cryptoVision

Technical Data Sheet

GreenShield File

09/2019

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 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	• Schlüsselnutzung von Smartcard / USB-Token / Softkey* • Generierung von Zertifikatsanträgen und selbstsignierten Zertifikaten* • PIN-Caching* • 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	• GreenShield für Microsoft Windows • GreenShield Core System • PKCS#11 Modul**
Unterstützte Standards	• S/MIME Version 3.2 / 4 einschließlich ECC • PKCS#11 • PKIX • Zufall von Smartcard / Pseudozufallsgenerator nach TR2101-1* • LDAP / OCSP / HTTP(S)
Zulassung	• Verschlusssache – Nur für den Dienstgebrauch (VS-NfD) • NATO Restricted • EU Restricted Zulassungsnummer: BSI-VSA-10244
Unterstützte Betriebssysteme	• Microsoft Outlook Windows 7 SP1 • Microsoft Windows 10 (1809)

* Für VS-NfD, EU Restricted und NATO Restricted nicht zugelassen
** Konfigurierbar, aber zur Nutzung für VS-NfD obligatorisch

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: • ePasslet Suite v3.0 auf NXP JCOP 3 • 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 • ePasslet Suite v2.1 auf NXP JCOP 2.4.2 PKI: • nach BSI-TR-03145 mit den zusätzlichen Anforderungen von BSI-TR-03145 (VS-NfD-konform) Zertifikate und Sperrlisten: • CRL oder OCSP Middleware: • cryptovision SCinterface 7.1x (PKCS#11-Modul**)

* Für VS-NfD, EU Restricted und NATO Restricted nicht zugelassen
** Im Lieferumfang enthalten
*** Nur zum Entschlüsseln, um Kompatibilität mit veralteten Verfahren zu gewährleisten

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