



Technical Data Sheet

GreenShield Mail

01/2021

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	<p>Funktionen für den Schutz von E-Mails (mit Ende-zu-Ende-Sicherheit):</p> <ul style="list-style-type: none"> • Signieren und Verifizieren von E-Mails • Ver- und Entschlüsseln von E-Mails • Schlüssel- und Zertifikatsmanagement
Features	<ul style="list-style-type: none"> • Schlüsselnutzung von Smartcard / USB-Token / Softkey** • Generierung von Zertifikatsanträgen und selbstsignierten Zertifikaten* • PIN-Caching* • Erzeugung von RSA- und EC- Schlüsseln • Key Escrow (Message Recovery) • Zentrale Konfiguration und Verwaltung • Mehrere Zertifizierungsstellen gleichzeitig nutzbar • LDAP- / OCSP- / HTTP(S)-Unterstützung • HTTP-Proxy-Unterstützung • Verifizierung von Zertifikaten • X.509-Zertifikate, X.509-Sperrlisten • Efail-Immunität
Lieferumfang	<ul style="list-style-type: none"> • GreenShield-Add-in für Microsoft Outlook • GreenShield Add-in für IBM Notes • GreenShield Core System • PKCS#11 Modul
Unterstützte Standards	<ul style="list-style-type: none"> • S/MIME Version 3.2 / 4 einschließlich ECC • PKCS#11 • PKIX • CDSA Sicherheits-Architektur • Zufall von Smartcard / Pseudozufallsgenerator nach TR2102 • LDAP / OCSP / HTTP(S)
Zulassung	<ul style="list-style-type: none"> • Verschlussache – Nur für den Dienstgebrauch (VS-NfD) • NATO Restricted • EU Restricted <p>Zulassungsnummer: BSI-VSA-10467</p>
Unterstützte E-Mail-Clients	<ul style="list-style-type: none"> • Microsoft Outlook 2010 / 2013 / 2016 / 2019 / 365 • IBM Notes 9.0.x, HCL Notes 11

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

** In Abstimmung mit dem BSI

Technical Data Sheet - GreenShield Mail

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**
System-voraussetzungen	<p>Client-Betriebssystem:</p> <ul style="list-style-type: none">• Microsoft Windows 7 SP1***• Microsoft Windows 10 (1809) <p>E-Mail-Server:</p> <ul style="list-style-type: none">• IBM Domino 8.5 oder höher• Microsoft Exchange 2000 oder höher
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

*** Microsoft-Support eingestellt zum 14.1.2020



cv cryptovision GmbH
Munscheidstr. 14
D-45886 Gelsenkirchen

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

www.cryptovision.com
info@cryptovision.com