Technical Data Sheet

Eviden GreenShield File

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	• S/MIME & OpenPGP support • Symmetric encryption (password-based) • Key storage on smart card / USB token / softkey • Generation of RSA and EC keys • Generation of certificate requests and self-signed certificates • Generation of key rings and revocations • X.509 certificates and X.509 revocation lists • Usage of several certificate authorities in parallel • LDAP / OCSP / HTTP(S) support • HTTP proxy support • PIN caching • Centralized configuration and management • GUI- and commandline-based usage • API for integration in third-party applications*
Scope of supply	• GreenShield Extension for Windows Explorer and Ubuntu Nautilus • GreenShield Core System • PKCS#11 module
Supported standards	• S/MIME version 3.2 / 4 including ECC • OpenPGP • PKCS#11
Accessibility	• Very good accessibility for users without sight and for users with motor or auditory impairments • Good accessibility for users with impaired vision
Supported operating systems	• Microsoft Windows 11 • Ubuntu Linux 20.04 LTS

* Extension

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 • PQC-Preview: ML-DSA und ML-KEM** 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-160* • MD2, MD4, MD5*
Approval and usage requirements: VS-NfD, NATO Restricted EU Restricted	Smartcards: • Eviden ePasslet Suite v3.0 on NXP JCOP 3 • Eviden ePasslet Suite v3.0 on G&D Sm@rtCafé Expert 7 (Veridos Suite v3.0) • CardOS V5.0 with QES V1.1 • Elektronischer Dienst- und Truppenausweis, based on CardOS V5.0 (v4.2, v4.3, v4.4) • PKIBw-Card (PKI-Bw v1.7, v1.8, v1.9, tPKI-Bw v7.1), based on CardOS V5.0 • CardOS V5.3 QES, V1.0 • CardOS DI V5.4 QES Version 1.0 • CardOS V6.0 DI (R1.0, R1.1) • TCOS 3.0 – Signature Card Version 2.0 Release 2 • TCOS 4.0 – TeleSec IDKey with NetKey Plus • Secunet SINA Workstation virtual SmartCard from SINA OS 3.5.2.3 PKI: • VS-NfD approval according to BSI-TR-03145 Middleware: • Eviden SCinterface 8.3.x (PKCS#11 module) Approval IDs: • BSI-VSA-10912

* For decryption only, supported to ensure compatiblility with outdated algorithms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

Security made in EU
Trust Seal
www.teletrust.de/itsmie

Eviden Digital Identity
cv cryptovision GmbH
Munscheidstr. 14
D 45886 Gelsenkirchen

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

www.eviden.com