Data Sheet

NCP VS GovNet Connector for Windows

Centrally managed software-based solution for remote access workstations processing sensitive data

- Approval for NATO RESTRICTED and RESTREINT UE/EU RESTRICTED (BSI-VSA-10710)
- Central management
- Self-check to ensure integrity
- Managed firewall
- Friendly net detection
- Hotspot Logon
- VPN Path Finder Technology
- (Fallback IPsec/HTTPS)
- Strong authentication
- Support for Wi-Fi and mobile data
- Custom Branding

Software-based Solution

NCP VS GovNet Connector complies with NATO RESTRICTED and EU RESTRICTED classifications and provides a secure link between government workstations and remote systems. As a purely software-based solution, it can be easily distributed to workstations using standard tools. Users benefit from the wide range of features which offer an advanced level of security but remain easy to use.

Based on the IPsec standard, highly secure data connections can be established with the NCP VS GovNet Server that comply with the specifications of authorities and governments.

Thanks to the support of standard interfaces, the software can be combined with other approved authentication hardware (e.g. smartcard readers) or software (e.g. hard disk encryption).

Users can access secure networks from anywhere in the world from computers running Microsoft Windows. NCP VS GovNet Connector supports seamless roaming to automatically switch to the best available connection medium – ideal for always-on operation. Even if the connection medium is changed or briefly interrupted, the connection medium can maintain an application session with the NCP VS GovNet Server.

Self Check

The integrity service in the VS GovNet Connector continuously monitors that operating system components are working correctly. If the VS GovNet Connector is compromised the device enters a secure state and blocks all communication.

Furthermore, the integrity service supports secure remote updates to the VS GovNet Connector via central management at all times.

VPN Path Finder Technology

This feature can bypass firewalls or proxies that block IPsec traffic. It automatically switches to a modified IPsec protocol mode which uses the HTTPS port to establish a VPN tunnel. This offers the same security features as IPsec, which means that the VPN Path Finder protocol does not need to be re-evaluated for security reasons.
The budget manager included in the NCP VS GovNet Connector enables cost-effective operation. Volume

and time budgets can be set for individual providers to ensure that online costs do not get out of hand.

Authentication

In addition to supporting certificates or smart cards in a PKI (Public Key Infrastructure), NCP VS GovNet Connector has optional support for OTP solutions[2] [3] or biometric authentication[2] before the VPN connection is established, for example via fingerprint or facial recognition. The authentication process begins when users click connect in the connector UI, but the connection is not initiated until biometric authentication has been successfully completed. If the device does not have any hardware for biometric authentication or if this is not activated, the user may alternatively enter a password.

Firewall

The NCP VS GovNet Connector includes an integrated dynamic personal firewall. This can be managed centrally, so that rules for ports, IP addresses, segments and applications can be set by the administrator. Firewall rules can also be configured for the VPN tunnel and external networks. The NCP VS GovNet Connector is enabled automatically on system startup.

Friendly Net Detection

Friendly net detection feature detects secure corporate or government networks (friendly networks) using certificate-based authentication. When a friendly network is detected, firewall rules configured in the VS GovNet Connector for the friendly network can be activated automatically to allow secure data exchange without a VPN tunnel or to allow administrative access to the device. Manual VPN connection can also be disabled when the user is connected to a friendly network.

Hotspot Logon

Often users are prevented from accessing Wi-Fi hotspots by security requirements that only permit communication through the VPN tunnel in insecure network environments, as the initial login page is accessed via the web browser without a VPN tunnel.

This issue is solved by the Hotspot Logon feature in the VS GovNet Connector, which offers the highest level of security while logging on to hotspots before the VPN tunnel is set up through a dedicated, secure web browser and dynamic firewall rules. If the login is successful, the VS GovNet Connector automatically sets up the VPN tunnel.

Central Management

Organizations can deploy, set up, update and manage the NCP VS GovNet Connector via NCP Secure Enterprise Management (SEM) and the associated VS GovNet Connector plug-in as a single point of administration (a prerequisite for using the NCP VS GovNet Connector). All settings in the NCP VS GovNet Connector can be locked by the administrator. This prevents users from making any unwanted or unintended changes to the configuration.

Log files generated by the VS GovNet Connector, as well as the new audit log with all security-relevant events, are periodically transmitted to central management servers for evaluation.

Custom branding

With the custom branding option, companies can display their own logo or support information in the client. The client also supports accessibility features including screen readers.

Operating Systems [1]	Microsoft Windows 10 (64-bit) version 1607 or later (x86-64) Microsoft Windows 11 (64-bit) (x86-64)
Security Features	Support of all IPsec standards according to the RFC
Personal Firewall Firewall configuration	Stateful packet inspection IP-NAT (Network Address Translation) Differentiated filter rules for: Protocols, ports, applications and addresses, protection of the LAN adapter; IPv4 and IPv6 support; central administration Friendly Net Detection (automatic configuration of firewall rules when the connected network is detected using an NCP FND server [4]); Secure Hotspot login; Home Zone [2];
VPN Bypass [2]	The VPN bypass function allows you to define applications that are allowed to communicate directly via the Internet outside of the VPN connection despite disabling split tunneling. Alternatively, data communication outside the VPN tunnel can be permitted by domain or destination address.
Virtual Private Networking [3]	IPsec (Layer 3 tunneling), RFC-conformant; IKEv1/ IKEv2; Event log; Communication only in tunnel; MTU size fragmentation and reassembly; DPD; NAT traversal (NAT-T); IPsec tunnel mode
Encryption [3]	Symmetric encryption: AES 128, 192, 256 bits; Blowfish 128, 448 bits; Triple-DES 112, 168 bits; Dynamic methods for key exchange: RSA up to 8192 bits; Seamless Rekeying (PFS); Hash algorithms: SHA-1, SHA-256, SHA-384, SHA-512, MD5, DH group 1, 2, 5, 14-21, 25-30
Authentication Methods [3]	IKEv1 (Aggressive and Main Mode), Quick Mode; XAUTH for extended user authentication; IKEv2 IKE config mode for dynamic allocation of a virtual address from the internal address range (private IP); PFS; PAP, CHAP, MS CHAP V.2; IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): Extended authentication against switches and access points (Layer 2); EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): Extended authentication against switches and access points based on certificates (Layer 2); Support for certificates in a PKI: Soft certificates, smart cards, USB tokens and certificates with ECC technology Multi-certificate configuration; one-time passwords and challenge response systems (including RSA SecurID Ready)
Strong Authentication [3]	X.509 v.3 Standard; biometric authentication[2] PKCS#11 interface for encryption tokens (USB and smartcards); Smartcard Operating Systems: TeleSec TCOs 3.0 Signature Card Version 2.0 Release 1, Atos CardOS V5.3 QES, v1.0;

	Smartcard Reader Interfaces: PC/SC, CT API; Microsoft CSP; PKCS#12 Interface for private keys in soft certificates; CSP for using user certificates in the Windows certificate store; CSP for using smart cards via the manufacturer's API [7] PIN policy; administrative specification for entering arbitrarily complex PINs; Revocation: EPRL (End-entity Public-key Certificate Revocation List, form. CRL), CARL (Certification Authority Revocation List, form. ARL), OCSP
PKI Enrollment [2]	CMP (Certificate Management Protocol)
Networking Features	LAN emulation: Virtual Ethernet Adapter, Full WWAN Support (Wireless Wide Area Network, Mobile Broadband)
Network Protocols	IPv4 / IPv6 Dual Stack Support
Dialer [2]	NCP Internet Connector or Microsoft RAS Dialer (for ISP dial-up via dial-up script)
Seamless Roaming [2, 6]	Automatic transfer of the VPN tunnel to a different communication medium (LAN/Wi-Fi/3G/4G) without changing the IP address to avoid interrupting communication via the VPN tunnel or disconnecting application sessions.
VPN Path Finder [6]	NCP Path Finder Technology: Fallback to HTTPS from IPsec (port 443) if neither port 500 nor UDP encapsulation are available
IP Address Allocation	DHCP (Dynamic Host Control Protocol); DNS [2]: Selection of the central gateway with dynamic public IP address by querying the IP address via a DNS
Connection Media	Internet, LAN, WLAN, GSM (inc. HSCSD), GPRS, UMTS, LTE, HSDPA, 5G
Line Management	DPD with configurable time interval; Short Hold Mode; Timeout (time and fee controlled); Budget Manager (management of connection time and/or volume for GPRS/UMTS and WLAN, separate management for roaming abroad for GPRS/UMTS) Connection modes: automatic, manual, variable (The connection setup depends on the method of disconnection.)
APN from SIM card	The APN (Access Point Name) defines the access point of a provider for a mobile data connection. The APN data is automatically transferred from the respective SIM card to the client configuration during a provider change
Data Compression	IPCOMP (lzs), deflate (only for IKEv1)
Optional Features [3]	Automatic media recognition, UDP encapsulation, WISPr support (T-Mobile Hotspots), IPsec roaming or Wi-Fi roaming (Prerequisite: NCP (Virtual) Secure Enterprise VPN Server or NCP VS GovNet Server)
Point-to-Point Protocols	PPP over GSM, PPP over Ethernet, MLP, CCP, CHAP
Internet Society RFCs and Drafts	RFC 2401 –2409 (IPsec), RFC 3947 (Nat-T negotiations), RFC 3948 (UDP encapsulation), IP Security Architecture, ESP, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP, IKEv2 authentication according to

	RFC 7427 (padding method)
Client Monitor Intuitive GUI	Multilingual (German, English); Client Info Center; Configuration, connection control and monitoring, connection statistics, log files (colored display, simple copy and paste function); Internet availability test tool; Trace tool for fault diagnosis; Display of connection status; Integrated support for Mobile Connect Cards; Configuration and profile management with password protection, configuration parameter lock
Central Management	The following software versions or newer versions are a prerequisite for the operation and central management of the NCP VS GovNet Connector: NCP Secure Enterprise Management Server version 6.10 or higher NCP Management Console: Version 6.10 or later VS GovNet Connector Configuration Plugin: Version 2.20 or later License Plugin: Version 12.30 or later Firewall Plug-in: Version 12.30 or later PKI Enrollment Plug-in: Version 4.05 or later Endpoint Policy Plug-in: Version 4.00 or later

[1] For NATO RESTRICTED/ EU RESTRICTED compliance, the BSI requirements regarding the operating system used must be observed.

[2] This feature is not part of the BSI approval.

[3] For NATO RESTRICTED /EU RESTRICTED compliance, only the algorithms provided for this purpose and BSI approved solutions for NATO RESTRICTED/EU RESTRICTED compliant authentication may be used. Suitable authentication methods may include a smart card reader integrated into the terminal device or an external smart card reader with an integrated PIN pad, such as the REINER SCT cyberJack® RFID standard.

[4] The NCP Friendly Net Detection Server can be downloaded free of charge as an add-on here:
https://www.ncp-e.com/de/service/download-vpn-client/

[5] Prerequisite:
NCP Secure Enterprise VPN Server, NCP Virtual Secure Enterprise VPN Server or NCP VS GovNet Server,
NCP Secure Enterprise Management

[6] Prerequisite:
NCP Secure Enterprise VPN Server, NCP Virtual Secure Enterprise VPN Server or NCP VS GovNet Server

[7] To function correctly the manufacturer's smartcard API must be installed (Telesec TCOs Read Only Card Module for Microsoft SmartCard BaseCSP with ECC support V1.1.0.0; Atos CardOS API V5.5)

The German Federal Office for Information Security (BSI) approved the NCP VS GovNet Connector 2.20 on May 12, 2023 (BSI-VSA-10710).

A fully functional 30-day trial may be requested from: sales@ncp-e.com

NCP PATH FINDER®

NCP engineering GmbH
Dombuehler Str. 2
90449 Nuremberg
Germany

+49 911 9968 0
info@ncp-e.com
www.ncp-e.com

NCP engineering, Inc.
19321 US Highway 19 N, Suite 401
Clearwater, FL 33764
USA

+1 650 316 6273
info@ncp-e.com
www.ncp-e.com