cryptoVision

Technical Data Sheet

GreenShield Mail

09/2019

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

GreenShield Mail ist eine Lösung für das Verschlüsseln und Signieren von E-Mails. Als Add-in für Microsoft Outlook und IBM Notes bietet GreenShield Mail Ende-zu-Ende-Sicherheit.

Funktionen	Funktionen für den Schutz von E-Mails (mit Ende-zu-Ende-Sicherheit): • Signieren und Verifizieren von E-Mails • Ver- und Entschlüsseln von E-Mails • Schlüssel- und Zertifikatsmanagement
Features	• Schlüsselnutzung von Smartcard / USB-Token / Softkey* • Generierung von Zertifikatsanträgen und selbstsignierten Zertifikaten* • PIN-Caching* • Key Escrow (Message Recovery) • Zentrale Konfiguration und Verwaltung • Nutzung mehrerer Zertifizierungsstellen gleichzeitig • LDAP- / OCSP- / HTTP(S)-Unterstützung • HTTP-Proxy-Unterstützung • Verifizierung von Zertifikaten • X.509-Zertifikate, X.509-Sperrlisten • Efail-Immunität
Lieferumfang	• GreenShield-Add-in für Microsoft Outlook • GreenShield Add-in für IBM Notes • GreenShield Core System • PKCS#11 Modul**
Unterstützte Standards	• S/MIME Version 3.2 / 4 einschließlich ECC • PKCS#11 • PKIX • CDSA Sicherheits-Architektur • 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 E-Mail-Clients	• Microsoft Outlook 2010 / 2013 / 2016 / 2019 • IBM Notes 9.0.x

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

Technical Data Sheet - GreenShield Mail

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***
System-voraussetzungen	Client-Betriebssystem: • Microsoft Windows 7 SP1 • Microsoft Windows 10 (1809) E-Mail-Server: • IBM Domino 8.5 oder höher • Microsoft Exchange 2000 oder höher
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