Technical Data Sheet (Fiche technique)

cryptovision GreenShield Mail

Cryptage d'e-mails avec homologation BSI pour VS-NfD, NATO RESTRICTED et RESTREINT UE

GreenShield Mail est une solution pour le cryptage et la signature des e-mails. En tant que module complémentaire (Add-in) pour Microsoft Outlook et IBM Notes, GreenShield Mail offre une sécurité de bout en bout.

Fonctions	Fonctions pour la protection des e-mails (avec sécurité de bout en bout) : • Signer et vérifier les e-mails • cryptage et décryptage des e-mails • Gestion des clés et des certificats
Caractéristiques	• Support S/MIME et OpenPGP • Utilisation de clés par carte à puce / clé USB / softkey • Génération de clés RSA et EC • Génération de demandes de certificats et de certificats auto-signés • Clé Ecrow (récupération de message) • Certificats X.509 et listes de révocation X.509 • Utilisation simultanée de plusieurs autorités de certification • Génération de trousseaux de clés et de révocations • Configuration et gestion centralisées • Prise en charge LDAP / OCSP / HTTP(S) • Prise en charge du proxy HTTP • Cryptage par mot de passe pour les destinataires sans certificat • Mise en cache du code PIN*. • API pour la connexion par des fournisseurs tiers** • Immunité Efail
Contenu de la livraison	• GreenShield Add-in pour Microsoft Outlook • GreenShield Add-in pour IBM Notes • Système GreenShield Core • Module PKCS#11

* Non autorisé pour VS-NfD, NATO RESTRICTED et RESTREINT UE ** Extension

Technical Data Sheet (Fiche technique) - GreenShield Mail

Normes soutenues	• S/MIME version 3.2 / 4 y compris ECC • OpenPGP • PKCS#11 • PKIX • Architecture de sécurité CDSA • Carte Aléatoire / PRNG inspiré de TR2102 / basé sur Jitter • LDAP / OCSP / HTTP(S)
Homologation	• Informations sécurisées - Réservé à l'usage officiel (VS-NfD) • NATO Restricted • EU Restricted Numéros d'agrément : BSI-VSA-10602, BSI-VSA-10632
E-Mail-Clients adaptés	• Microsoft Outlook 2016 / 2019 / 365 • IBM Notes 9.0.x, HCL Notes 11
Algorithmes adaptés	Algorithmes de cryptographie asymétrique : • RSA (jusqu'à 16384 bits, jusqu'à PKCS1#v2 y compris PSS/OAEP • DSA/DH (jusqu'à 2048 bits) • ECC (jusqu'à 521 bits) : courbes NIST et Brainpool Algorithmes de cryptographie symétrique : • DES (56 bits)* • Triple DES (168 bits)* • RC2 (40 bits, 64 bits, 128 bits)* • AES, AES-GCM (128 bits, 196 bits, 256 bits) Algorithmes de hachage : • SHA-1**, SHA-224**, SHA-256, SHA-384, SHA-512 • RIPEMD-128, RIPEMD-140, RIPEMD-160* • MD2, MD4, MD5*
Configuration requise	Système d'exploitation client : • Microsoft Windows 10 (1809) • Microsoft Windows 11 Serveur E-Mail • IBM Domino 8.5 ou supérieur • Microsoft Exchange 2000 ou supérieur

* Pour le décryptage uniquement, afin d'assurer la compatibilité avec les méthodes anciennes.
** Non autorisé pour VS-NfD, NATO RESTRICTED et RESTREINT UE

Technical Data Sheet (Fiche technique) - GreenShield Mail

Conditions d'usage : VS-NfD, NATO RESTRICTED RESTREINT UE	Cartes à puce : • Cryptovision ePasslet Suite v2.1 sur NXP JCOP 2.4.2r3 • Cryptovision ePasslet Suite v3.0 sur NXP JCOP 3 • Cryptovision ePasslet Suite v3.0 sur G&D Sm@rtCafé Expert 7 • (Veridos Suite v3.0) • CardOS V5.0 avec QES V1.1 d'Atos IT Solutions and Services GmbH • Carte de service et de troupe électronique, sur la base de CardOS • V5.0 (v4.2, v4.3, v4.4) • PKIBw-Card (PKI-Bw v1.7, v1.8, v1.9, tPKI-Bw v7.1), sur la base de • CardOS • V5.0 • 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 avec NetKey Plus PKI : • Validation selon BSI-TR-03145 pour VS-NfD Certificats et listes de révocation : • CRL ou OCSP Middleware : • cryptovision SCinterface 8.0.x (module PKCS#11)

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

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

www.cryptovision.com