Technical Data Sheet (Fiche technique)

# cryptovision GreenShield File

## Cryptage de fichiers avec homologation BSI pour VS-NfD, NATO RESTRICTED et RESTREINT UE

GreenShield File est une solution pour le cryptage et la signature de fichiers. Ainsi l'usage simplifié de GreenShield est lié à son intégration dans le système d'exploitation Microsoft Windows. Les fichiers cryptés peuvent notamment être envoyés par e-mail et sont reconnus comme des fichiers cryptés par les clients de messagerie courants.

| | |
|---|---|
| Fonctions | Fonctions pour la protection des fichiers :<br>• Signature et vérification des fichiers<br>• Cryptage et décryptage de fichiers<br>• Gestion des clés et des certificats |
| Caractéristiques | • Support S/MIME et OpenPGP<br>• Cryptage symétrique (mot de passe)<br>• Utilisation de clés par carte à puce / clé USB / clé logicielle<br>• Génération de clés RSA et EC<br>• Génération de demandes de certificats et de certificats auto-signés<br>• Génération de trousseaux de clés et de révocations<br>• Certificats X.509 et listes de révocation X.509<br>• Utilisation simultanée de plusieurs autorités de certification<br>• Prise en charge LDAP / OCSP / HTTP(S)<br>• Prise en charge du proxy HTTP<br>• Mise en cache des codes PIN<br>• Configuration et gestion centralisées<br>• Utilisation possible par interface graphique ou basée sur des scripts par ligne de commande<br>• API pour la connexion par des fournisseurs tiers* |
| Contenu de la livraison | • Extension GreenShield pour Windows Explorer et Ubuntu Nautilus<br>• Système GreenShield Core<br>• Module PKCS#11 |
| Normes soutenues | • S/MIME version 3.2 / 4 y compris ECC<br>• OpenPGP<br>• PKCS#11<br>• LDAP / OCSP / HTTP(S) |

* Extension

# Technical Data Sheet (Fiche technique) - GreenShield File

| | |
|---|---|
| Accessibilité | • Très bonne accessibilité pour les utilisateurs sans vision ainsi que pour les utilisateurs ayant des difficultés motrices ou auditives<br>• Bonne accessibilité pour les utilisateurs ayant une vision réduite |
| Systèmes d'exploitation adaptés | • Microsoft Windows 11<br>• Ubuntu Linux 20.04 LTS |
| Algorithmes adaptés | Algorithmes de cryptographie asymétrique :<br>• RSA (jusqu'à 16384 bits, jusqu'à PKCS1#v2 y compris PSS/OAEP)<br>• DSA/DH (jusqu'à 2048 bits)<br>• ECC (jusqu'à 521 bits) : courbes NIST et Brainpool<br>• PQC Preview: Dilithium et Kyber**<br>Algorithmes de cryptographie symétrique :<br>• DES (56 bits)*<br>• Triple DES (168 bits)*<br>• RC2 (40 bits, 64 bits, 128 bits)*<br>• AES, AES-GCM (128 bits, 196 bits, 256 bits)<br>Algorithmes de hachage :<br>• SHA-1**, SHA-224**, SHA-256, SHA-384, SHA-512<br>• RIPEMD-128, RIPEMD-160*<br>• MD2, MD4, MD5* |

* 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 File

| | |
|---|---|
| Homologation et conditions d'usage : VS-NfD, NATO RESTRICTED RESTREINT UE | Cartes à puce :<br>• Cryptovision ePasslet Suite v3.0 sur NXP JCOP 3<br>• Cryptovision ePasslet Suite v3.0 sur G&D Sm@rtCafé Expert 7 (VeridosSuite v3.0)<br>• CardOS V5.0 avec QES V1.1<br>• Carte électronique de service et de troupe, sur la base de CardOS<br>• V5.0 (v4.2, v4.3, v4.4)<br>• PKIBw-Card (PKI-Bw v1.7, v1.8, v1.9, tPKI-Bw v7.1), sur la base de<br>• CardOS<br>• V5.0<br>• CardOS V5.3 QES, V1.0<br>• CardOS V6.0 DI (R1.0, R1.1)<br>• CardOS DI V5.4 QES version 1.0<br>• TCOS 3.0 - Signature Card Version 2.0 Release 2<br>• TCOS 4.0 - TeleSec IDKey avec NetKey Plus<br>• Secunet SINA Workstation virtual SmartCard à partir de SINA OS 3.5.2.3<br><br>PKI :<br>• Validation selon BSI-TR-03145 pour VS-NfD<br><br>Middleware :<br>• cryptovision SCinterface 8.1.x (module PKCS#11)<br><br>Numéros d'homologation:<br>• BSI-VSA-10876, BSI-VSA-10912 |

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