Technical Data Sheet

cryptovision GreenShield Mail

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

GreenShield Mail is a solution for encrypting and signing emails. 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): • Signing and verifying mails • Encryption and decryption of mails • Key- and certificate management
Features	• S/MIME & OpenPGP support • Key storage on smart card / USB token / softkey • Generation of RSA and EC keys • Generation of certificate requests and self-signed certificates • Key escrow (message recovery) • X.509 certificates and X.509 revocation lists • Usage of several certification authorities in parallel • Generation of key rings and revocations • Centralized configuration and management • LDAP / OCSP / HTTP(S) support • HTTP proxy support • Password encryption for recipients without certificate • PIN caching* • API for integration in third-party applications** • Efail immunity
Scope of supply	• GreenShield add-in for Microsoft Outlook • GreenShield add-in for HCL Notes • GreenShield Core System • PKCS#11 module
Supported standards	• S/MIME Version 3.2 / 4 including ECC • OpenPGP • PKCS#11 • PKIX • CDSA security architecture • Randomness from card / TR2101-1 based PRNG / jitter-based RNG
Evaluation and approval	• Verschlusssache – Nur für den Dienstgebrauch (VS-NfD) • NATO Restricted • EU Restricted Approval number: BSI-VSA-10602, BSI-VSA-10632
Supported email clients	• Microsoft Outlook 2016 / 2019 / 365 • IBM Notes 9.0.x, HCL Notes 11

* Not permitted for VS-NfD, EU Restricted and NATO Restricted ** Extension

Technical Data Sheet - GreenShield Mail

Supported algorithms	Asymmetric crypto algorithms: • RSA (up to 16384 bit, up to PKCS1#v2 incl. PSS/OAEP) • DSA/DH (up to 2048 Bit) • ECC (up to 571 Bit): NIST and Brainpool curves Symmetric crypto algorithms: • DES (56 bit)* • Triple-DES (168 bit)* • RC2 (40 bit, 64 bit, 128 bit)* • AES (128 bit, 196 bit, 256 bit) Hash algorithms: • SHA-1**, SHA-224**, SHA-256, SHA-384, SHA-512 • RIPEMD-128, RIPEMD-140, RIPEMD-160* • MD2, MD4, MD5*
System requirements	Client operating system: • Microsoft Windows 10 (1809) • Microsoft Windows 11 Email server: • IBM Domino 8.5 or higher • Microsoft Exchange 2000 or higher
Usage requirements: VS-NfD, NATO Restricted EU Restricted	Smartcards: • Cryptovision ePasslet Suite v2.1 on NXP JCOP 2.4.2r3 • Cryptovision ePasslet Suite v3.0 on NXP JCOP 3 • Cryptovision ePasslet Suite v3.0 on G&D Sm@rtCafé Expert 7 (Veridos Suite v3.0) • CardOS V5.0 with QES V1.1 of Atos IT Solutions and Services GmbH • Elektronischer Dienst- und Truppenausweis, based on CardOS V5.0 (v4.2, v4.3, v4.4) • PKIBw-Card (PKI-Bw v1.7, v1.8, v1.9, tPKI-Bw v7.1), CardOS V5.0 based • CardOS V5.3 QES, V1.0 • CardOS DI V5.4 QES Version 1.0 • TCOS 3.0 – Signature Card Version 2.0 Release 2 • TCOS 4.0 – TeleSec IDKey with NetKey Plus PKI: • VS-NfD approval according to BSI-TR-03145 Certificates and revocation lists: • CRL or OCSP Middleware: • cryptovision SCinterface 8.0.x (PKCS#11 module)

* For decryption only, supported to ensure compatiblility with outdated algorithms

** Not permitted for VS-NfD, EU Restricted and NATO Restricted

SecurITy made in EU
Trust Seal www.teletrust.de/itsmie

Eviden Digital Identity
cv cryptovision GmbH
Munscheidstr. 14
D 45886 Gelsenkirchen

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

www.cryptovision.com