DATASHEET

AUTHENTICATION WITH KEYS

What is key authentication?
The introduction of authentication with keys is part of the use of two-factor authentication. This rovides additional security for user credentials during the login process. This results in the introduction of additional layers of authentication.

WHY USE **KEY AUTHENTICATION?**?

- Minimize the risk of data leakage,
- the ability to authorize user accounts,
- full support in the process of configuring the certificate and Apache Tomcat 8.5,
- protection against unwanted access,
- use of ePass as an additional authentication layer,
- use of encrypted communication (HTTPS).

TWO-FACTOR AUTHENTICATION IN THE EAUDITOR SYSTEM

The eAuditor system enables authentication through an authentication layer, referred to as ePass. With this, in addition to the standard way of logging in (providing an access element such as a login and password), which confirms the user's credentials through the system for local accounts or AD DS./LDAP for domain accounts, authentication with physical hardware security is required.

HIGH SECURITY WITH ENCRYPTED COMMUNICATION

The default system configuration uses HTTP (unencrypted data transfer for the Internet). Configuration of HTTPS encrypted communication is required for two-factor authentication. As part of the implementation, IT administrators receive full support for generating a certificate and configuring Apache Tomcat 8.5.

TECHNICAL REQUIREMENTS OF USB TOKENS

Supported operating systems
- 32bit and 64bit Windows XP SP3, Server 2003, Vista, Server 2008, 7
- 32bit and 64bit Linux
- MAC OS X

Software "middleware"
- Microsoft Windows MiniDriver
- Windows middleware for Windows CSP
- PKCS#11 library for Windows, Linux, MAC

Standards
- X.509 v3 certificate store, SSl v3, IPSec, ISO 7816 1-4 8 9 12, CCID

Cryptographic functions
- Key pair generation (inside key)
- Electronic signature and signature verification (inside the key)
- Data encryption and decryption (inside the key)

Cryptographic algorithms
- RSA 512/1024/RSA 2048 bit
- ECDSA 192/256 bit
- DES/3DES
- AES 128/192/256 bit
- SHA-1/SHA-256

Cryptographic APIs
- Microsoft Crypto API (CAPI), Cryptography API: Next generation (CNG)
- Microsoft Smart Card MiniDriver
- PKCS#11
- PC/SC

Processor
- 16 bit smart card chip (Common Criteria EAL 5+ certified)

Memory
- 64KB (EEPROM)

Memory life
- At least 500,000 write/read cycles
- More than 10 years

Connection
- USB 2.0, type A connector

Power consumption
- Less than 250 mW

Operating temperature
- Od 0 do +70 degrees

Storage temperature
- -20 do +85 degrees

Humidity
- From 0% to 100% without condensation