



Technical Data Sheet

GreenShield File

11/2021

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	<p>Functions for protecting files:</p> <ul style="list-style-type: none"> • Signing and verifying files • Encryption and decryption of files • Key- and certificate management
Features	<ul style="list-style-type: none"> • 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 • OpenPGP key rings and revocations* • Commandline-based usage possible*
Scope of supply	<ul style="list-style-type: none"> • GreenShield for Microsoft Windows and Ubuntu Linux • GreenShield Core System • PKCS#11 module
Supported standards	<ul style="list-style-type: none"> • S/MIME version 3.2 / 4 including ECC • OpenPGP* • PKCS#11 • Randomness from smart card / TR2101-1 based pseudo random number generator / jitter-based mechanisms • LDAP / OCSP / HTTP(S)
Evaluation and approval	<ul style="list-style-type: none"> • Verschlusssache – Nur für den Dienstgebrauch (VS-NfD) • NATO Restricted • EU Restricted <p>Zulassungsnummer: BSI-VSA-10600</p>
Supported operating systems	<ul style="list-style-type: none"> • Microsoft Windows 10 (from 1809) • Ubuntu Linux 20.04 LTS*

* In coordination with the BSI ** Not permitted for VS-NfD, EU Restricted and NATO Restricted

Technical Data Sheet - GreenShield File

Supported algorithms	<p>Asymmetric crypto algorithms:</p> <ul style="list-style-type: none">• 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 <p>Symmetric crypto algorithms:</p> <ul style="list-style-type: none">• DES (56 bit)*• Triple-DES (168 bit)*• RC2 (40 bit, 64 bit, 128 bit)*• AES (128 bit, 196 bit, 256 bit) <p>Hash algorithms:</p> <ul style="list-style-type: none">• 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	<p>Smartcards:</p> <ul style="list-style-type: none">• Cryptovision ePasslet Suite v2.1 on NXP JCOP 2.4.2r3• Cryptovision ePasslet Suite v3.0 on NXP JCOP 3• Cryptovision ePasslet Suite v3.0 on G&D Sm@rtCafé Expert 7 (Veridos Suite v3.0)• CardOS V5.0 with QES V1.1 of Atos IT Solutions and Services GmbH• Elektronischer Dienst- und Truppenausweis, based on CardOS V5.0 (v4.2, v4.3)• PKIBw-Card (PKI-BW v1.7, PKI-BW v1.8), based on CardOS V5.0• CardOS V5.3 QES, V1.0• CardOS DI V5.4 QES Version 1.0• TCOS 3.0 – Signature Card Version 2.0 Release 2• TCOS 4.0 – TeleSec IDKey with NetKey Plus <p>PKI:</p> <ul style="list-style-type: none">• VS-NfD approval according to BSI-TR-03145 <p>Certificates and revocation lists:</p> <ul style="list-style-type: none">• CRL or OCSP <p>Middleware:</p> <ul style="list-style-type: none">• cryptovision SCinterface 8.0.x (PKCS#11 module)

* For decryption only, supported to ensure compatibility with outdated algorithms

** Not permitted for VS-NfD, EU Restricted and NATO Restricted



cv cryptovision GmbH
Munscheidstr. 14
D-45886 Gelsenkirchen

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

www.cryptovision.com
info@cryptovision.com