R&S®TRUSTED DISK

Specifications

Description

R&S®Trusted Disk is a full disk encryption solution which was developed based on current BSI (German Federal Office for Information Security) standards aiming for VS-NfD (RESTRICTED) approval. This includes up-to-date random number generation and flexible re-keying according to time and amount of data. In addition to the data, R&S®Trusted Disk encrypts the complete operating system, including all temporary files.

R&S®Trusted Disk uses a transparent real-time encryption method to ensure full, hassle-free productivity on all computers (laptops, desktops and server systems). A pre-boot authentication procedure employs a smart card-based two-factor authentication to validate the users' identity using their PIN. Modern secure boot mechanisms are employed as well as a SHIM boot loader to facilitate easy rollout into large installations.

Overview

Core features	• Two-factor pre-boot authentication (PBA) with smart card • PBA: On-screen keyboard (tablets, touch screens) • PBA: PIN change • PBA: PIN reset with PUK and challenge response • PBA: Customizable in accordance with corporate design (colors, background image, position of buttons) • PIN policy • Windows PE-based recovery tool (decryption of system / EDE volumes) • Stealth mode • Audit log • Encryption of external storage devices (e.g. USB and Thunderbolt storage devices) • Maintenance mode for fully, non-interactive reboots of the system
Central and local management	• Managed & standalone variants • Authorization of up to 15,000 users • PKI management via central management • User and workstation management via central management • Smart card personalization via R&S®Trusted Identity Manager
Deployment	• Windows feature update support • Initialization of encryption via GUI wizard or command line (CLI) • SHIM support for easy rollout into large deployments
Compatible operating systems	• Windows 7[1] • Windows 8.1 • Windows 10 • Windows 11 • Windows Server 2016, Windows Server 2019, Windows Server 2022

[1] Only Legacy BIOS/MBR with SP1 installed

Security features

General	Encryption rekeying	Based on time and written bytes or manually triggered
	UEFI Secure Boot	SHIM
		Manual system takeover
Random number generation	Hash DRBG and NIST HMAC_DRBG	Smart card seeding
User authentication	Two-factor authentication	RSA >= 2048 bit
		Public keys embedded into X.509 certificates
		Private keys stored on smart cards
Encryption algorithms	AES-XTS 512 bit	
	RSA blinding	Protection of communication between reader and system
Secure data deletion	Gutmann	
Crypto libraries	Botan	
Supported smart cards	Atos CardOS	Version 5.0 Version 5.3 Version 5.3 DI
	Gemalto eToken	
	Electronic service and troop ID	
PKCS#11-Middleware	Atos CardOS API	Version >= 5.5.2
	Nexus Personal Desktop Client	Version >= 4.29.5
	Safenet Authentication Client	Version >= 9.0.43

Miscellaneous

Smart card readers	SIM-size reader	
	Full-size reader	
Smart card reader recommendation	IDBridge CT30, IDBridge K30, IDBridge K50, ACS ACR39T-A1/-A5 (USB-A/C)	
System requirements	An internal hard disk drive for encryption	
	UEFI mode	GPT-formatted
		Windows and EFI system partition on the same hard disk drive
		50 MB free disk space on EFI system partition (ESP)
	Legacy boot	MBR-formatted
		Windows on two partitions (boot partition and system partition)
		50 MB free disk space on boot partition

Rohde & Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Germany
Info: +49 30 65884-222
Email: cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity

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

Certified Quality Management
ISO 9001

PD 3607.5831.22 | Version 02.00 | March 2022 (sch)
R&S®Trusted Disk