Rohde & Schwarz Cybersecurity

R&S®TRUSTED DISK

VS-NfD,
EU RESTRICTED,
NATO RESTRICTED

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

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

Product Flyer
Version 07.00

ROHDE&SCHWARZ
Make ideas real

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

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

Rohde & Schwarz training
www.training.rohde-schwarz.com
Rohde & Schwarz customer support
www.rohde-schwarz.com/support

PD 3607.5831.32 | Version 07.00 | Oktober 2024 (dh)
R&S®Trusted Disk
Data without tolerance limits is not binding | Subject to change