Technical Data Sheet

cryptovision GreenShield File

Datei-Verschlüsselung mit BSI-Zulassung für VS-NfD, NATO Restricted und EU Restricted

GreenShield File ist eine Lösung für das Verschlüsseln und Signieren von Dateien. Durch die Integration in Microsoft Windows ist GreenShield leicht zu bedienen. Verschlüsselte Dateien lassen sich unter anderem per E-Mail verschicken und werden von den gängigen Mail-Clients als verschlüsselte Mails erkannt.

Funktionen	Funktionen für den Schutz von Dateien: • Signieren und Verifizieren von Dateien • Ver- und Entschlüsseln von Dateien • Schlüssel- und Zertifikatsmanagement
Features	• S/MIME- und OpenPGP-Unterstützung • Symmetrische Verschlüsselung (Passwort) • Schlüsselnutzung von Smartcard / USB-Token / Softkey • Erzeugung von RSA- und EC- Schlüsseln • Generierung von Zertifikatsanträgen und selbstsignierten Zertifikaten • Generierung von Schlüsselbunden und Widerrufen • X.509-Zertifikate und X.509-Sperrlisten • Mehrere Zertifizierungsstellen gleichzeitig nutzbar • LDAP- / OCSP- / HTTP(S)-Unterstützung • HTTP-Proxy-Unterstützung • PIN-Caching* • Zentrale Konfiguration und Verwaltung • Verwendung per GUI oder skriptbasiert per Kommandozeile möglich • API zur Anbindung durch Drittanbieter**
Lieferumfang	• GreenShield Extension für Windows Explorer und Ubuntu Nautilus • GreenShield Core System • PKCS#11 Modul
Unterstützte Standards	• S/MIME Version 3.2 / 4 einschließlich ECC • OpenPGP • PKCS#11 • Zufall von Smartcard / Pseudozufallsgenerator angelehnt an TR2102 / Jitter-basierte Mechanismen
Zulassung	• Verschlusssache – Nur für den Dienstgebrauch (VS-NfD) • NATO Restricted • EU Restricted Zulassungsnummer: BSI-VSA-10602, BSI-VSA-10632
Unterstützte Betriebssysteme	• Microsoft Windows 10 (ab 1809) • Microsoft Windows 11 • Ubuntu Linux 20.04 LTS

* Für VS-NfD, EU Restricted und NATO Restricted nicht zugelassen ** Erweiterung

Technical Data Sheet - GreenShield File

Unterstützte Algorithmen	Asymmetrische Krypto-Algorithmen: • RSA (bis 16384 Bit, bis PKCS1#v2 inkl. PSS/OAEP) • DSA/DH (bis 2048 Bit) • ECC (bis 521 Bit): NIST- und Brainpool-Kurven Symmetrische Krypto-Algorithmen: • DES (56 Bit)* • Triple-DES (168 Bit)* • RC2 (40 Bit, 64 Bit, 128 Bit)* • AES, AES-GCM (128 Bit, 196 Bit, 256 Bit) Hash-Algorithmen: • SHA-1**, SHA-224**, SHA-256, SHA-384, SHA-512 • RIPEMD-128, RIPEMD-140, RIPEMD-160* • MD2, MD4, MD5*
Einsatzbedingungen: VS-NfD, NATO Restricted EU Restricted	Smartcards: • Cryptovision ePasslet Suite v2.1 auf NXP JCOP 2.4.2r3 • Cryptovision ePasslet Suite v3.0 auf NXP JCOP 3 • Cryptovision ePasslet Suite v3.0 auf G&D Sm@rtCafé Expert 7 (Veridos Suite v3.0) • CardOS V5.0 mit QES V1.1 von Atos IT Solutions and Services GmbH • Elektronischer Dienst- und Truppenausweis, auf Basis von CardOS V5.0 (v4.2, v4.3, v4.4) • PKIBw-Card (PKI-Bw v1.7, v1.8, v1.9, tPKI-Bw v7.1), auf Basis von 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 mit NetKey Plus PKI: • Freigabe nach BSI-TR-03145 für VS-NfD Zertifikate und Sperrlisten: • CRL oder OCSP Middleware: • cryptovision SCinterface 8.0.x (PKCS#11-Modul)

* Nur zum Entschlüsseln, um Kompatibilität mit veralteten Verfahren zu gewährleisten

** Für VS-NfD, EU Restricted und NATO Restricted nicht zugelassen

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.cryptovision.com