Netzwerk- Authentifizierungen (Lokal, Domäne)

Protocol	Definition	Confidentiality, Integrity, Availability (CIA)	Status
Kerberos	Ticketbasierte Authentifizierung an einer Domäne (seit Windows 2000)		State of the Art
NT Lan Manager Version 2 (NTLMv2)	Verbesserte (sicherere) Version (seit Windows NT4 SP4)		not recommended
NT Lan Manager (NTLM)	Authentifizierung an der Domäne (Windows NT)		Legacy

RAS – VPN Authentifizierungen

Authentifizierung innerhalb des VPN-Tunnels

Protocol	Definition	Confidentiality, Integrity, Availability (CIA)	Status	Anmerkungen
Extensible Authentication Protocol (EAP)	Smartcard oder anderes Zertifikat (EAP-TLS) Authentifizierung per Zertifikat Geschütztes EAP (PEAP) Authentifizierung per Benutzername + Kennwort EAP – MS-CHAPv2 Authentifizierung per Benutzername + Kennwort über MS-CHAPv2		State of the Art	
Internet Key Exchange Protocol (IKEv2 / with Ipsec)	Authentifizierung mit Zertifikaten + DH – Schlüsselaustausch		State of the Art	Add Authentication to IPsec
Microsoft Challenge Handshake Protocol (MS-CHAPv1 / v2)	Authentifizierung per Challenge Handshake (Hash)			Only use with EAP if necessary
Challenge Handshake Protocol (CHAP)	Authentifizierung per Challenge Handshake (Hash) / Microsoft Arbeitsgruppe		Legacy	Only use with EAP if necessary
Password Authentication Protocol (PAP)	Benuzername + Passwort im Klartext		Legacy	Do not use anymore

Virtual Private Network Protocols (VPN) Tunneling

Aufbau, Authentifizierung und Verschlüsselung des VPN-Tunnels

Developers	Protocols	Confidentiality, Integrity, Availability (CIA) Supported Levels	Verschlüsselungsarten	Authentifizierungsarten	Authentifizierung	Status	Ports	Anmerkungen	Links
Jason A. Donenfeld	Wireguard					New Comer	UDP	Direkt im Linux Kernel ab V5.6 integriert	https://en.wikipedia.org/wiki/WireGuard
University Tsukuba Japan	SoftEther					New Comer			https://en.wikipedia.org/wiki/SoftEther_VPN
OpenVPN Technologies	OpenVPN (auch als SSL-VPN mit OpenSSL)	Confidentiality, Integrity	AES-160, 256 Bit	EAP-TLS, EAP-TTLS, PEAP, EAP-MS-CHAPv2, etc	Benutzer und Computer	State of the Art	UDP 1194 / TCP 443	Allrounder	https://en.wikipedia.org/wiki/OpenVPN
Microsoft	Secure Socket Tunneling Protocol (SSTP / SSL-VPN)	Confidentiality, Integrity	AES-256 Bit	EAP, MS-CHAPv2	Nur Benutzer	State of the Art	TCP 442	Empfohlen für Windows VPNs	https://en.wikipedia.org/wiki/Secure_Socket_Tunneling_Protocol
Microsoft / Cisco	Internet Key Exchange Protocol (IKEv2 / with IPsec)	Confidentiality, Integrity	AES-256 Bit	IKEv2, EAP	Benutzer und Computer	State of the Art	UDP 500	Sehr robust bei instabilen Verbindungen	https://en.wikipedia.org/wiki/Internet_Key_Exchange
Internet Engineering Task Force (IETF)	Layer 2 Tunneling Protocol via L2TP / IPsec	Confidentiality, Integrity	AES-256 Bit	EAP	Benutzer und Computer	Possible Compromised by NSA	UDP 500 : TCP 1701		https://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol#L2TP.2FIPsec
Internet Engineering Task Force (IETF)	Internet Protocol Security (IPsec)	Confidentiality, Integrity	AES-256 Bit	None	-	Legacy	UDP 1293 / TCP 1293	Combined with L2TP or IKEv2 to provide authentication	https://en.wikipedia.org/wiki/IPsec
Internet Engineering Task Force (IETF)	Layer 2 Tunneling Protocol (L2TP)	Confidentiality, Integrity only for L2TP Header no for data	None	PAP, CHAP	Benutzer oder Computer	Legacy	UDP 1701 / TCP 1701	Nachfolger von PPTP / MSPPTP und Cisco Layer 2 Forwarding (L2F)	https://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol#L2TP.2FIPsec
Microsoft, Cisco	Microsoft Point to Point Protocol / Encryption (MSPPTP / MPPE)	Confidentiality	40, 56, 128 Bit	PAP, CHAP, MS-CHAP v1/v2	Benutzer oder Computer	Legacy	TCP 1723 / IP Port 47	Microsoft Implementierung des PPTP Protokolls	https://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol
Microsoft, 3Com, Ascend Communication	Point to Point Tunneling Protocol (PPTP) (mit GRE)	Confidentiality	No specified depends on the PPP Protocol	No specified depends on the PPP Protocol	Nur Benutzer	Legacy	TCP 1723 / IP Port 47	Aufbauend auf PPP + Erweiterung GRE / Standard VPN-Protokoll	https://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol
	Point to Point Protocol (PPP) (PPPoE / PPPoA)	Confidentiality, Integrity	Encryption Control Protocol (ECP), MPPE	PAP, CHAP, EAP	Nur Benutzer	Standard bei ISP		Basis Remote Access Protokoll für höhere Schichtprotokolle e.g IP, PPTP, L2TP etc. allein Legacy	https://en.wikipedia.org/wiki/Point-to-Point_Protocol

The table below breaks down the cipher suite string above into what is preferred in order (best key exchange algorithm/strongest encryption first).

Order	Key Exchange Algorithm	Authentication Algorithm	Block Cipher Encryption Algorithm	Mac Algorithm
#1	Elliptic Curve Diffie-Hellman (ECDH)	Elliptic Curve Digital Signature Algorithm (ECDSA)	AES 256 in Galois Counter Mode (AES256-GCM)	SHA384
#2	Elliptic Curve Diffie-Hellman (ECDH)	RSA	AES 256 in Galois Counter Mode (AES256-GCM)	SHA384
#3	Elliptic curve Diffie-Hellman (ECDH)	Elliptic Curve Digital Signature Algorithm (ECDSA)	ChaCha20 (CHACHA20)	POLY1305
#4	Elliptic curve Diffie-Hellman (ECDH)	RSA	ChaCha20 (CHACHA20)	POLY1305
#5	Elliptic Curve Diffie-Hellman (ECDH)	Elliptic Curve Digital Signature Algorithm (ECDSA)	AES 128 in Galois Counter Mode (AES128-GCM)	SHA256
#6	Elliptic curve Diffie-Hellman (ECDH)	RSA	AES 128 in Galois Counter Mode (AES128-GCM)	SHA256
#7	Elliptic Curve Diffie-Hellman (ECDH)	Elliptic Curve Digital Signature Algorithm (ECDSA)	AES 256 (AES256)	SHA384
#8	Elliptic curve Diffie-Hellman (ECDH)	RSA	AES 256 (AES256)	SHA384
#9	Elliptic Curve Diffie-Hellman (ECDH)	Elliptic Curve Digital Signature Algorithm (ECDSA)	AES 128 (AES128)	SHA256
#10	Elliptic curve Diffie-Hellman (ECDH)	RSA	AES 128 (AES128)	SHA256

Quellen:

https://en.wikipedia.org/wiki/Virtual_private_network
https://de.wikipedia.org/wiki/Virtual_Private_Network

https://de.wikipedia.org/wiki/Point-to-Point_Protocol
https://en.wikipedia.org/wiki/Point-to-Point_Protocol
https://de.wikipedia.org/wiki/IPsec
https://en.wikipedia.org/wiki/IPsec
https://en.wikipedia.org/wiki/Internet_Key_Exchange
https://de.wikipedia.org/wiki/Layer_2_Tunneling_Protocol
https://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol
https://en.wikipedia.org/wiki/Secure_Socket_Tunneling_Protocol

https://en.wikipedia.org/wiki/Authentication_protocol
https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol
https://de.wikipedia.org/wiki/Extensible_Authentication_Protocol
https://de.wikipedia.org/wiki/Challenge_Handshake_Authentication_Protocol
https://en.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol
https://en.wikipedia.org/wiki/Password_Authentication_Protocol
https://de.wikipedia.org/wiki/Password_Authentication_Protocol

https://proprivacy.com/vpn/guides/vpn-encryption-the-complete-guide
https://www.vpnmentor.com/blog/vpn-protocol-comparison-pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/
https://thebestvpn.com/pptp-l2tp-openvpn-sstp-ikev2-protocols/
https://www.experte.de/vpn/protokolle
https://de.vpnmentor.com/blog/welches-vpn-protokoll-soll-ich-benutzen/
https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-pptp/

https://www.webhostingsecretrevealed.net/the-a-to-z-vpn-guide/

https://de.wikipedia.org/wiki/WireGuard
https://en.wikipedia.org/wiki/SoftEther_VPN
https://www.softether.org/