PRODUCT SHEET

LANPCS-RG2

PROTECTION OF LAN/WAN COMMUNICATION

S.ICZ THE DAUGHTER COMPANY OF ICZ, CERTIFIED BY THE NATIONAL SECURITY AGENCY (NBÚ) FOR ACCESS TO CLASSIFIED INFORMATION UP TO LEVEL „TOP SECRET“, OFFERS COMPLEX SERVICES IN THE FIELD OF PROTECTION OF CLASSIFIED INFORMATION

LANPCS-RG2 establishes a layer of guaranteed protection for the network communication of a workstation that is used to process sensitive or classified information. The LANPCS-RG2 is an IPSec encryptor integrated into an internal network card, which is inserted inside the worsktation. This allows the use of current unsecured network infrastructure (wiring, firewalls, switches etc.) for connecting workstation, located in standard offices, to an information system certified for processing classified information.

When an information system is designed and built using the LANPCS-RG2 technology great savings are achieved due to the need of less stringent physical security requirements. At the same time, it removes barriers to effectively extending and utilizing system for processing classified information. Implementing LANPCS-RG2 transfers the communication layer outside the boundaries of the certified information system. This eliminates the costs tied to improving security of all communication routes and data centres as well as the costs of building a secondary separate and concurrently operated data network. Finally, this eliminates any restriction stemming from the geographical locations of the end user workstations. This lets you operate your information system where you really need it, and you can accommodate all organizational and operational changes with minimal costs.

CERTIFICATION

NBÚ certificate ID number K20185, is valid through 23.11.2020 and certifies the fitness of the cryptographical device for protection of classified information up to and including classification level:

- **RESTRICTED**
- **RESTREINT UE/EU RESTRICTED**
- **NATO RESTRICTED**

[EXECUTION]

The device is a self-contained cryptographic device (IPSec encryptor) in the form of a network card for the PCI Express bus.

The operating system is unaffected by the presence of the device as simple network interface drivers allow its use.

Basic functionality

The cryptographic device becomes an integral part of the workstation but its (the device's) cryptographical functions are completely separated from the operating system.

Fundamental security – Only encrypted data can leave the workstation, the operating system cannot affect the function of the device.

Eliminates the need for secondary, separate and concurrently operated data networks.

No crypto officer is necessary for the cryptographical device.

Enables single sealing (single protection) – security of the interior of the workstation extends to the protection of the built-in IPSec encryptor.

Implementation effectivity

The LANPCS-RG2 device is intended for standard IBM PC compatible computers MS windows or Linux OS.

Installation into the workstation OS is accomplished via software drivers that do not require classifying the HDD to any classification level.

From the point of view of the workstation and its OS, LANPCS-RG2 behaves like a standard network card and does not require or allow any management. Thus it places no burden on the user (It does not require a cryptographic device operator).

The choice of location of the workstation with a LANPCS-RG2 device does not influence the placement of any other components of the information system.

Typical use cases

Protection of communication in LAN and WAN environments (Use of existing unsecured or public communication infrastructure).

Connecting PC's currently isolated by Geography or networks (separate workstations intended for processing classified information). Opens the possibility of on-line management of the workstation and online exchange of CI thus limiting the need to export CI onto classified media.

Transfer of the current users workstation intended for processing classified information from separate protected spaces directly to the users workplace (extension of the existing certified information system for processing classified information).

Creating new IS intended for processing CI with full use of standard commercial products (e.g. for communication infrastructure, network services, AD domains including management)

Secure terminal operation designed for processing of CI (a PC in the form of a terminal without the ability to store CI on a local disk).

Advantages of a HW encrypted connection with LANPCS-RG2

Unified method – standardisation of data transfer between computers using online encryption, which is fully transparent for the host systems.

HW encryption of all transferred data brings both a physical and a logical barrier of independent protection, which is located between the workstation and the communication network.

Enables use of current communication infrastructure (wiring, network elements) without the necessity of making changes or restricting any functionality.

No special training for the end user is necessary – the end user does not become an operator of cryptographical device.

The device is fully transparent for the OS (it requires the installation of no software except for network card drivers)

The cryptographic keys never leave the LANPCS-RG2 (they are not available outside the confines of the device or workstation).

All cryptographic algorithms are performed within the LANPCS-RG2 device and cannot be influenced from the workstation.

The device ensures secure storage, management and destruction of encryption keys, and this is fully independent of the OS of the workstation it resides in.

LANPCS-RG2 supports multi level management and remote monitoring.

Supports operation using a model of simple local administration (does not require the management and monitoring center).

Provides independent auditability of security related events which are stored on a memory module inside the LANPCS-RG2 device which ensures their protection against unauthorizaed manipulation.

[POWERFUL DEVICE FOR CENTRAL LOCATIONS]

When building large systems, where individual workstations equipped with the LANPCS-RG2 cryptographic devices, need to communicate with one or more central locations, the powerful LANPCS-Rack solution is provided to ensure sufficient capacity and throughput. This solution is fully compatible with the other cryptographic devices of the LANPCS family (LAPNCS-RG2, LANPCSe-AES, LANPCS-AES). Detailed information about the boundary cryptographic device LANPCS-Rack can be found in its own product list.

[REFERENCES]

Using the cryptographic devices of the LANPCS family along with other security products provided by S.ICZ (e.g. PCS1, AirGap 02) real certified information systems for processing classified information, with significant user comfort and large added security value can be built. Users can then work with online applications for processing classified information from the comfort of thei won office and simultaneously the solution allows the systems to provide lasting exchange of classified information between organizations. An example of such an information system is the upgrade of IS EU Extranet ČR-V, which is designed for national distribution of official classified document from the EU commission.

[BASIC PARAMETERS OF LANPCS-RG2]

Workstation requirements:

- PCI Express interface (empty PCI Express slot for a card of 168mm length)

Technical parameters:

- Size (L x H x W): 168 x 56 x 12,1 (mm)
- Weight: 180g
- Physical PCI interface: PCI Express 1.1 x1
- Physical network layer: Ethernet 10/100/1000 Mbps (RJ 45 connector)
- Basic network layer: IPv4, IPv6
- IP security extension: IPsec (RFC 2406 – ESP)
- Smart card reader: ISO 7816 &EMV 2000 level 1 connected to and internal or external USB connector of the LANPCS-RG2 Device
- Operational temperature: 0-40 deg. C (internal PC temperature)
- Relative humidity: 5-90% (noncondensing)

Supported OS's:

- MS Windows
- Linux kernel 2.6 and higher (Debian distribution preferred)
- Support for 32 and 64 bit OS's

Data throughput:

- 80 Mbps (real operation)

Operational modes:

- Manual mode (operation configuration stored in a smart card)
- Autonomous mode (no crypto officer necessary, operation configuration of the cryptographic device stored in LANPCS-RG2)

Remote monitoring:

- ICMP
- SNMP
- FTP log transfer

Cryptography:

- Algorithms: AES 256, HMAC SHA-256, Diffie-Hellman

Internal security functions:

- Physical randomness generator
- Independent service
- Independent audit
- Monitoring processor

Cryptographic device class:

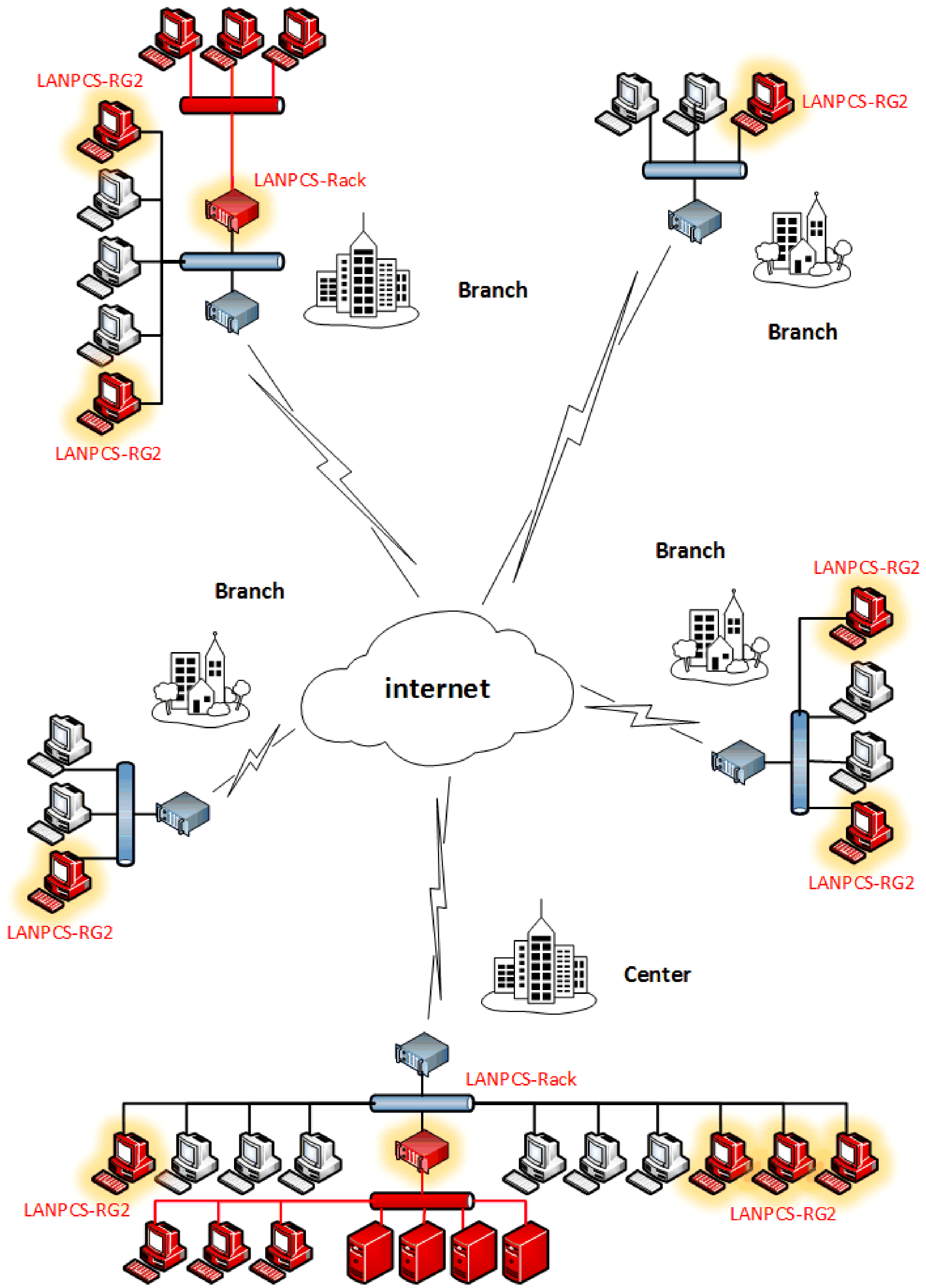
- CCI

Common Criteria security assurances:

- Design and development was performed in accordance with requirements for security assurances at the EAL4+ level

Sales contact

S.ICZ a.s. Na hřebenech II 1718/10
140 00 Praha 4 Nusle
TEL.: +420 222 271 111
E-MAIL: obchod_SICZ@iczgroup.com


LANPCS-RG2
LANPCS-Rack
Branch
LANPCS-RG2
LANPCS-RG2
Branch
Branch
LANPCS-RG2
Branch
internet
LANPCS-RG2
LANPCS-RG2
Center
LANPCS-Rack
LANPCS-RG2
LANPCS-RG2