R&S®TRUSTED DISK

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

VS-NfD,
EU RESTRICTED,
NATO RESTRICTED

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

R&S®TRUSTED DISK

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. 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.

R&S®TRUSTED DISK

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 Sicherheitszertifi zierungen

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

Hinweis für Behördenkunden

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

Kaufhaus des Bundes

R&S®TRUSTED DISK

Datenverschlüsselung	
Interne Datenträger	► Ein interner physischer oder mehrere interne physische Datenträger ► Max. Größe physischer und logischer Datenträger: jeweils 20 TB ► Maximal 8 interne logische Datenträger
Externe Datenträger	USB, max. Größe: 2 TB
Logische Sektorgröße	► Nur 512 Bytes unterstützt: 512n/512-Byte Native oder Advanced Format mit 512e/512-Byte-Emulation ► Nicht unterstützt: 4Kn/4K Native oder andere Formate, die auch Windows standardmäßig nicht unterstützt
Partitionslayout	Alle zu verschlüsselnden Partitionen müssen in einem einzigen, zusammenhängenden Bereich angeordnet sein.
Sektorbasierte Verschlüsselung	AES-XTS-512
Sicherheit	
Boot-Prozess	► Manipulationssicher durch Nutzung von UEFI Secure Boot ► Bootloader-Varianten: – Von Microsoft signierter Shim-Bootloader – Von Rohde & Schwarz Cybersecurity selbst mit einer eigenen Secure-Boot-PKI signierter RSCS-Bootloader für besondere Sicherheitsanforderungen
Authentifizierung	► Pre-Boot-Authentifizierung (PBA): 2FA mittels Smartcard und PIN ► PIN-Richtlinie vorgebbar
Asymmetrische Verschlüsselung	► RSA mit 2048-Bit-, 3072-Bit- oder 4096-Bit-Schlüssellänge ► Öffentliche Schlüssel in X.509-Zertifikaten eingebettet
Sichere Zufallszahlengenerierung	► Smartcard-Seeding: Smartcard als sichere Zufallszahlenquelle ► Hash-DRBG und HMAC-DRBG
Kommunikation mit Smartcard-Reader	Abgesichert mittels Blinding
Krypto-Algorithmen	Vom BSI freigegebene Botan-Krypto-Bibliothek
Kommunikation zwischen Endgerät und Managementsystem	Über TLS-gesicherten Kommunikationskanal
Daten-Umschlüsselung	► Auslöser: – Nach 4 Jahren oder wenn 5 TB Daten geschrieben wurden – Bei sicherheitsrelevanten Ereignissen, z.B. Entfernen einer Berechtigung ► Für interne Datenträger: automatisch ► Für externe Datenträger: beim Einbinden nach Nutzerbestätigung
Datenlöschung auf ext. Datenträgern	Löschung der kryptografischen Schlüssel mit Gutmann-Methode
Ereignisprotokoll Audit-Log	Protokollierung sicherheitsrelevanter Ereignisse
Optionaler Stealth-Modus	Verschleiert, dass Verschlüsselung überhaupt eingesetzt wird
Unterstützte Endgeräte	
Systemanforderungen	► Firmware basierend auf UEFI-Spezifikation ab Version 2.3.1/Errata C von Juni 2012 ► Hardware entsprechend Microsoft-Mindestanforderungen für Windows 10 und 11 ► Davon abweichend: – Nur x86-64-Prozessor – In der Regel mindestens 16 GB Arbeitsspeicher. Je nach eingesetzter Software kann mehr Arbeitsspeicher nötig werden. – Bildschirmauflösung für PBA-Bildschirm ≥ 1024 × 768 (XGA) ► Datenträger: – GPT-formatiert – Windows- und EFI-Systempartition (ESP) auf demselben Datenträger – ESP-Größe ≥ 200 MB, dauerhaft freier Speicherplatz ≥ 50 MB
Kompatibilität	Erfahrungsgemäß besteht eine hohe Kompatibilität insbesondere mit gängigen Business-Modellen von Dell, HP und Lenovo. Aufgrund der häufigen Modellwechsel, der Vielzahl möglicher Modellkonfigurationen, unterschiedlicher Firmware-Varianten und -Stände sowie interner und externer Hardwarekomponenten kann jedoch keine pauschale Gewähr für die Kompatibilität gegeben werden. Daher wird eine initiale Bewertung empfohlen.
Gerätespezifischer 3rd-Level-Support	Bis zum EOS (offiziellen Support-Ende) des jeweiligen Geräteherstellers, maximal aber 5 Jahre nach Verkaufsstart
Betriebssystemunterstützung	
Windows 10 und 11	► 64-Bit-Versionen der Pro- und Enterprise-Editionen ► Ziel ist die Unterstützung aller regulären Versionen (Funktionsupdates) mit allen jeweils aktuell verfügbaren wichtigen Updates und Sicherheitsupdates bis zum Support-Ende ► LTS- und andere Editionen auf Anfrage/projektspezifisch
Windows-Server	Auf Anfrage/projektspezifisch: Windows Server 2016, 2019 und 2022

R&S®TRUSTED DISK

Lokalisierung	
PBA	► Bedienoberfläche: Deutsch, Englisch ► Tastatur-Layouts: Englisch (en_US), Deutsch (de_DE) und Französisch (fr_FR)
Windows-Applikation	Bedienoberfläche: Deutsch, Englisch
Smartcards	
Unterstützte Typen und Versionen	► CardOS-Smartcards: Versionen 5.0, 5.3, 5.3 DI ► Weitere auf Anfrage/projektspezifisch
Personalisierung und Management	► Variante mit zentralem Managementsystem: Mittels zentralem R&S®Trusted Objects Manager und lokalem R&S®Trusted Identity Manager kann die Personalisierung bei bestehender Netzwerkverbindung wahlweise entweder zentral durch einen Administrator oder die Anwender selbst durchgeführt werden ► Standalone-Variante ohne zentrales Managementsystem: Einzelplatzlösung R&S®Trusted Identity Manager Standalone für Administratoren mit eingeschränktem Funktionsumfang ► Externes Smartcard-Management, das kompatible Smartcard-Profile verwendet
PKCS#11-Smartcard-Middleware	► CardOS API ► Nexus Personal: Auf Anfrage/projektspezifisch
Smartcard-Reader	
Standards	► ISO/IEC 7816 ► PC/SC 2.x ► CCID 1.1
PIN-Eingabe	► Über separate Tastatur oder Bildschirmtastatur ► Eingabe an speziellen Smartcard-Reader-Tastaturen wird nicht unterstützt
Smartcard-Zugriff	Nur zulässig im direkten Kontakt (kontaktbehaftet)
Kompatibilität	Regulär getestet werden nur die im Abschnitt „Bestellinformationen“ gelisteten Typen von externen USB-Smartcard-Readern. Erfahrungsgemäß besteht eine hohe Kompatibilität zu vielen weiteren internen und externen Smartcard-Readern. Da wir jedoch keine pauschale Gewähr für die Kompatibilität geben können, ist eine initiale Bewertung der Eignung erforderlich. Auftretende Inkompatibilitäten resultieren fast immer aus nicht-standardkonformem Verhalten von Hardware oder Firmware von Smartcard-Readern. Eine Lösung erfordert in der Regel immer Anpassungen durch den Hardware-Hersteller. Unterstützt werden mit hoher Wahrscheinlichkeit Smartcard-Reader, die hier ohne Einschränkungen (insbesondere mit Blick auf die Extended APDU) gelistet sind: Supported CCID readers/ICCD tokens (apdu.fr) Beim Recovery-Tool besteht dagegen eine geringere Kompatibilität zu internen und externen Smartcard-Readern anderer Hersteller. Die Verwendung eines der im Abschnitt „Bestellinformationen“ gelisteten Typen von externen USB-Smartcard-Readern wird empfohlen.
Mehrbenutzerfähigkeit	
Anzahl von Berechtigungen	Bis zu 15.000 Berechtigungen pro Datenträger
Zentrales Management	
R&S®Trusted Objects Manager	Server/Netzwerkgerät: siehe separates Datenblatt
Anzahl verwaltbarer Nutzer/Endgeräte	Bis zu 50.000, abhängig insbesondere von der Anzahl der Zertifikate pro Nutzer; darüber hinaus projektspezifisch
BSI-Zulassung	
BSI-VSA-10580	► Nur für den Dienstgebrauch (VS-NfD) ► EU Restricted (EU-R) für den nationalen Einsatz ► NATO Restricted (NR)
Lieferumfang	
SW-Komponenten für Microsoft Windows	► Trusted Disk ► Trusted Disk Recovery ► Bei zentralem Managementsystem: – Trusted Workstation Agent – Trusted Identity Manager ► Ohne zentrales Managementsystem, optional: – Trusted Identity Manager Standalone ► MS Visual Studio Redistributable(s) ► CardOS API
Dokumentation	► Release Notes, Englisch ► Benutzerhandbücher, Deutsch und Englisch ► Administratorhandbücher, Deutsch und Englisch ► Trusted Identity Manager Standalone: Dokumentation nur Englisch
Bereitstellung	Erfolgt ausschließlich elektronisch

R&S®TRUSTED DISK

Variante	Lizenz / Typ	Lizenzmodell / Laufzeit	Bestellnummern (ehemals R&S Cybersecurity, SLA Priority)	Artikelnummern (gültig ab 01.09.2026)
Lizenzen, Wartung und 3rd-Level-Support				
Mit zentralem Management	VS-NfD/EU-R/NR	Subscription 1 J./3 J./variabel	3648.3133.12/36/37	40161/40162/40163
	Andere, exportfähig	Subscription 1 J./3 J./variabel	3648.7468.12/36/37	40168/40169/40170
Ohne zentrales Management	VS-NfD/EU-R/NR	Subscription 1 J./3 J./variabel	3641.3873.12/36/37	40148/40149/40150
	Andere, exportfähig	Subscription 1 J./3 J./variabel	3641.1058.12/36/37	40141/40142/40143
	R&S®Trusted Identity Manager Standalone	Subscription 1 J./3 J./variabel	4609.0010.12/36/37	40171/40172/40173
Zusätzl. Smartcards, wenn Anzahl Smartcards > Clients	Trusted Identity Manager Basic	Subscription 1 J./3 J./variabel	4619.9340.12/36/37	40184/40185/40186
Managementsystem				
R&S®Trusted Objects Manager	HW-Appliance	TOM-S Gen. 2 TOM-M Gen. 2	4619.8343.02 4619.8350.04	folgt 40425
	HW-Wartung	1 J./3 J./variabel	3648.4830.12/36/37	40412/40413/40414
Erweiterungslizenzen	Mandantenfähigkeit	Subscription 1 J./3 J./variabel	3645.5112.12/36/37	40431/40432/40433
	Genua-Unterstützung I: Client-Zertifikate und CSR-Support	Subscription 1 J./3 J./variabel	3741.2855.12/36/37	40077/40078/40079
	Genua II: Konfiguration + Management von Genuscreen SRA-Gateways & Genuconnect Clients	Subscription 1 J./3 J./variabel	3748.2844.12/36/37	40050/40051/40052
Optionale Unterstützung weiterer Zertifikate auf gleicher Smartcard	OpenPGP/GnuPG VS-Desktop	Subscription 1 J./3 J./variabel	3739.0271.12/36/37	40073/40074/40075
	Document Signing	Subscription 1 J./3 J./variabel	3746.2201.12/36/37	40090/40091/40092
	S/MIME	Subscription 1 J./3 J./variabel	3744.2785.12/36/37	40082/40083/40084
	Windows-Anmeldung	Subscription 1 J./3 J./variabel	3747.2840.12/36/37	40093/40094/40095
Smartcards				
CardOS 5.3	Volle Größe	Smartcard, nicht personalisiert	4619.9162.22	40127
	SIM-Größe	Smartcard, nicht personalisiert	619.9162.21	40130
Smartcard-Reader				
Volle Größe	USB-A	USB-Gerät IDBridge CT30	4619.8937.02	40129
	Optionaler Standfuß	Für USB-Gerät IDBridge CT30	4619.8850.02	40128
SIM-Größe	USB-A	USB-Token ACR39T-A1, RS-Branding	3697.5871.04	40133
	USB-C	USB-Token ACR39T-A5, RS-Branding	3697.5871.05	40134
Dienstleistungen				
Service vor Ort	Tagessatz technischer Experte	Exklusive Reisekosten	3666.9000.51	40122
Reisekosten	Pauschaler Tagessatz	Innerhalb Deutschlands	5413.9920.15	folgt

Rohde & Schwarz Networks and Cybersecurity GmbH
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info.rs-nc@rohde-schwarz.com | www.rohde-schwarz.com/networks-and-cybersecurity

ROHDE&SCHWARZ
Make ideas real