DRIVELOCK SMART DISKENCRYPT 10

- Weiterentwicklung von SafeGuard Device Encryption unter Windows 10 64-bit UEFI für Behörden.
- VS-NfD-Zulassung in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) in Arbeit.
- Administrationskonzept mittels des von SafeGuard Enterprise bekannten Management Centers und von Client Configuration MSI-Dateien.
- Unterstützung BSI-zertifizierter Smart Cards in der PBA
- XTS-AES 256 Bit als Algorithmus zur Festplattenchiffrierung
- Via Policy wählbare schnelle oder vollständige Initialchiffrierung

DRIVELOCK SMART DISKENCRYPT 10

Die DriveLock SE aus München entwickelt das Produkt SafeGuard Device Encryption / Easy auf der aktuellen Windows Betriebssystemplattform Windows 10, 64-bit UEFI, weiter.

ZUGELASSENE VERSION FÜR VS-NFD

Für deutsche Behördenkunden und die geheimschutzbetreute Industrie wird das Produkt gemäß den Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entworfen und entwickelt, so dass eine neue VS-NfD-Zulassung für die Festplattenverschlüsselung unter Windows 10 erteilt wird.

Für das neue Produkt ist bereits unter dem Namen „DriveLock Smart Disk Encrypt“ und „Utimaco DiskEncrypt“ beim BSI die Zulassung beantragt und die Zulassungsarbeiten sind bereits in Umsetzung.

Die technischen Randbedingungen für die VS-NfD-Zulassung fordern, dass die Authentisierung in der UEFI-basierenden Pre-Boot Authentication (PBA) inkl. UEFI Secure Boot ausschließlich mittels einer kryptographischen Smart Card erfolgen darf, die ebenfalls zertifiziert, bzw. vom BSI freigeben, ist.

Die Administrationskonzepte des Produktes bleibt unverändert.

Für die VS-NfD-Version erfolgt sie, wie bei SafeGuard Device Encryption 5.60.3 VS-NfD, über das auf dem SafeGuard Enterprise Management Center basierende DriveLock Management Center und mittels der von SafeGuard bekannten Client Configuration MSI Dateien.

Im Detail heißt das für die VS-NfD-Version:

Auf dem Client:

- Stand-alone Modus
- Verschlüsselungsalgorithmus: XTS-AES-256
- Möglichkeit, Crypto-Token Benutzer in der PBA auf dem jeweiligen Client-Rechner lokal zu administrieren.
- Es ist nicht möglich, den letzten PBA-Benutzer zu löschen.
- Initialchiffrierung:
  - Vollständige Partitionschiffrierung
  - Fast Initial Encryption
- Vom BSI für VS-NfD zugelassener Zufallszahlengenerator.
- In der PBA sind nur Benutzer mit Crypto-Smart Card (BSI-Vorgabe und BSI-zertifiziert) erlaubt
- Service Account Listen und PBA-Benutzer

Das zentrale administrative Backend:

- DriveLock Smart DiskEncrypt Management Center
- DriveLock Smart DiskEncrypt Server
- DriveLock Smart DiskEncrypt Datenbank Server
- Die Kommunikation zwischen dem Management Center und einem Smart DiskEncrypt Client erfolgt ausschließlich offline via Client Configuration Files (MSI-Format).
- Die administrativen Aktionen der diversen Security Officers im Smart DiskEncrypt Management Center werden geloggt und in der zentralen Smart DiskEncrypt Datenbank hinterlegt.

DriveLock Smart DiskEncrypt wird sowohl den jeweiligen Windows 10 Semi-Annual Channel (1607, 1703, 1709, 1803, etc.) wie auch den integrierten Microsoft In-Place Upgrade Mechanismus unterstützen, so dass es möglich ist, trotz Smart DiskEncrypt-verschlüsselter Windows System-Partitionen von einer Windows 10 Semi-Annual Channel (SAC) Version auf eine Nachfolgeversion upzugraden.