



Technical Data Sheet

GreenShield File

01/2021

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	<p>Funktionen für den Schutz von Dateien:</p> <ul style="list-style-type: none"> • Signieren und Verifizieren von Dateien • Ver- und Entschlüsseln von Dateien • Schlüssel- und Zertifikatsmanagement
Features	<ul style="list-style-type: none"> • Schlüsselnutzung von Smartcard / USB-Token / Softkey** • Generierung von Zertifikatsanträgen und selbstsignierten Zertifikaten* • Symmetrische Verschlüsselung (Passwort)* • PIN-Caching* • Erzeugung von RSA- und EC- Schlüsseln • Zentrale Konfiguration und Verwaltung • Mehrere Zertifizierungsstellen gleichzeitig nutzbar • LDAP- / OCSP- / HTTP(S)-Unterstützung • HTTP-Proxy-Unterstützung • Verifizierung von Zertifikaten • X.509-Zertifikate und X.509-Sperrlisten
Lieferumfang	<ul style="list-style-type: none"> • GreenShield für Microsoft Windows • GreenShield Core System • PKCS#11 Modul
Unterstützte Standards	<ul style="list-style-type: none"> • S/MIME Version 3.2 / 4 einschließlich ECC • PKCS#11 • Zufall von Smartcard / Pseudozufallsgenerator nach TR2102 • LDAP / OCSP / HTTP(S)
Zulassung	<ul style="list-style-type: none"> • Verschlusssache – Nur für den Dienstgebrauch (VS-NfD) • NATO Restricted • EU Restricted <p>Zulassungsnummer: BSI-VSA-10467</p>
Unterstützte Betriebssysteme	<ul style="list-style-type: none"> • Microsoft Outlook Windows 7 SP1*** • Microsoft Windows 10 (ab 1809)

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

** In Abstimmung mit dem BSI

*** Microsoft-Support eingestellt zum 14.1.2020

Technical Data Sheet - GreenShield File

Unterstützte Algorithmen	<p>Asymmetrische Krypto-Algorithmen:</p> <ul style="list-style-type: none">• RSA (bis 16384 Bit, bis PKCS1#v2 inkl. PSS/OAEP)• DSA/DH (bis 2048 Bit)• ECC (bis 521 Bit): NIST- und Brainpool-Kurven <p>Symmetrische Krypto-Algorithmen:</p> <ul style="list-style-type: none">• DES (56 Bit)**• Triple-DES (168 Bit)**• RC2 (40 Bit, 64 Bit, 128 Bit)**• AES, AES-GCM (128 Bit, 196 Bit, 256 Bit) <p>Hash-Algorithmen:</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**
Einsatzbedingungen: VS-NfD, NATO Restricted EU Restricted	<p>Smartcards:</p> <ul style="list-style-type: none">• ePasslet Suite v3.5 auf NXP JCOP4• ePasslet Suite v3.5 auf G&D Sm@rtcafe 7• ePasslet Suite v3.5 auf Infineon SECORA ID X• ePasslet Suite v3.0 auf NXP JCOP 3• ePasslet Suite v2.1 auf NXP JCOP 2.4.2• Elektronischer Dienst- und Truppenausweis, basierend auf CardOS-5-Smartcard (v4.2,v4.3)• PKIBw-Karte (PKI-8Wv1.7, PKI-BWvL.8), basierend auf CardOS-5-Smartcard• TCOS 3.0, 4.0• TeleSec NetKey 3.0• Secunet Sina Workstation virtuelle SmartCard <p>PKI:</p> <ul style="list-style-type: none">• Freigabe nach BSI-TR-03145 für VS-NfD <p>Zertifikate und Sperrlisten:</p> <ul style="list-style-type: none">• CRL oder OCSP <p>Middleware:</p> <ul style="list-style-type: none">• cryptovision SCinterface 7.3.x (PKCS#11-Modul)

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

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



cv cryptovision GmbH
Munscheidstr. 14
D-45886 Gelsenkirchen

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

www.cryptovision.com
info@cryptovision.com