cryptoVision


Technical Data Sheet

# GreenShield Mail

04/2021

**E-mail encryption with BSI approval for VS-NfD, NATO Restricted and EU Restricted**

GreenShield Mail is a solution for encrypting and signing e-mails. As an add-in for Microsoft Outlook and IBM Notes, GreenShield enables end-to-end security.

| | |
|---|---|
| **Functionality** | Functions for protecting e-mails (end-to-end security):<br>• Signing and verifying mails<br>• Encryption and decryption of mails<br>• Key- and certificate management |
| **Features** | • Key usage from smart card / USB token / softkey**<br>• Generation of certification requests and self-signed certificates*<br>• PIN caching*<br>• Generation of RSA and EC keys<br>• Key escrow (message recovery)<br>• Centralized configuration and management<br>• Several certification authorities can be used in parallel<br>• LDAP / OCSP / HTTP(S) support<br>• HTTP proxy support<br>• Verification of certificates<br>• X.509 certificates and X.509 revocation lists<br>• Efail immunity |
| **Scope of supply** | • GreenShield add-in for Microsoft Outlook<br>• GreenShield add-in for HCL Notes<br>• GreenShield Core System<br>• PKCS#11 module |
| **Supported standards** | • S/MIME Version 3.2 / 4 including ECC<br>• PKCS#11<br>• PKIX<br>• CDSA security architecture<br>• Random from Smartcard / TR2101-1 pseudo random number generator<br>• LDAP / OCSP / HTTP(S) |
| **Evaluation and approval** | • Verschlusssache – Nur für den Dienstgebrauch (VS-NfD)<br>• NATO Restricted<br>• EU Restricted<br>Approval number: BSI-VSA-10552 |
| **Supported email clients** | • Microsoft Outlook 2010 / 2013 / 2016 / 2019<br>• IBM Notes 9.0.x, HCL Notes 11 |

* Not permitted for VS-NfD, EU Restricted and NATO Restricted
** In coordination with the BSI

# Technical Data Sheet - GreenShield Mail

| | |
|---|---|
| **Supported algorithms** | Asymmetric crypto algorithms:<br>• RSA (up to 16384 bit, up to PKCS1#v2 incl. PSS/OAEP)<br>• DSA/DH (up to 2048 Bit)<br>• ECC (up to 571 Bit): NIST and Brainpool curves<br>Symmetric crypto algorithms:<br>• DES (56 bit)**<br>• Triple-DES (168 bit)**<br>• RC2 (40 bit, 64 bit, 128 bit)**<br>• AES (128 bit, 196 bit, 256 bit)<br>Hash algorithms:<br>• SHA-1*, SHA-224*, SHA-256, SHA-384, SHA-512<br>• RIPEMD-128, RIPEMD-140, RIPEMD-160**<br>• MD2, MD4, MD5** |
| **System requirements** | Client operating system:<br>• Microsoft Windows 7 SP1***<br>• Microsoft Windows 10 (1809)<br>Email server:<br>• IBM Domino 8.5 or higher<br>• Microsoft Exchange 2000 or higher |
| **Usage requirements:**<br>**VS-NfD,**<br>**NATO Restricted**<br>**EU Restricted** | Smartcards:<br>• ePasslet Suite v3.0 on NXP JCOP 3<br>• ePasslet Suite v2.1 on NXP JCOP 2.4.2<br>• Electronic service and army identity card, based on CardOS-5 smart card (v4.2,v4.3)<br>• PKIBw card (PKI-8Wv1.7, PKI-BWvL.8), based on CardOS-5-smart card<br>• CardOS V5.0 with QES V1.1<br>PKI:<br>• VS-NfD approval according to BSI-TR-03145<br>Certificates and revocation lists:<br>• CRL or OCSP<br>Middleware:<br>• cryptovision SCinterface 8.0.x (PKCS#11 module) |

* Not permitted for VS-NfD, EU Restricted and NATO Restricted
** For decryption only, supported to ensure compatiblility with outdated algorithms
*** Microsoft support dicontinued as of 14 January 2020

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