R&S®TRUSTED DISK

Spezifikationen

Release 3.7.2

Datenverschlüsselung

Interne Datenträger	• Ein 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 werden 4Kn/4K Native oder andere Formate, die auch von Windows standardmäßig nicht unterstützt werden
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 ≥ 1024x768 (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

Hinweis für IT-Administratoren: Die Festplattenverschlüsselung ist eine kritische Systemkomponente. Daher sollten Endgeräte mit R&S®Trusted Disk Teil der Testumgebung sein, in der alle Windows-Updates vor deren organisationsweitem Roll-out getestet werden.

Lokalisierung

PBA	Bedienoberfläche: Deutsch, Englisch
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 an beliebigen Endgeräten, wobei Benutzer ihre Smartcards selbst aktualisieren können • Standalone-Variante ohne zentrales Managementsystem: Einzelplatzlösung R&S®Trusted Identity Manager Standalone für Administratoren • 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 mit passendem Linux-Treiber, die hier ohne Einschränkungen (insbesondere mit Blick auf die Extended APDU) gelistet sind: Supported CCID readers/ICCD tokens (apdu.fr)

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 100.000, abhängig insbesondere von der Anzahl der Zertifikate pro Nutzer

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
Bereitstellung	Erfolgt ausschließlich elektronisch

Bestellinformationen

Lizenzen, Wartung und 3rd-Level Support

Variante	Lizenz	Lizenzmodell, Laufzeit	Bestellnr. (SLA Class./Prio.)
Ohne zentrales Management	VS-NfD/EU-R/NR	Subscription 1 Jahr	3641.1735.12 / 3641.3873.12
		Subscription 3 Jahre	3641.1735.36 / 3641.3873.36
		Subscription variabel	3641.1735.37 / 3641.3873.37
		Perpetual	3641.3873.02
	Exportfähig	Subscription 1 Jahr	3641.0616.12 / 3641.1058.12
		Subscription 3 Jahre	3641.0616.36 / 3641.1058.36
		Subscription variabel	3641.0616.37 / 3641.1058.37
		Perpetual	3641.1058.02
	R&S®Trusted Identity Manager Standalone	Subscription 1 Jahr	4609.0062.12 / 4609.0010.12
		Subscription 3 Jahre	4609.0062.36 / 4609.0010.36
		Subscription variabel	4609.0062.37 / 4609.0010.37
		Perpetual	4619.9204.02
	Option Trusted Identity Manager Basic: Zusätzliche Smartcard, wenn Anzahl Smartcards > Clients	Subscription 1 Jahr	Auf Anfrage
		Subscription 3 Jahre	Auf Anfrage / 4619.9340.36
		Subscription variabel	Auf Anfrage
		Perpetual	4619.9340.02
	Option Trusted Identity Manager Extended: Verwendung kunden-spezifischer Zertifikate auf gleicher Smartcard, pro Zertifikat/Smartcard	Subscription 1 Jahr	3663.3401.12 / 3663.3218.12
		Subscription 3 Jahre	3663.3401.36 / 3663.3218.36
		Subscription variabel	3663.3401.37 / 3663.3218.37
		Perpetual	3663.3218.02
Mit zentralem Management	VS-NfD/EU-R/NR	Subscription 1 Jahr	3648.3110.12 / 3648.3133.12
		Subscription 3 Jahre	3648.3110.36 / 3648.3133.36
		Subscription variabel	3648.3110.37 / 3648.3133.37
		Perpetual	3648.3133.02
	Exportfähig	Subscription 1 Jahr	3648.6690.12 / 3648.7468.12
		Subscription 3 Jahre	3648.6690.36 / 3648.7468.36
		Subscription variabel	3648.6690.37 / 3648.7468.37
		Perpetual	3648.7468.02
Unabhängig vom Management	Perpetual	Wartung & Support 1 Jahr	3648.5188.12 / 3648.5171.12
		Wartung & Support 3 Jahre	3648.5188.36 / 3648.5171.36
		Wartung & Support variabel	3648.5188.37 / 3648.5171.37

Managementsystem

Für Varianten und Materialnummern von R&S®Trusted Objects Manager siehe separates Datenblatt.

Smartcards

CardOS 5.3	Volle Größe	Smartcard, nicht personalisiert	4619.9162.22
	SIM-Größe	Smartcard, nicht personalisiert	4619.9162.21

Smartcard-Reader

Volle Größe	USB-A	USB-Gerät IDBridge CT30	4619.8937.02
	Optionaler Standfuß	Für USB-Gerät IDBridge CT30	4619.8850.02
SIM-Größe	USB-A	USB-Token ACR39T-A1, RS-Branding	3697.5871.04
	USB-C	USB-Token ACR39T-A5, RS-Branding	3697.5871.05

Dienstleistungen

Service vor Ort	Tagessatz technischer Experte	Reisekosten innerhalb DE inkl.	3664.6333.02

Rohde & Schwarz Cybersecurity GmbH
Mühldorfstraße 15, 81671 München
www.rohde-schwarz.com/cybersecurity
cybersecurity@rohde-schwarz.commailto:

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

PD 3607.5831.21 | Version 03.00 | August 2024 (wm)
R&S®Trusted Disk