



## Technical Data Sheet

# GreenShield Mail

11/2021

### 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.

<b>Functionality</b>	<p>Functions for protecting e-mails (end-to-end security):</p> <ul style="list-style-type: none"> <li>• Signing and verifying mails</li> <li>• Encryption and decryption of mails</li> <li>• Key- and certificate management</li> </ul>
<b>Features</b>	<ul style="list-style-type: none"> <li>• Key usage from smart card / USB token / softkey*</li> <li>• Generation of certification requests and self-signed certificates*</li> <li>• PIN caching**</li> <li>• Generation of RSA and EC keys*</li> <li>• Key escrow (message recovery)</li> <li>• Centralized configuration and management</li> <li>• Several certification authorities can be used in parallel</li> <li>• LDAP / OCSP / HTTP(S) support</li> <li>• HTTP proxy support</li> <li>• Verification of certificates</li> <li>• X.509 certificates and X.509 revocation lists</li> <li>• OpenPGP key rings and revocations*</li> <li>• Efail immunity</li> </ul>
<b>Scope of supply</b>	<ul style="list-style-type: none"> <li>• GreenShield add-in for Microsoft Outlook</li> <li>• GreenShield add-in for HCL Notes</li> <li>• GreenShield Core System</li> <li>• PKCS#11 module</li> </ul>
<b>Supported standards</b>	<ul style="list-style-type: none"> <li>• S/MIME Version 3.2 / 4 including ECC</li> <li>• OpenPGP*</li> <li>• PKCS#11</li> <li>• PKIX</li> <li>• CDSA security architecture</li> <li>• Randomness from smart card / TR2101-1 based pseudo random number generator / jitter-based mechanisms</li> <li>• LDAP / OCSP / HTTP(S)</li> </ul>
<b>Evaluation and approval</b>	<ul style="list-style-type: none"> <li>• Verschlusssache – Nur für den Dienstgebrauch (VS-NfD)</li> <li>• NATO Restricted</li> <li>• EU Restricted</li> </ul> <p>Approval number: BSI-VSA-10600</p>
<b>Supported email clients</b>	<ul style="list-style-type: none"> <li>• Microsoft Outlook 2016 / 2019 / 365</li> <li>• IBM Notes 9.0.x, HCL Notes 11</li> </ul>

\* In coordination with the BSI

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

## Technical Data Sheet - GreenShield Mail

<b>Supported algorithms</b>	<p>Asymmetric crypto algorithms:</p> <ul style="list-style-type: none"><li>• RSA (up to 16384 bit, up to PKCS1#v2 incl. PSS/OAEP)</li><li>• DSA/DH (up to 2048 Bit)</li><li>• ECC (up to 571 Bit): NIST and Brainpool curves</li></ul> <p>Symmetric crypto algorithms:</p> <ul style="list-style-type: none"><li>• DES (56 bit)*</li><li>• Triple-DES (168 bit)*</li><li>• RC2 (40 bit, 64 bit, 128 bit)*</li><li>• AES (128 bit, 196 bit, 256 bit)</li></ul> <p>Hash algorithms:</p> <ul style="list-style-type: none"><li>• SHA-1**, SHA-224**, SHA-256, SHA-384, SHA-512</li><li>• RIPEMD-128, RIPEMD-140, RIPEMD-160*</li><li>• MD2, MD4, MD5*</li></ul>
<b>System requirements</b>	<p>Client operating system:</p> <ul style="list-style-type: none"><li>• Microsoft Windows 10 (1809)</li></ul> <p>Email server:</p> <ul style="list-style-type: none"><li>• IBM Domino 8.5 or higher</li><li>• Microsoft Exchange 2000 or higher</li></ul>
<b>Usage requirements: VS-NfD, NATO Restricted EU Restricted</b>	<p>Smartcards:</p> <ul style="list-style-type: none"><li>• Cryptovision ePasslet Suite v2.1 on NXP JCOP 2.4.2r3</li><li>• Cryptovision ePasslet Suite v3.0 on NXP JCOP 3</li><li>• Cryptovision ePasslet Suite v3.0 on G&amp;D Sm@rtCafé Expert 7 (Veridos Suite v3.0)</li><li>• CardOS V5.0 with QES V1.1 of Atos IT Solutions and Services GmbH</li><li>• Elektronischer Dienst- und Truppenausweis, based on CardOS V5.0 (v4.2, v4.3)</li><li>• PKIBw-Card (PKI-BW v1.7, PKI-BW v1.8), based on CardOS V5.0</li><li>• CardOS V5.3 QES, V1.0</li><li>• CardOS DI V5.4 QES Version 1.0</li><li>• TCOS 3.0 – Signature Card Version 2.0 Release 2</li><li>• TCOS 4.0 – TeleSec IDKey with NetKey Plus</li></ul> <p>PKI:</p> <ul style="list-style-type: none"><li>• VS-NfD approval according to BSI-TR-03145</li></ul> <p>Certificates and revocation lists:</p> <ul style="list-style-type: none"><li>• CRL or OCSP</li></ul> <p>Middleware:</p> <ul style="list-style-type: none"><li>• cryptovision SCinterface 8.0.x (PKCS#11 module)</li></ul>

\* For decryption only, supported to ensure compatibility with outdated algorithms

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



cv cryptovision GmbH  
Munscheidstr. 14  
D-45886 Gelsenkirchen

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

[www.cryptovision.com](http://www.cryptovision.com)  
[info@cryptovision.com](mailto:info@cryptovision.com)