

MS Bitlocker mit CryptoPro Secure Disc – das Fort Knox für ihre Daten

1. Standard-Konfiguration mit Windows Vista/7- Bitlocker ohne PreBoot-Authentisierung PBA

BIOS/Boot
 BitLocker-
 Verschlüsselung

Windows-Login

Nachteile:
 - TPM-Modul nicht in allen PCs/Notebooks verfügbar.
 - Windows-Admin-Passwort kann per DMA-Hack gelöscht werden.

2. Standard-Konfiguration mit Windows Vista/7- Bitlocker ohne TPM/mit USB mit PBA

BIOS/Boot
 BitLocker-
 Verschlüsselung
 Recovery Key auf USB-Stick

Windows-Login

Nachteile:
 - USB-Stick ist zum Start immer erforderlich.
 - 32stelliger Recovery Key muss bei Verlust des USB-Sticks manuell eingetragen werden.
 - Recovery Key wird unverschlüsselt auf USB-Stick gespeichert.
 - Bei Verlust/Diebstahl des USB-Sticks sind die Daten verfügbar.
 - PBA ohne Passwort-Regelung gemäß Microsoft Credentials
 - Doppeltes Login (PBA und Windows)
 - Kein Fingerprint/Smartcard für PBA möglich

3. Windows Vista/7- Bitlocker ohne TPM/mit Crypto Secure for Bitlocker

BIOS/Boot
 BitLocker-Verschlüsselung
 CryptoSecure mit PBA
 (User/Passwort /
 Fingerprint / Smartcard)

Windows-Login
 Automatisches
 SignalSignOn durch
 CryptoSecure

Vorteile:
Anmeldung / Sicherheit:
 - Online PBA mit SignalSignON – nur eine Anmeldung
 - Passwort-Regelung gemäß Microsoft Credentials
 - Höchste Sicherheit auch ohne TPM

Recovery Keys:
 - Speicherung der verschlüsselten Recovery Keys in CryptoSecure-Datenbank (lokal oder auf DB-Server-MS SQL-Server/mysql/QOracle)

Einfache und kostenreduzierende Verwaltung:
 - Zentrale Administration
 - ActiveDirectory-Anbindung
 - Gemeinsame/einheitliche Verwaltung mit Windows XP-Systemen mit CryptoSecure-Verschlüsselung.

Help-Desk:
 - Sofort-Hilfe für vergessene Passworte oder blockierte Smartcard