DATASHEET

UWIERZYTELNIANIE ZA POMOCĄ KLUCZY

Czym jest uwierzytelnianie za pomocą kluczy?
Wprowadzenie uwierzytelniania za pomocą kluczy, stanowi element wykorzystania uwierzytelniania dwuskładnikowego. Dzięki temu możliwe jest dodatkowe zabezpieczenie poświadczeń użytkownika podczas procesu logowania. Skutkuje to wprowadzeniem dodatkowych warstw uwierzytelniających.

DLACZEGO WARTO KORZYSTAĆ Z **UWIERZYTELNIANIA ZA POMOCĄ KLUCZY**?

- Minimalizowanie ryzyka wycieku danych,
- możliwość autoryzacji kont użytkowników,
- pełne wsparcie w procesie konfiguracji certyfikatu oraz Apache Tomcat 8.5,
- zabezpieczenie przed niepożądanym dostępem,
- wykorzystanie ePass jako dodatkowej warstwy uwierzytelniającej,
- wykorzystanie szyfrowanej komunikacji (HTTPS).

UWIERZYTELNIANIE DWUSKŁADNIKOWE W SYSTEMIE EAUDITOR

System eAuditor umożliwia uwierzytelnianie za pomocą warstwy uwierzytelniającej, określanej jako ePass. Dzięki temu oprócz standardowego sposobu logowania (podanie elementu dostępu, jakim jest login i hasło), który potwierdza poświadczenia użytkownika przez system dla kont lokalnych lub AD DS./LDAP dla kont domenowych, wymagana jest autoryzacja fizycznym zabezpieczeniem sprzętowym.

WYSOKIE BEZPIECZEŃSTWO ZA POMOCĄ SZYFROWANEJ KOMUNIKACJI

Domyślna konfiguracja systemu wykorzystuje protokół HTTP (niezaszyfrowane przesyłanie danych dla sieci internetowej). Do uwierzytelniania dwuskładnikowego wymagane jest skonfigurowanie szyfrowanej komunikacji HTTPS. Administratorzy IT w ramach implementacji otrzymują pełne wsparcie w zakresie generowania certyfikatu oraz konfigurowania Apache Tomcat 8.5.

WYMAGANIA TECHNICZNE TOKENÓW USB

Wspierane systemy operacyjne
- 32 bit oraz 64 bit Windows XP SP3, Server 2003, Vista, Server 2008, 7
- 32bit oraz 64bit Linux
- MAC OS X

Oprogramowanie “middleware”
- Microsoft Windows MiniDriver
- Windows middleware for Windows CSP
- Biblioteka PKCS#11 dla Windows, Linux, MAC

Standardy
- Magazyn certyfikatów X.509 v3, SSl v3, IPSec, ISO 7816 1-4 8 9 12, CCID

Funkcje kryptograficzne
- Generowanie pary klucza (wewnątrz klucza)
- Podpis elektroniczny i weryfikacja podpisu (wewnątrz klucza)
- Szyfrowanie i deszyfrowanie danych (wewnątrz klucza)

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

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

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

Pamięć
- 64KB (EEPROM)

Trwałość pamięci
- Przynajmniej 500 000 cykli zapis/odczyt
- Ponad 10 lat

Podłączenie
- USB 2.0, złącze typu A

Zużycie energii
- Mniej niż 250 mW

Temperatura pracy
- Od 0 do +70 stopni

Temperatura przechowywania
- -20 do +85 stopni

Wilgotność
- Od 0% do 100% bez kondensacji