R&S®TRUSTED DISK

Spezifikationen

Beschreibung

R&S®Trusted Disk ist eine Festplattenverschlüsselungslösung, die auf Basis aktueller BSI-Standards mit dem Ziel der VS-NfD-Zulassung entwickelt wurde. Dies schließt eine aktuelle Zufallszahlengenerierung und die flexible Umschlüsselung in Abhängigkeit der Zeit und der geschriebenen Daten ein. R&S®Trusted Disk verschlüsselt das gesamte Betriebssystem, einschließlich aller temporärer Dateien.

R&S®Trusted Disk nutzt eine transparente Echtzeitverschlüsselung, um die vollumfängliche Produktivität aller Computer (Laptops, Desktops, Serversysteme) problemlos zu gewährleisten. Ein Pre-Boot-Authentifizierungsverfahren nutzt eine Smartcard-basierte Zwei-Faktor-Authentifizierung, um die Identität der Benutzer mittels Smartcard und PIN zu validieren. Es werden sichere Boot-Mechanismen sowie ein SHIM-Bootloader genutzt. Dies soll eine einfache Bereitstellung auf einer großen Anzahl von Endgeräten ermöglichen.

Überblick

Kernfeatures	• Zwei-Faktor-Pre-Boot-Authentifizierung (PBA) mit Smartcard • PBA: Bildschirmtastatur (Tablets, Touchscreens) • PBA: PIN ändern • PBA: PIN zurücksetzen mit PUK und Challenge Response-Verfahren • PBA: Anpassbar an Corporate Design (Farben, Hintergrundbild, Position der Schaltflächen) • PIN-Richtlinie • Windows PE-basiertes Recovery Tool (Entschlüsseln von System-/ EDE-Datenträger) • Stealth-Modus • Audit-Log • Verschlüsselung externer Speichermedien (z.B. USB- und Thunderbolt-Speichermedien) • Wartungsmodus für vollautomatische Reboots ohne Nutzerinteraktion
Zentrales und lokales Management	• Varianten „Managed“ und „Standalone“ • Berechtigung für bis zu 15.000 Benutzern • PKI-Management über zentrales Management • Benutzer- und Workstationverwaltung über zentrales Management • Smartcard-Personalisierung über R&S®Trusted Identity Manager
Bereitstellung	• Support von Windows Feature Updates • Initialisierung der Verschlüsselung durch GUI-Wizard oder Command Line (CLI) • SHIM-Support für einfache Bereitstellung auf einer großen Anzahl von Endgeräten
Kompatibilität Betriebssystem	• Windows 7[1] • Windows 8.1 • Windows 10 • Windows 11 • Windows Server 2016, Windows Server 2019, Windows Server 2022

[1] Nur Legacy BIOS/MBR mit installiertem SP1

Sicherheitsfeatures

Allgemein	Umschlüsselung	Basierend auf Zeit, geschriebenen Daten, oder manuell ausgelöst
	UEFI Secure Boot	SHIM
		Manuelle Plattformübernahme
Zufallszahlen	Hash DRBG und HMAC DRBG	Smartcard-Seeding
Nutzerauthentifizierung	Zwei-Faktor-Authentifizierung	RSA >= 2048-Bit
		Öffentliche Schlüssel in X.509-Zertifikaten eingebettet
		Private Schlüssel auf Smartcards gespeichert
Verschlüsselungsalgorithmen	AES-XTS 512 Bit	
	RSA-Blinding	Absicherung der Kommunikation zwischen Reader und System
Sichere Datenlöschung	Gutmann	
Krypto-Bibliotheken	Botan	
Unterstützte Smartcards	Atos CardOS	Version 5.0 Version 5.3 Version 5.3 DI
	Gemalto eToken	
	Elektronischer Dienst- und Truppenausweis	
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

Verschiedenes

Smartcard-Readers	SIM-Size Reader	
	Full-Size Reader	
Smartcard-Reader Empfehlung	IDBridge CT30, IDBridge K30, IDBridge K50, ACS ACR39T-A1/-A5 (USB-A/C)	
Systemanforderungen	Ein internes Festplattenlaufwerk für die Verschlüsselung	
	UEFI-Modus	GPT-formatiert
		Windows und EFI-Systempartition (ESP) auf demselben Festplattenlaufwerk
		50 MB freier Speicherplatz auf EFI-Systempartition (ESP)
	Legacy Boot	MBR-formatiert
		Windows auf zwei Partitionen (Bootpartition und Systempartition)
		50 MB freier Speicherplatz auf Bootpartition

Rohde & Schwarz Cybersecurity GmbH
Mühldorfstraße 15 | 81671 München
Info: +49 30 65884-222
E-Mail: cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity

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

Certified Quality Management
ISO 9001

PD 3607.5831.21 | Version 02.00 | März 2022 (sch)
R&S®Trusted Disk