PCS1e

WORKSTATION SECURITY

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.

The PCS1e cryptographic device represents a comprehensive solution to the problem of securing sensitive data stored on a workstation's local or remote storage device. The technology is based on the permanent storage of sensitive data solely in an encrypted form regardless of the specific technical solution used for the data storage. In order to ensure the maximum level of security, all encryption and decryption is performed in a separate dedicated hardware module which cannot be negatively influenced from the workstation. Access to the device's cryptographic functions and protected keys is only possible once the device has successfully authenticated the user. These measures ensure that it is only possible to gain access to the data in an unencrypted form once the user has been authenticated by both the workstation and the cryptographic device. The PCS1e solution thus provides comprehensive hardware protection for a workstation which is used to process classified information up to and including the "SECRET" level.

A compact hardware device with its own operating system which is physically installed in the host PC, but performs its functions completely independently of the host PC's CPU, memory and data storage, lies at the heart of the reliable encryption. The active and permanent protection of the cryptographic keys and any operations performed with them is a central feature of the solution. Using the PCS1e cryptographic device in your information system's workstations not only ensures the certified cryptographic protection of classified information, but also primarily provides you with security technology which allows you to lower the physical and administrative security requirements of your information system.

CERTIFICATION

The Czech NSA certificate, registration number K20165, is valid until 22.01.2019 and it certifies the fitness of the cryptographic device for the protection of classified information up to and including the following levels:

- SECRET for national classified information
- CONFIDENTIEL UE/EU CONFIDENTIAL
- NATO CONFIDENTIAL

Design

- A hardware adapter in the form of a PCI Express expansion card for an IBM PC compatible computer which preforms all security related and cryptographic functions fully separately from the host PC.
- Software for a host PC running a Microsoft Windows operating system which ensures the integration of the cryptographic and security related functions into the user environment and applications.

Basic functionality

- The online cryptographic protection of files (containing classified information) processed in the host PC and realised in the form of transparent encryption of the stored files and allowing for the management of the cryptographic functionalities at the level of folders, logical disks, removable media and remote network storage.
- The offline cryptographic protection of files (containing classified information) processed in the host PC and realised in the form of secure encrypted file archives primarily intended for the storage and transfer of data across the boundary of the secured information system (e.g. using e-mail over a public network such as the Internet).

User experience

- PCS1e is designed for IBM PC compatible computers with a Microsoft Windows operating system.
- PCS1e is a user friendly solution – the encryption and decryption occurs transparently and automatically. The user only needs to provide the device with authentication using a smart card and a PIN.
- Installation of the PCS1e cryptographic device makes it possible to reduce the requirements placed on physical security and the security of the communication systems.

Ensuring comprehensive protection

- User access control of the host PC's operating system is realised using a smart card.
- Access to the data in the encrypted files stored on the host PC's local, network and removable data storage devices is authorized using a smart card.
- System protection ensured by the encryption of the user profile, parts of the system's data regions, the temporary and residual information on disk and the system configuration.
- An independent audit log of security relevant events is created and stored in the PCS1e hardware device's internal memory module and is protected from any unauthorized modification.

The key features of the PCS1e hardware encryption solution

- The transparent encryption of files containing classified information when they are being stored locally or remotely
- An independent file access control layer for encrypted and unencrypted files which complements the standard file access control at the OS level
- An integration interface (customer applications with strong security functionalities, integration of cryptographic protection into standard applications)
- Strong cryptographic key protection – the keys never leave the PCS1e and are inaccessible to the host PC
- Secure implementation of the cryptographic algorithms – the algorithms are inaccessible to the processes running on the host PC (they can only be accessed through an API)
- Secure storage and constant protection of the keys – the keys in the device are actively protected even when the power is turned off

The key capabilities of the PCS1e solution

- The constant protection of the files in the certified IS (classified information needs never appear in any local, network or removable data storage in plain text)
- The construction of a complex, secured workstation (the strong identification and authentication of the user, the constant protection of files containing classified information and the protection of the system data and configuration)
- Independent access control and protection for files containing classified information – strong guarantees (separate information categories, multiple independent levels of protection, ability to allow/deny classified information export in plain text to removable media, limited access of the administrator to the stored data)
- Expansive cryptographic key management functionalities, flexible key management (more choices for the information system architect), the management can be automated

References

The integration of the PCS1e cryptographic device with other security products from S.ICZ makes it possible to design and build certified information systems for processing classified information with a high user comfort factor and a high added security value. An example of just such an information system is the MZV-KR IS which contains nodes with different levels of classification and allows the processing and exchange of classified information between the Ministry of Foreign Affairs of the Czech Republic and Czech embassies abroad.

Basic PCS1e parameters

PC requirements:

- PCI Express interface (a free slot for a 168 mm long card)

Technical parameters

- size (L x H x W): 168 x 111 x 14.7 (mm)
- physical PCI interface: PCI Express 1.1 x1
- smart card reader: ISO 7816 & EMV 2000 level 1 connected to either the internal or the external LANPCSe-AES connector
- operating temperature: 0-45 deg. C (internal temperature of the PC)
- relative humidity: 5-95% (no condensation)

Supported OS:

- MS Windows 7, MS Windows server 2008 R2 (online and offline encryption with support for 32 and 64 bit OS)
- MS Windows XP (only for offline encryption)

User authentication

- A physical smart card operated by the PCS1e hardware adapter
- Follow up methods of I/A to the OS: secret password, certificate (Smart Card Logon)

Application interface

- PKCS #11
- MS Crypto API

Implementation of encryption in the OS:

- Transparent online encryption: files, folders, logical disks, removable media, remote network storage
- Offline file encryption
- Asymmetry (signatures, encryption)

Cryptography:

- Algorithms: National algorithm (speed 3.2 MB/s), AES 256 (speed 12 MB/s), RSA 2048
- SHA 256 hash algorithm

Secure key storage:

- Deactivation/destruction – it can be wired to an external contact
- A multi-level key system
- Max. number of storage units: 30
- Max. number of keys in a unit: 400
- Max. number of keys: 12,000 (30x400)

Other security functions

- A physical random number generator
- Independent time
- Independent audit

A security processor

- System security
- The user profile can be encrypted
- The system data can be encrypted (spooler, temp, ...)
- The export of data in the plain text format can be controlled

Cryptographic device class

- CCI

Physical security

- Parameter S1=7

Common Criteria assurance level

- The design and development have been 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