R&S®TRUSTED VPN CLIENT

Spezifikationen

Kurzbeschreibung

R&S®Trusted VPN Client als SRA-(Secure Remote Access) Lösung schützt die organisationsinterne Netzwerkkommunikation zwischen Client-Plattform und VPN Gateway. Endgeräte der Mitarbeiter wie Laptops können sich somit sicher mit dem Intranet verbinden, obwohl der Datenverkehr über ein unsicheres Netzwerk wie das Internet geleitet wird.

R&S®Trusted VPN Client wurde gemäß den Anforderungen des BSI (Bundesamt für Sicherheit in der Informationstechnik) VS-Anforderungsprofils für vertrauenswürdige VPN Clients konzipiert, mit dem die Übertragung von VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) klassifizierten Daten erlaubt ist.

Übersicht

Kernleistung	• Softwarebasierter VPN Client • Zwei-Faktor-Authentisierung mittels Smartcard • Gehärtete, minimalinvasive Isolationsplattform zur Kapselung von Windows 10™ • UEFI Firmware-Schutz • Transparenten Umleitung des vollständigen Netzwerkverkehrs durch die VPN-Verbindung • Unterstützung von LAN und WLAN Zugangstechnologie für die VPN-Verbindung
Management	• Produktübergreifende Fernkonfiguration durch das zentrale Managementsystem R&S®Trusted Objects Manager • Netzwerkzugriffe als Gruppen- und Benutzerkonfigurationen einstellbar • Warm Standby Support • Master/ Slave VPN Gateway Support
Deployment	• Softwareinstallation und -verteilung über ECM-Systeme wie z. B. Microsoft® SCCM™ • Keine Beeinträchtigung der bestehenden Windows 10™-Installation
Kompatibilität	• Microsoft® Windows 10™ • Intel® Core™ Mobile-Prozessoren (ab Generation 6) • Virtualization Based Security Features (VBS) • R&S®Trusted Disk (Full Disk Encryption) • R&S®Trusted Identity Manager Extended (PKI & Smartcard Management) • R&S®Trusted VPN • R&S®Trusted Objects Manager • R&S®Browser in the Box (Hyper-V Edition) • CardOS API V5.0, V5.3

Netzwerk

Technologien	Ethernet	LAN
	Wi-Fi/ WLAN	WPA2 Personal
	USB	LAN-Adapter
		WLAN-Adapter
VPN Modi	Client-to-Site VPN	
	IPsec Tunnel Mode (ESP)	
R&S®Trusted VPN (VPN Gateway)	R&S®Trusted VPN L Gen 2 (TPM 2.0) Version 6.x.x	VS-NfD (German)
		SoCM-Standard (EU restricted (national))
		SoM-Standard (NATO restricted)

Sicherheitsfeatures

Internet Key Exchange (IKEv2)	RSA bis 4096 Bits	Ausschließlich nicht-VS-NfD
	ECC-512 (Brainpool-Kurve, 512 Bit)	ECDSA-SHA-2-512
		ECDH
Client-Authentifizierung	Multifaktor-Authentifizierung	mittels Smartcard und PIN
Verschlüsselungsalgorithmen	Asymmetrisch	RSA
		ECC
	Symmetrisch	AES-256-GCM
		SHA-2 bis 512 Bits
Krypto-Bibliotheken	Botan	
Atos CardOS Smartcards	CardOS Version	V5.0
		V5.3

Systemanforderungen

R&S®Trusted VPN Client		
CPU	Intel® Core™	≥ Dual Core 2.2 GHz
		≥ i-Core™6th Generation (available since 2015)
Speicher	RAM	≥ 8 GB RAM
	Disk Space	≥ 1 GB freier Festplattenspeicher
Betriebssystem	Windows™	Microsoft® Windows 10™ mit UEFI (GPT)

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 3608.0779.21 | Version 01.01 | Oktober 2020 (sch)
R&S®Trusted VPN Client