R&S®TRUSTED DISK

Hard disk encryption to protect classified information approved by the German Federal Office for Information Security

VS-NfD,
EU RESTRICTED,
NATO RESTRICTED

The electronic processing of classified information is subject to strict legal requirements. The sensitive data must be protected from unauthorized access, and only certified IT security products with a special approval may be used.

The R&S®Trusted Disk hard disk and mobile data storage device encryption is one such security product with approval for classified information at the „Nur für den Dienstgebrauch“ and EU Restricted and NATO Restricted levels. It protects classified information on turned off computers against unauthorized access, loss or theft, and maintenance and repair of the device. End devices with Windows operating systems are supported, which can be used also by multiple users if required:

- Notebooks, tablets and desktop PCs
- PCs installed in police and military vehicles
- External USB data storage devices connected to them
- Windows servers

R&S®TRUSTED DISK

Secure encryption

R&S®Trusted Disk can encrypt the internal system data medium and up to seven other internal data media of an end device and, if required, external USB data media. After a certain time or amount of data has been written, or alternatively in the event of security-relevant events such as the removal of a user's authorization, updating the smart card key or ending maintenance mode, internal data media are automatically rekeyed.

For external data storage devices, rekeying is started either manually or on request. The boot process is tamper-proof by using Secure Boot. Either a shim bootloader signed by Microsoft or, for special security requirements, a bootloader signed by Rohde & Schwarz Cybersecurity itself with its own Secure Boot PKI can be used.

The mandatory two-factor pre-boot authentication requires a user-specific smart card and the entry of a PIN. The range of functions and background image for the unlock screen can be customized. An on-screen keyboard enables the PIN to be entered using a mouse or touch display.

Users can change or reset their personal PIN if necessary. A PIN policy can be enforced. If desired, a special stealth mode can conceal the fact that encryption is being used at all by booting a parallel system without sensitive data. Security-relevant events can be traced at any time via an audit log.

Simple administration

R&S®Trusted Disk can be easily rolled out to a large number of appropriately configured end devices. The initialization of the encryption can be automated using a command line tool. User productivity is not affected, as both the initial encryption and subsequent rekeying are carried out in the background and a special maintenance mode enables unattended restarts without user interaction.

Without a management system, both the management and the personalization of the smart cards with the R&S®Trusted Identity Manager Standalone must be carried out by an administrator on a separate device. With management system, smart card management is carried out via this. Personalization with the R&S®Trusted Identity Manager can be carried out either by an administrator or by the users themselves.

Alternatively, management and personalization of the smart cards can be done in an external smart card management system, which must use compatible profiles. If user smart cards are lost, security administrators can still access the encrypted data. Data recovery scenarios are supported by a recovery tool included in the delivery.

Central management

The use of the central management system R&S®Trusted Objects Manager simplifies administration considerably. It enables company-specific remote management of end devices, users, smart cards, groups and rights. A connection to LDAP directory services, e.g. Active Directory, is possible.

Required device and user certificates for the personalization of smart cards can be generated using an integrated PKI and easily managed throughout their entire lifecycle. Security policies can be enforced centrally. A tamper-proof audit log of the management system and all managed end devices with possible Syslog connection, SNMP and SMTP enable effective operational monitoring.

Point of difference

- Only VS-NfD compliant solution with central network-based management
- Wide hardware support
- Developed entirely in Germany with fast and reliable manufacturer support from Germany
- No known security incident since product launch 12 years ago
- In the BSI program of accelerated security certifications

Trust Seal
www.teletrust.de/itsmie

R&S®TRUSTED DISK

Data encryption	
Internal data media	► One or more internal physical data media ► Max. size of physical and logical data media: 20 Tbytes each ► Maximum of 8 internal logical data media
External data media	USB, max. size: 2 TB
Logical sector size	► Only 512 bytes supported: 512n/512 byte native or advanced format with 512e/512 byte emulation ► Not supported: 4Kn/4K Native or other formats that Windows also does not support by default.
Partition layout	All partitions to be encrypted must be arranged in a single, continuous area.
Sector-based encryption	AES-XTS-512
Security	
Boot process	► Tamperproof with UEFI Secure Boot ► Bootloader variants: – Microsoft-signed Shim bootloader – RSCS bootloader signed by Rohde & Schwarz Cybersecurity with its own secure boot PKI for specific security requirements
Authentication	► Pre-Boot Authentication (PBA): 2FA with smart card and PIN ► PIN policy can be specified
Asymmetrical encryption	► RSA with 2048 bit, 3072 bit or 4096 bit key length ► Public keys embedded into X.509 certificates
Secure random number generation	► Smart card seeding: smart card as a secure source of random numbers ► Hash-DRBG and HMAC-DRBG
Communication with smart card reader	Secured by blinding
Crypto algorithms	Botan crypto library, approved by the German BSI
Communication between device and management system	Through TLS-secured communication channel
Data rekeying	► Trigger: – After 4 years or after 5 Tbytes data have been written – In case of security-relevant events, e.g. removal of a permission ► For internal data media: automatically ► For external data media: When mounting, after user confirmation
Deletion of data on external data media	Deletion of the cryptographic keys using the Gutmann method
Event log audit log	Logging of security-related events
Optional stealth mode	Conceals that encryption is used at all
Supported devices	
System requirements	► Firmware based on UEFI specification from version 2.3.1/Errata C of June 2012 ► Hardware according to minimum Microsoft requirements for Windows 10 and 11 ► Deviating from this: – Only x8664 CPU – Usually at least 16 Gbytes RAM. Depending on the software used, more RAM can be necessary. – Display resolution for PBA screen ≥ 1024 × 768 (XGA) ► Data medium: – GPT-formatted – Windows and EFI system partition (ESP) on the same data medium – ESP size ≥ 200 Mbytes, permanently free storage ≥ 50 Mbytes
Compatibility	Experience has shown that there is a high level of compatibility, particularly with common Dell, HP and Lenovo notebook models. However, due to frequent model changes, the multiplicity of possible model configurations, different firmware variants versions as well as internal and external hardware components, we cannot generally guarantee compatibility. An initial assessment is therefore recommended.
Device-specific 3rd level support	Until EOS (end of support) of the respective device manufacturer, but not more than 5 years after the start of sales
Supported operating systems	
Windows 10 and 11	► 64-bit versions of the Pro and Enterprise editions ► The objective is to support all regular versions (functionality updates) with all currently available important updates and security updates until the end of support (EOS). ► LTS and other editions on request/project-specific
Windows server	On request/project-specific Windows Server 2016, 2019 and 2022

Note for IT administrators: Full-disk encryption is a critical system component. Therefore, end devices with R&S®Trusted Disk should be part of the test environment in which all Windows updates are tested prior to their organization-wide roll-out.

R&S®TRUSTED DISK

Localization	
PBA	► User interface: German, English ► Keyboard layouts: English (en_US), German (de_DE) and French (fr_FR)
Windows application	User interface: German, English
Smartcards	
Supported types and versions	► CardOS smart cards: Versions 5.0, 5.3, 5.3 DI ► More versions on request/project-specific
Personalization and management	► Variant with central management system: Using the central R&S®Trusted Objects Manager and local R&S®Trusted Identity Manager, personalization can be carried out either centrally by an administrator or by the users themselves when there is an existing network connection. ► Standalone variant without central management system: R&S®Trusted Identity Manager Standalone for administrators with limited functionality ► External smart card management with compatible smart card profiles
PKCS#11 smart card middleware	► CardOS API ► Nexus Personal: on request/project-specific
Smartcard reader	
Standards	► ISO/IEC 7816 ► PC/SC 2.x ► CCID 1.1
PIN-Eingabe	► Separate keyboard or on-screen keyboard ► Special smart card readers are not supported
Compatibility	Only the types of external USB smart card readers listed in the "Scope of delivery" section are regularly tested. Experience has shown that there is a high compatibility with many other internal and external ISO-7816 smart card readers. However, since we cannot provide a general guarantee of compatibility, an initial assessment of the suitability is necessary. When incompatibilities occur, they almost always result from non-standard behavior of hardware or firmware of smartcard readers. A solution usually always requires adjustments by the hardware manufacturer. Smartcard readers, which are listed here without restrictions (especially regarding the Extended APDU), are very likely to be supported: Supported CCID readers/ICCD tokens (apdu.fr) The recovery tool, however, has less compatibility with internal and external smart card readers from other vendors. The use of one of the types of external USB smart card readers listed in the "Ordering Information" section is recommended.
Multi-user functionality	
Number of permissions	Up to 15,000 permissions per data medium
Central management	
R&S®Trusted Objects Manager	Server/network device: see separate data sheet
Number of users/clients	Up to 50,000, depending in particular on the number of certificates per user; beyond this number project-specific
Approval by the German Federal Office for Information Security	
BSI-VSA-10580	► Restricted (Verschlusssache - Nur für den Dienstgebrauch, VS-NfD) ► EU Restricted (EU-R) for national use ► NATO Restricted (NR)
Scope of delivery	
Software components for Microsoft Windows	► Trusted Disk ► Trusted Disk Recovery ► With central management system: – Trusted Workstation Agent – Trusted Identity Manager ► Without central management system, optional: – Trusted Identity Manager Standalone ► MS Visual Studio Redistributable(s) ► CardOS API
Documentation	► Release notes, English ► User manuals, German and English ► Administrator manuals, German and English ► Trusted Identity Manager Standalone: Documentation English only
Deployment	Only digital

R&S®TRUSTED DISK

Variant	License / type	License model / validity	Order numbers (formerly R&S Cybersecurity, SLA Priority)	Item numbers (effective as of Sept. 01, 2026)
Licenses, maintenance, and 3rd level support				
With central management	VS-NfD/EU-R/NR	Subscription 1 yr./3 yrs./var.	3648.3133.12/36/37	40161/40162/40163
	Other, exportable	Subscription 1 yr./3 yrs./ var.	3648.7468.12/36/37	40168/40169/40170
Without central management	VS-NfD/EU-R/NR	Subscription 1 yr./3 yrs./var.	3641.3873.12/36/37	40148/40149/40150
	Other, exportable	Subscription 1 yr./3 yrs./var.	3641.1058.12/36/37	40141/40142/40143
	R&S®Trusted Identity Manager Standalone	Subscription 1 yr./3 yrs./var.	4609.0010.12/36/37	40171/40172/40173
Additional smart cards if number of smart cards > clients	Trusted Identity Manager Basic	Subscription 1 yr./3 yrs./var.	4619.9340.12/36/37	40184/40185/40186
Management system				
R&S®Trusted Objects Manager	HW appliance	TOM-S Gen. 2 TOM-M Gen. 2	4619.8343.02 4619.8350.04	follows 40425
	HW maintenance	1 yr./3 yrs./var.	3648.4830.12/36/37	40412/40413/40414
Extension licenses	Multi-client capability	Subscription 1 yr./3 yrs./var.	3645.5112.12/36/37	40431/40432/40433
	Genua support I: client certificates and CSR support	Subscription 1 yr./3 yrs./var.	3741.2855.12/36/37	40077/40078/40079
	Genua support II: configuration & management of Genuscreen SRA gateways and Genuconnect clients	Subscription 1 yr./3 yrs./var.	3748.2844.12/36/37	40050/40051/40052
Optional support for additional certificates on the same smart card	OpenPGP/GnuPG VS-Desktop	Subscription 1 yr./3 yrs./var.	3739.0271.12/36/37	40073/40074/40075
	Document Signing	Subscription 1 yr./3 yrs./var.	3746.2201.12/36/37	40090/40091/40092
	S/MIME	Subscription 1 yr./3 yrs./var.	3744.2785.12/36/37	40082/40083/40084
	Windows logon	Subscription 1 yr./3 yrs./var.	3747.2840.12/36/37	40093/40094/40095
Smart cards				
CardOS 5.3	Full size	Smart card, not personalized	4619.9162.22	40127
	SIM size	Smart card, not personalized	4619.9162.21	40130
Smart card readers				
Full size	USB-A	USB device IDBridge CT30	4619.8937.02	40129
	Optional stand	For USBdevice IDBridge CT30	4619.8850.02	40128
SIM size	USB-A	USB token ACR39T-A1, RS-Branding	3697.5871.04	40133
	USB-C	USB token ACR39T-A5, RS-Branding	3697.5871.05	40134
Services				
On-site service	Daily rate for technical sipport	Excluding travel expenses	3666.9000.51	40122
Travel expenses	Flat daily rate	Within Germany	5413.9920.15	follows

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

ROHDE&SCHWARZ
Make ideas real