Rohde & Schwarz Cybersecurity

R&S®TRUSTED DISK

VS-NfD,
EU RESTRICTED,
NATO RESTRICTED

BSI-zugelassene Festplattenverschlüsselung zum Schutz von Verschlusssachen der Geheimhaltungsstufe „Nur für den Dienstgebrauch“

Die elektronische Verarbeitung von Verschlusssachen unterliegt strengen gesetzlichen Vorgaben. Die sensiblen Daten müssen vor unbefugtem Zugriff geschützt werden, wobei ausschließlich vom BSI zertifizierte IT-Sicherheitsprodukte mit einer speziellen Zulassung verwendet werden dürfen.

Die Festplatten- und Datenträgerverschlüsselung R&S®Trusted Disk ist ein solches Sicherheitsprodukt mit Zulassung für Verschlusssachen der Geheimhaltungsstufe „Nur für den Dienstgebrauch“, EU Restricted und NATO Restricted. Sie schützt Verschlusssachen auf ausgeschalteten Computern vor nicht autorisiertem Zugriff, bei Verlust oder Diebstahl sowie Wartung und Reparatur des Geräts. Unterstützt werden Endgeräte mit Windows-Betriebssystem, welche bei Bedarf auch durch mehrere Anwender genutzt werden können:

- Notebooks, Tablets und Desktop-PCs
- in Polizei- und Militärfahrzeugen verbaute PCs
- daran angeschlossene externe USB-Datenträger
- Windows-Server

Produkt-Flyer
Version 07.00

ROHDE&SCHWARZ
Make ideas real

Sichere Verschlüsselung

R&S®Trusted Disk kann den Systemdatenträger und bis zu sieben weitere interne Datenträger eines Endgeräts sowie bei Bedarf auch externe USB-Datenträger verschlüsseln. Nach einer bestimmten Zeit oder geschriebenen Datenmenge oder alternativ bei sicherheitsrelevanten Ereignissen, wie z.B. dem Entfernen der Berechtigung eines Benutzers, der Aktualisierung des Smartcard-Schlüssels oder der Beendigung des Wartungsmodus, werden interne Datenträger automatisch umgeschlüsselt. Für externe Datenträger werden Umschlüsselungen entweder manuell oder nach Aufforderung gestartet.
Der Boot-Prozess ist durch Nutzung von Secure Boot manipulationssicher. Dafür kann entweder ein von Microsoft signierter Shim-Bootloader oder, für besondere Sicherheitsanforderungen, ein von Rohde & Schwarz Cybersecurity selbst mit einer eigenen Secure-Boot-PKI signierter Bootloader verwendet werden. Die obligatorische Zwei-Faktor-Pre-Boot-Authentifizierung erfordert eine nutzerspezifische Smartcard und die Eingabe einer PIN. Für den Entsperrbildschirm sind dabei Funktionsumfang und Hintergrundbild anpassbar. Eine Bildschirmtastatur ermöglicht die Eingabe der PIN über Maus oder Touch-Displays. Anwender können bei Bedarf ihre persönliche PIN ändern oder zurücksetzen. Eine PIN-Richtlinie ist durchsetzbar. Falls gewünscht, kann ein spezieller Stealth-Modus durch Booten eines parallelen Systems ohne sensible Daten verschleiern, dass überhaupt Verschlüsselung eingesetzt wird.
Sicherheitsrelevante Ereignisse können jederzeit über ein Audit-Log nachvollzogen werden.

Einfache Administration

R&S®Trusted Disk lässt sich einfach auf eine große Anzahl passend konfigurierter Endgeräte ausrollen. Dabei ist die Initialisierung der Verschlüsselung über ein Kommandozeilen-Tool automatisierbar. Die Produktivität der Anwender wird dabei nicht beeinträchtigt, da sowohl die initiale Verschlüsselung als auch spätere Umschlüsselungen im Hintergrund erfolgen und ein spezieller Wartungsmodus unbeaufsichtigte Neustarts ohne Nutzerinteraktion ermöglicht.
Ohne Managementsystem müssen sowohl das Management als auch die Personalisierung der Smartcards mit dem R&S®Trusted Identity Manager Standalone durch einen Administrator auf einem separaten Endgerät erfolgen.

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig

Mit Managementsystem erfolgt das Smartcard-Management über dieses. Die Personalisierung mit dem R&S®Trusted Identity Manager kann dabei wahlweise entweder nur durch einen Administrator oder die Anwender selbst durchgeführt werden. Alternativ können Management und die Personalisierung der Smartcards in einem externen Smartcard-Management erfolgen, welches kompatible Profile verwenden muss.
Bei Verlust von Anwender-Smartcards können Sicherheitsadministratoren weiterhin auf die verschlüsselten Daten zugreifen. Datenrettungsszenarien werden durch ein im Lieferumfang befindliches Recovery Tool unterstützt.

Zentrales Management

Die Verwendung des zentralen Managementsystems R&S®Trusted Objects Manager vereinfacht die Administration erheblich. Es ermöglicht die unternehmensgerechte Fernverwaltung von Endgeräten, Benutzern, Smartcards, Gruppen und Rechten. Eine Anbindung an LDAP-Verzeichnisdienste, z.B. Active Directory, ist möglich. Benötigte Geräte- und Benutzer-Zertifikate für die Personalisierung von Smartcards können mittels einer integrierten PKI erzeugt und über ihren gesamten Lifecycle einfach verwaltet werden. Sicherheitsrichtlinien sind zentral durchsetzbar. Ein manipulationssicheres Audit-Protokoll des Managementsystem und aller verwalteten Endgeräte mit möglicher Syslog-Anbindung, SNMP und SMTP ermöglichen eine effektive Betriebsüberwachung.

Alleinstellungsmerkmale

- Einzige VS-NfD-konforme Lösung mit einem zentralen netzwerkbasierten Management
- Breite Hardware-Unterstützung
- Vollständig in Deutschland entwickelt mit schnellem und zuverlässigem Hersteller-Support aus Deutschland
- Kein bekannter Sicherheitsvorfall seit Produkt-Launch vor 12 Jahren
- Im BSI-Programm beschleunigter Sicherheitszertifizierungen

Hinweis für Behördenkunden

Es besteht die Bezugsmöglichkeit aus dem Rahmenvertrag 21907 des Beschaffungsamtes des Bundesministeriums des Inneren.

Kaufhaus des Bundes

Rohde & Schwarz Cybersecurity GmbH
Mühldorfstraße 15 | 81671 München
Info: +49 30 65884-222
E-Mail: cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity

Rohde & Schwarz GmbH & Co. KG
www.rohde-schwarz.com

PD 3607.5831.31 | Version 07.00 | Oktober 2024 (dh)
R&S®Trusted Disk