

# R&S® TRUSTED DISK

## Specifications

### Release 3.8.0

#### Data encryption

Internal data media	<ul style="list-style-type: none"><li>• One or more internal physical data media</li><li>• Max. size of physical and logical data media: 20 Tbytes each</li><li>• Maximum of 8 internal logical data media</li></ul>
External data media	USB, max. size: 2 Tbytes
Logical sector size	<ul style="list-style-type: none"><li>• Only 512 bytes supported: 512n/512-byte native or advanced format with 512e/512-byte emulation</li><li>• Not supported: 4Kn/4K Native or other formats that Windows also does not support by default.</li></ul>
Partition layout	All partitions to be encrypted must be arranged in a single, continuous area.
Sector-based encryption	AES-XTS-512

#### Security

Boot process	<ul style="list-style-type: none"><li>• Tamper-proof with UEFI Secure Boot</li><li>• Bootloader variants:<ul style="list-style-type: none"><li>▪ Microsoft-signed Shim bootloader</li><li>▪ RSCS bootloader signed by Rohde &amp; Schwarz Cybersecurity with its own secure boot PKI for specific security requirements</li></ul></li></ul>
Authentication	<ul style="list-style-type: none"><li>• Pre-Boot Authentication (PBA): 2FA with smart card and PIN</li><li>• PIN policy can be specified</li></ul>
Asymmetrical encryption	<ul style="list-style-type: none"><li>• RSA with 2048-bit, 3072-bit or 4096-bit key length</li><li>• Public keys embedded into X.509 certificates</li></ul>
Secure random number generation	<ul style="list-style-type: none"><li>• Smart card seeding: smart card as a secure source of random numbers</li><li>• Hash-DRBG and HMAC-DRBG</li></ul>
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	<ul style="list-style-type: none"><li>• Trigger:<ul style="list-style-type: none"><li>▪ After 4 years or after 5 Tbytes data have been written</li><li>▪ In case of security-relevant events, e.g. removal of a permission</li></ul></li><li>• For internal data media: automatically</li><li>• For external data media: When mounting, after user confirmation</li></ul>
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	<ul style="list-style-type: none"> <li>Firmware based on UEFI specification from version 2.3.1/Errata C of June 2012</li> <li>Hardware according to minimum Microsoft requirements for Windows 10 and 11</li> <li>Deviating from this: <ul style="list-style-type: none"> <li>Only x86-64 CPU</li> <li>Usually at least 16 Gbytes RAM. Depending on the software used, more RAM can be necessary.</li> <li>Display resolution for PBA screen <math>\geq 1024 \times 768</math> (XGA)</li> </ul> </li> <li>Data medium: <ul style="list-style-type: none"> <li>GPT-formatted</li> <li>Windows and EFI system partition (ESP) on the same data medium</li> <li>ESP size <math>\geq 200</math> Mbytes, permanently free storage <math>\geq 50</math> Mbytes</li> </ul> </li> </ul>
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	<ul style="list-style-type: none"> <li>64-bit versions of the Pro and Enterprise editions</li> <li>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).</li> <li>LTS and other editions on request/project-specific</li> </ul>
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.

## Localization

PBA	<ul style="list-style-type: none"> <li>User interface: German, English</li> <li>Keyboard layouts: English (en_US), German (de_DE) and French (fr_FR)</li> </ul>
Windows application	User interface: German, English

## Smart cards

Supported types and versions	<ul style="list-style-type: none"> <li>CardOS smart cards: Versions 5.0, 5.3, 5.3 DI</li> <li>More versions on request/project-specific</li> </ul>
Personalization and management	<ul style="list-style-type: none"> <li>Variant with central management system: Using the central R&amp;S®Trusted Objects Manager and local R&amp;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.</li> <li>Standalone variant without central management system: R&amp;S®Trusted Identity Manager Standalone for administrators with limited functionality</li> <li>External smart card management with compatible smart card profiles</li> </ul>
PKCS#11 smart card middleware	<ul style="list-style-type: none"> <li>CardOS API</li> <li>Nexus Personal: on request/project-specific</li> </ul>

## Smart card readers

Standards	<ul style="list-style-type: none"> <li>• ISO/IEC 7816</li> <li>• PC/SC 2.x</li> <li>• CCID 1.1</li> </ul>
PIN input	<ul style="list-style-type: none"> <li>• Separate keyboard or on-screen keyboard</li> <li>• Special smart card readers are not supported</li> </ul>
Compatibility	<p>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:  <a href="#">Supported CCID readers/ICCD tokens (apdu.fr)</a>  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.</p>

## 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	<ul style="list-style-type: none"> <li>• Restricted (Verschlussache – Nur für den Dienstgebrauch, VS-NfD)</li> <li>• EU Restricted (EU-R) for national use</li> <li>• NATO Restricted (NR)</li> </ul>
---------------	---

## Scope of delivery

Software components for Microsoft Windows	<ul style="list-style-type: none"> <li>• Trusted Disk</li> <li>• Trusted Disk Recovery</li> <li>• With central management system: <ul style="list-style-type: none"> <li>▪ Trusted Workstation Agent</li> <li>▪ Trusted Identity Manager</li> </ul> </li> <li>• Without central management system, optional: <ul style="list-style-type: none"> <li>▪ Trusted Identity Manager Standalone</li> </ul> </li> <li>• MS Visual Studio Redistributable(s)</li> <li>• CardOS API</li> </ul>
Documentation	<ul style="list-style-type: none"> <li>• Release notes, English</li> <li>• User manuals, German and English</li> <li>• Administrator manuals, German and English</li> <li>• Trusted Identity Manager Standalone: Documentation English only</li> </ul>
Deployment	Only digital

## Ordering information

### Licenses, maintenance and 3rd level support

Variant	License / type	License model / validity term	Order no. (SLA priority)
With central management	VS-NfD/EU-R/NR	Subscription 1 yr./3 yrs./var.	3648.3133.12/36/37
	Other, exportable	Subscription 1 yr./3 yrs./var.	3648.7468.12/36/37
Without central management	VS-NfD/EU-R/NR	Subscription 1 yr./3 yrs./var.	3641.3873.12/36/37
	Other, exportable	Subscription 1 yr./3 yrs./var.	3641.1058.12/36/37
	R&S®Trusted Identity Manager Standalone	Subscription 1 yr./3 yrs./var.	4609.0010.12/36/37
Additional smart cards if number of smart cards > clients	Trusted Identity Manager Basic	Subscription 1 yr./3 yrs./var.	4619.9340.12/36/37

### Management system

R&S®Trusted Objects Manager	HW appliance	TOM-S Gen. 2	4619.8343.02
		TOM-M Gen. 2	4619.8350.04
	HW maintenance	1 yr./3 yrs./variable	3648.4830.12/36/37
Extension licenses	Multi-client capability	Subscription 1 yr./3 yrs./var.	3645.5112.12/36/37
	Genua support I: client certificates and CSR support	Subscription 1 yr./3 yrs./var.	3741.2855.12/36/37
	Genua support II: configuration & management of Genuscreen SRA gateways and Genuconnect clients	Subscription 1 yr./3 yrs./var.	3748.2844.12/36/37
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
	Document signing	Subscription 1 yr./3 yrs./var.	3746.2201.12/36/37
	S/MIME	Subscription 1 yr./3 yrs./var.	3744.2785.12/36/37
	Windows logon	Subscription 1 yr./3 yrs./var.	3747.2840.12/36/37

### Smart cards

CardOS 5.3	Full size	Smart card, not personalized	4619.9162.22
	SIM size	Smart card, not personalized	4619.9162.21

### Smart card readers

Full size	USB-A	USB device IDBridge CT30	4619.8937.02
	Optional stand	For USB device IDBridge CT30	4619.8850.02
SIM size	USB-A	USB token ACR39T-A1, RS branding	3697.5871.04
	USB-C	USB token ACR39T-A5, RS branding	3697.5871.05

### Services

On-site service	Daily rate for technical expert	Excluding travel expenses	3666.9000.51
Travel expenses	Flat daily rate	Within Germany	5413.9920.15

#### Rohde & Schwarz Cybersecurity GmbH

Mühdorfstrasse 15, 81671 Munich, Germany

[www.rohde-schwarz.com/cybersecurity](http://www.rohde-schwarz.com/cybersecurity)  
[cybersecurity@rohde-schwarz.com](mailto:cybersecurity@rohde-schwarz.com)

Rohde & Schwarz GmbH & Co. KG

[www.rohde-schwarz.com](http://www.rohde-schwarz.com)

Certified Quality Management

ISO 9001

Certified Information Security Management

ISO 27001

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG

Trade names are trademarks of the owners

PD 3607.5831.22 | Version 05.00 | July 2025 (wm)

R&S®Trusted Disk

Data without tolerance limits is not binding | Subject to change

© 2021 – 2025 Rohde & Schwarz GmbH & Co. KG | 81671 Munich, Germany