

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 : <ul style="list-style-type: none"> • Signature et vérification des fichiers • Cryptage et décryptage de fichiers • Gestion des clés et des certificats
Caractéristiques	<ul style="list-style-type: none"> • Support S/MIME et OpenPGP • Cryptage symétrique (mot de passe) • Utilisation de clés par carte à puce / clé USB / clé logicielle • Génération de clés RSA et EC • Génération de demandes de certificats et de certificats auto-signés • Génération de trousseaux de clés et de révocations • Certificats X.509 et listes de révocation X.509 • Utilisation simultanée de plusieurs autorités de certification • Prise en charge LDAP / OCSP / HTTP(S) • Prise en charge du proxy HTTP • Mise en cache des codes PIN • Configuration et gestion centralisées • Utilisation possible par interface graphique ou basée sur des scripts par ligne de commande • API pour la connexion par des fournisseurs tiers*
Contenu de la livraison	<ul style="list-style-type: none"> • Extension GreenShield pour Windows Explorer et Ubuntu Nautilus • Système GreenShield Core • Module PKCS#11
Normes soutenues	<ul style="list-style-type: none"> • S/MIME version 3.2 / 4 y compris ECC • OpenPGP • PKCS#11 • LDAP / OCSP / HTTP(S)

* Extension

Technical Data Sheet (Fiche technique) - GreenShield File

Accessibilité	<ul style="list-style-type: none">• Très bonne accessibilité pour les utilisateurs sans vision ainsi que pour les utilisateurs ayant des difficultés motrices ou auditives• Bonne accessibilité pour les utilisateurs ayant une vision réduite
Systemes d'exploitation adaptés	<ul style="list-style-type: none">• Microsoft Windows 10• Microsoft Windows 11• Ubuntu Linux 20.04 LTS
Algorithmes adaptés	<p>Algorithmes de cryptographie asymétrique :</p> <ul style="list-style-type: none">• 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• PQC Preview: Dilithium et Kyber** <p>Algorithmes de cryptographie symétrique :</p> <ul style="list-style-type: none">• DES (56 bits)*• Triple DES (168 bits)*• RC2 (40 bits, 64 bits, 128 bits)*• AES, AES-GCM (128 bits, 196 bits, 256 bits) <p>Algorithmes de hachage :</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*

* 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 :

- Cryptovision ePasslet Suite v3.0 sur NXP JCOP 3
- Cryptovision ePasslet Suite v3.0 sur G&D Sm@rtCafé Expert 7 (VeridosSuite v3.0)
- CardOS V5.0 avec QES V1.1
- Carte électronique de service et de troupe, 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 V6.0 DI (R1.0, R1.1)
- 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
- Secunet SINA Workstation virtual SmartCard à partir de SINA OS 3.5.2.3

PKI :

- Validation selon BSI-TR-03145 pour VS-NfD

Middleware :

- cryptovision SCinterface 8.1.x (module PKCS#11)

Numéros d'homologation:

- BSI-VSA-10602, BSI-VSA-10632, BSI-VSA-10687

Secur|Ty
made
in
EU
Trust Seal
www.teletrust.de/itsme

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

T: +49 209 16724-50

F: +49 209 16724-61

www.cryptovision.com