

Technical Data Sheet

cryptovision GreenShield Mail

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 HCL 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"> • S/MIME und OpenPGP-Unterstützung • Schlüsselnutzung von Smartcard / USB-Token / Softkey • Erzeugung von RSA- und EC- Schlüsseln • Generierung von Zertifikatsanträgen und selbstsignierten Zertifikaten • Key Escrow (Message Recovery) • X.509-Zertifikate, X.509-Sperrlisten • Mehrere Zertifizierungsstellen gleichzeitig nutzbar • Generierung von Schlüsselbunden und -Widerrufen • Zentrale Konfiguration und Verwaltung • LDAP- / OCSP- / HTTP(S)-Unterstützung • HTTP-Proxy-Unterstützung • Passwortverschlüsselung für Empfänger ohne Zertifikat • PIN-Caching • API zur Anbindung durch Drittanbieter* • Efail-Immunität
Lieferumfang	<ul style="list-style-type: none"> • GreenShield-Add-in für Microsoft Outlook • GreenShield Add-in für HCL Notes • GreenShield Core System • PKCS#11 Modul
Unterstützte Standards	<ul style="list-style-type: none"> • S/MIME Version 3.2 / 4 einschließlich ECC • OpenPGP • PKCS#11 • PKIX • CDSA Sicherheits-Architektur • PQC-Readiness durch Unterstützung von Kyber und Dilithium*
Barrierefreiheit	<ul style="list-style-type: none"> • Sehr gute Zugänglichkeit für Nutzer ohne Sehvermögen sowie für Nutzer mit motorischen oder auditiven Einschränkungen • Gute Zugänglichkeit für Nutzer mit eingeschränktem Sehvermögen
Unterstützte E-Mail-Clients	<ul style="list-style-type: none"> • Microsoft Outlook 2016 / 2019 / 2021 / 365 • HCL Notes 11/12

* Erweiterung

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• PQC-Preview: Dilithium und Kyber** <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*
Systemvoraussetzungen	<p>Client-Betriebssystem:</p> <ul style="list-style-type: none">• Microsoft Windows 10• Microsoft Windows 11 <p>E-Mail-Server:</p> <ul style="list-style-type: none">• HCL Domino 8.5 oder höher• Microsoft Exchange 2000 oder höher
Zulassung und Einsatzbedingungen: VS-NfD, NATO Restricted, EU Restricted	<p>Smartcards:</p> <ul style="list-style-type: none">• Cryptovision ePasslet Suite v3.0 auf NXP JCOP 3• Cryptovision ePasslet Suite v3.0 auf G&D Sm@rtCafé Expert 7 (Veridos Suite v3.0)• CardOS V5.0 mit QES V1.1• Elektronischer Dienst- und Truppenausweis, auf Basis von CardOS V5.0 (v4.2, v4.3, v4.4)• PKIBw-Card (PKI-Bw v1.7, v1.8, v1.9, tPKI-Bw v7.1), auf Basis von CardOS V5.0• CardOS V5.3 QES, V1.0• CardOS DI V5.4 QES Version 1.0• CardOS V6.0 DI (R1.0, R1.1)• TCOS 3.0 – Signature Card Version 2.0 Release 2• TCOS 4.0 – TeleSec IDKey mit NetKey Plus• Secunet SINA Workstation virtuelle SmartCard ab SINA OS 3.5.2.3 <p>PKI:</p> <ul style="list-style-type: none">• Freigabe nach BSI-TR-03145 für VS-NfD <p>Middleware:</p> <ul style="list-style-type: none">• cryptovision SCinterface 8.1.x (PKCS#11-Modul) <p>Zulassungs-IDs</p> <ul style="list-style-type: none">• BSI-VSA-10602, BSI-VSA-10632, BSI-VSA-10687

* Nur zum Entschlüsseln, um Kompatibilität mit veralteten Verfahren zu gewährleisten

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



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

T: +49 209 16724-50

F: +49 209 16724-61

www.cryptovision.com