém, včetně tenkého klienta, v chráněném (read-only) režimu. Primární problém tohoto řešení spočívá v neschopnosti OS auditovat svou činnost, pokud není navázáno síťové spojení s centrem. Nasazení KP LANPCS-RG3 poskytne zcela nezávisle audit významných událostí (včetně zapnutí a vypnutí počítače) a tím se technologie bezpečných terminálů stane vhodnou i pro použití v rámci certifikovaných IS. Ve všech případech je i při nasazení KP LANPCS-RG3 nadále možné plné využití moderních informačních technologií a produktů, určených pro běžné (necertifikované) IS. Jedná se například o podporu vzdálených center, IP telefonii, jednotnou centrální správu či vzdálený monitoring. Pro zajištění dostatečného výkonu a průchodnosti datových center jsou určeny výkonné hraniční KP LANPCS-Rack. Ty jsou plně kompatibilní s ostatními KP z rodiny LANPCS.

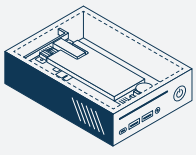
## Další produkty rodiny LANPCS:



**LANPCS Box**
Box řeší ochranu síťové komunikace periferních zařízení, jako jsou tiskárny, scannery nebo videokonferenční zařízení

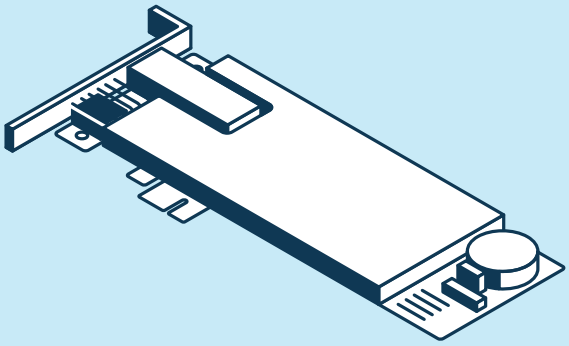


**LANPCS Rack**
Výkonné 1U zařízení určené pro budování rozsáhlých systémů zajistí dostatečný výkon / průchodnost center.



**LANPCS Terminál**
Stanice s možností bootu z read-only paměti.

# LANPCS RG3



## Základní parametry

### Požadavky na počítač:

- volný PCIe slot pro kartu s výškou 56 mm a délkou 168 mm

### Technické parametry:

- rozměry (D x V x Š): 168 x 69 x 12,1 mm (včetně konektoru)
- fyzické rozhraní: PCI Express 1.1 x1
- fyzická síťová vrstva: Ethernet 10/100/1000 Mbps (konektor RJ 45/volitelně optický interface)
- základní síťová vrstva: IPv4, IPv6
- bezpečnostní rozšíření IP: IPsec (RFC: 4301, 4303, 7296)
- provozní teplota: 0–45 °C (vnitřní teplota PC)

### Podporované OS:

- MS Windows a různé Linuxové distribuce
- Reálná datová propustnost:
- 80 Mbps (volitelně 220 Mbps s šifrovacím akcelerátorem)

### Provozní módy:

- manuální režim (provozní konfi gurace uložena v čipové kartě)
- autonomní režim (provozní konfi gurace je uložena v LANPCS-RG3)

### Vzdálený dohled:

- ICMP, SNMP agent, SNMP trap, syslog
- přenos logů na FTP

### Interní bezpečnostní funkce:

- fyzikální generátor náhody
- nezávislý čas
- nezávislý audit
- nezávislý dohledový procesor
- fyzická odolnost na úrovni FIPS 140-2 level 3

### Záruky dle Common Criteria:

- vývoj a návrh v souladu s požadavky úrovně EAL4+

### Třída kryptografi ckého prostředku:

- CCI dle standardu NÚKIB