LANPCSe-AES

PROTECTING LAN COMMUNICATION

S.ICZ, A SUBSIDIARY OF ICZ WHICH IS CERTIFIED BY THE CZECH NSA (NBÚ) FOR ACCESS TO CLASSIFIED INFORMATION UP TO THE "TOP SECRET" CLASSIFICATION LEVEL, OFFERS COMPREHENSIVE SERVICES IN THE FIELD OF CLASSIFIED INFORMATION PROTECTION.

LANPCSe-AES creates a layer of guaranteed network communication security for a workstation, which is used to process confidential or classified information. The main feature of the certified LANPCSe-AES solution is the integration of an IPSec encryption device as an internal network card, which is placed inside the workstation. Deploying this cryptographic device allows the use of existing unsecured communication infrastructure (Ethernet cables, network elements) for connecting workstations in normal offices to an information system certified for processing classified information.

When LANPCSe-AES is used when designing and building an information system, the overall cost of physical security measures that need to be deployed is markedly reduced. Furthermore, security restrictions which prevent the effective use and extension of systems processing classified information are removed. The use of LANPCSe-AES makes it possible to displace the actual underlying communication infrastructure beyond the boundaries of the certified information system. This eliminates the costs associated with increasing the physical security of all communication channels and any rooms containing communication infrastructure (such as hubs, switches, routers and similar). At the same time there is no need to create a separate and duplicate communication infrastructure for non-classified information, and geographical location no longer constitutes a barrier to extending the classified information system. This makes it possible to extend the information system to wherever you need it to be and to make cheap dynamic changes when necessary.

CERTIFICATION

The Czech NSA certificate, registration number K20158, is valid until 22.01.2019 and certifies the fitness of the cryptographic device for protection of classified information up to and including levels:

- RESTRICTED
- RESTREINT UE/EU RESTRICTED
- NATO RESTRICTED

Design

- LANPCSe-AES is a self-contained hardware cryptographic device (IPSec encryptor) in the form of a PCI Express network card.
- The OS can use the hardware as if it was a standard network card with a provided driver.

Basic functionality

- The cryptographic device becomes an integral part of the workstation, but its cryptographic functions are completely separated from the workstation's OS.
- Fundamental security – any data leaving the workstation over the network is always encrypted. The operating system cannot influence the functioning of the cryptographic device in any way.
- Eliminates the necessity for a duplicate and concurrently managed data network for unclassified information.
- Does not need cryptographic staff for day-to-day operation.
- Makes it possible to only use a single seal – the protection of the interior of the workstation also includes protection of the LANPCSe device.

Implementation

- LANPCSe-AES is intended for standard IBM PC compatible computers with a MS Windows or Linux operating system.
- The drivers that need to be installed in the computer OS do not necessitate that its HDD be classified.
- From the point of view of the operating system LANPCSe-AES behaves as a standard network card and no cryptographic staff is necessary for its normal operation.
- The choice of placement of a workstation using LANCPSe-AES has no effect on the placement of other information system components.

Typical usage

- Protecting communication over LAN/WAN networks (using existing unsecured, possibly public communication infrastructure).
- Connecting currently isolated PCs (independent workstations designated for processing classified information). Allows remote administration and online exchange of CI. Limits situations when CI must be exported.
- Transfer of existing workstations for processing CI from specially secured areas straight to the user's desktop (extension of the existing IS for processing CI).
- Design and implementation of new information systems with full use of standard tools (e.g., for communication infrastructure, basic network services or using AD services, including management).
- Processing CI via terminal access (the workstation acts as a terminal and has no ability to store CI locally).

Key advantages of using a HW encrypted connection with LANPCSe-AES

- Unified method – a standardized approach to data transmission using on-line encryption between computers. For all other components of the information system this is fully transparent.
- HW encryption of all transmitted data, providing both a physical and a logical barrier of independent security between the workstation and the network.
- Allows the utilization of existing communication infrastructure (cables, switches, routers, etc.) without necessitating changes of functionality.
- No special end user training required – the end user is not cryptographic staff.
- The device is fully transparent to the OS and any applications (no extra software needs to be installed save for the drivers).
- Cryptographic keys never leave the LANPCSe-AES device (they cannot be accessed by the workstation).
- All cryptographic algorithms are carried out fully in the LANPCSe-AES device and cannot be influenced by the workstation.
- Provides secure storage, management and destruction of encryption keys which is fully independent of the workstation OS.
- Allows multilevel management and remote oversight, but is also usable in a simple local management mode.
- Audits all security-relevant events internally in the memory of the LANPCSe-AES device, which ensures long-term protection against unauthorized manipulation.

Robust solution for centres

When large systems are being built, where individual workstations with LANPCSe-AES access one or more central computers, a more robust solution is necessary to ensure sufficient throughput. For these cases the LANPCS-Rack solution is available. LANPCS-Rack is fully compatible with all other cryptographic devices of the LANPCS family (LANPCSe-AES, LANPCS-AES). More details can be found in the dedicated product sheet for LANPCS-Rack.

References

Integrating the LANPCSe-AES cryptographic device with other security products from S.ICZ (e.g., PCS1, AirGap 02) enables the designing and building of certified information systems for processing classified information with a high user comfort factor and high added security value. It allows users to gain online access to classified information within their organization from their own office, and at the same time it is possible for these systems to securely exchange information even with other organizations. One example of the implementation of such a system is IS EU Extranet ČR, which is used for the nationwide distribution of official classified documents from the European Commission.

■ Basic LANPCSe-AES parameters

PC requirements:
- PCI Express interface (free slot for a card 168 mm in length)

Technical parameters
- size (L x H x W): 168 x 111 x 14.7 (mm)
- physical PCI interface: PCI Express 1.1 x1
- physical network layer: Ethernet 10/100 Mbps (RJ 45 connector)
- basic network layer: IPv4
- IP security enhancement: IPsec (RFC 2406 – ESP)
- smart card reader: ISO 7816 & EMV 2000 level 1 connected to either the internal or the external LANPCSe-AES connector
- operational temperature: 0-45 deg. C (internal temperature of the PC)
- relative humidity: 5-95% (no condensation)

Supported OS:
- MS Windows
- Linux kernel 2.6 and higher (Debian distribution preferred)
- supports both 32 and 64 bit OS

Data throughput:
- 40 Mbps (physical maximum)
- 34 Mbps (real operation)

Operational modes:
- manual mode (communication configuration stored on smart card)
- autonomous mode (no cryptographic staff necessary, configuration stored on LANPCSe-AES)

Remote monitoring:
- ICMP
- SNMP
- log transfer over FTP

Cryptography:
- algorithms: AES 256, HMAC SHA-256, Diffie-Hellman

Internal security functions:
- physical random number generator
- independent time
- independent audit
- security processor

Cryptographic device class:
- CCI

Common Criteria assurance level:
- design and development was performed in accordance with assurance level EAL4+

COMMERCIAL CONTACT

S.ICZ a.s. Na hrebenech II 1718/10
140 00 Prague 4
TEL.: +420 222 271 111
FAX: +420 222 271 112
E-MAIL: SIZC@i.cz