cryptoVision

Technical Data Sheet

GreenShield File

04/2021

File encryption with BSI approval for VS-NfD, NATO Restricted and EU Restricted

GreenShield File is a solution for encrypting and signing files. As an add-in for Windows, GreenShield is easy to use. Encrypted files can be sent by e-mail and are recognized as encrypted mails by all common mail clients.

Functionality	Functions for protecting files: • Signing and verifying files • Encryption and decryption of files • Key- and certificate management
Features	• Key storage from smart card / USB token / softkey** • Generation of certificate requests and self-signed certificates* • Symmetric encryption (password) • PIN caching* • Generation of RSA and EC keys • Centralized configuration and management • Several certificate authorities can be used in parallel • LDAP / OCSP / HTTP(S) support • HTTP proxy support • Verification of certificates • X.509 certificates and X.509 revocation lists
Scope of supply	• GreenShield for Microsoft Windows • GreenShield Core System • PKCS#11 module
Supported standards	• S/MIME version 3.2 / 4 including ECC • PKCS#11 • Random from Smartcard / TR2101-1 pseudo random number generator • LDAP / OCSP / HTTP(S)
Evaluation and approval	• Verschlusssache – Nur für den Dienstgebrauch (VS-NfD) • NATO Restricted • EU Restricted Zulassungsnummer: BSI-VSA-10552
Supported operating systems	• Microsoft Outlook Windows 7 SP1*** • Microsoft Windows 10 (from 1809)

* Not permitted for VS-NfD, EU Restricted and NATO Restricted
** In coordination with the BSI
*** Microsoft support dicontinued as of 14 January 2020

Technical Data Sheet - GreenShield File

Supported algorithms	Asymmetric crypto algorithms: • RSA (up to 16384 bit, up to PKCS1#v2 incl. PSS/OAEP) • DSA/DH (up to 2048 Bit) • ECC (up to 571 Bit): NIST and Brainpool curves Symmetric crypto algorithms: • DES (56 bit)** • Triple-DES (168 bit)** • RC2 (40 bit, 64 bit, 128 bit)** • AES (128 bit, 196 bit, 256 bit) Hash algorithms: • SHA-1*, SHA-224*, SHA-256, SHA-384, SHA-512 • RIPEMD-128, RIPEMD-140, RIPEMD-160** • MD2, MD4, MD5**
Usage requirements: **VS-NfD,** **NATO Restricted** **EU Restricted**	Smartcards: • ePasslet Suite v3.0 on NXP JCOP 3 • ePasslet Suite v2.1 on NXP JCOP 2.4.2 • Electronic service and army identity card, based on CardOS-5 smart card (v4.2,v4.3) • PKIBw card (PKI-8Wv1.7, PKI-BWvL.8), based on CardOS-5-smart card • CardOS V5.0 with QES V1.1 PKI: • VS-NfD approval according to BSI-TR-03145 Certificates and revocation lists: • CRL or OCSP Middleware: • cryptovision SCinterface 8.0.x (PKCS#11 module)

* Not permitted for VS-NfD, EU Restricted and NATO Restricted
** For decryption only, supported to ensure compatiblility with outdated algorithms

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig

cv cryptovision GmbH
Munscheidstr. 14
D-45886 Gelsenkirchen

T: +49 209 16724-50
F: +49 209 16724-61

www.cryptovision.com
info@cryptovision.com