# Data Sheet

## NCP VS GovNet Connector

for Windows

**Centrally administrable, software-based solution for enabling remote access to workstations that process classified information (VS-NfD or equivalent).**

- BSI certification (VS-NfD)
- NATO RESTRICTED and EU RESTRICTED
- Central management
- Self-checks to ensure integrity
- Network access control (endpoint policy)
- Manageable firewall
- Friendly Net Detection
- Hotspot Logon
- VPN Path Finder Technology (Fallback IPsec/HTTPS)
- Strong authentication
- Support for Wi-Fi and mobile communications
- Custom branding option

### Software-based Solution

NCP VS GovNet Connector provides a secure link between workstations that process classified data, i.e., data deemed for official use only (VS-NfD), and remote systems. It also complies with the guidelines for data classified as NATO RESTRICTED and EU RESTRICTED. 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 remains easy to use.

Based on the IPsec standard, highly secure data connections in compliance with the specifications of the Federal Office for Information Security (BSI) in Germany, can be established with the NCP Secure VPN GovNet Server.

Trust Seal www.teletrust.de/itsmig


Thanks to the support of standard interfaces, the software can be combined with other BSI-approved authentication hardware (e.g., smartcard readers) or software (e.g., hard disk encryption). NCP VS GovNet Connector also supports elliptic curve cryptography, a certificate verification method that is required by the BSI.

Users can access secure networks from anywhere in the world from computers running Microsoft Windows. The NCP VS GovNet Connector supports seamless roaming to automatically switch to the best available connection medium – ideal for always-on operation. Together with the NCP Secure VPN GovNet Server as a remote station, an application session with the GovNet Connector remains intact even during a media change or brief interruption.

### Self Check

The integrity service that comes with the VS GovNet Connector continuously monitors operating system components to assure they are working correctly. If the VS GovNet Connector is compromised, the terminal enters a secure state and blocks all communication. Furthermore, the integrity service supports secure remote updates to the VS GovNet Connector via central management.

NCP engineering GmbH
Dombuehler Str. 2
90449 Nuremberg, Germany

Phone: +49 911 9968 0

info@ncp-e.com
www.ncp-e.com

## VPN Path Finder Technology

NCP's patented VPN Path Finder Technology also enables remote access behind firewalls which block IPsec traffic. This is accomplished by automatically switching 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.

Cost-effective operation is also made possible by the budget manger included in the NCP VS GovNet Connector. 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 also optionally supports OTP solutions[3] (One Time Password), as well as biometric authentication, before the VPN connection is established, for example via fingerprint or facial recognition. The authentication process begins directly after the user clicks “Connect” in the connector GUI, 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.

## Network Access Control

The endpoint policy check prevents inadequately protected devices from accessing the secure central network. Here information about the status of a virus scanner, the domain affiliation, the status of the operating system, and other factors can be queried.

## 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 with or without a VPN connection. Additionally, the firewall of the NCP VS GovNet Connector is automatically enabled during the system startup of the computer.

## Friendly Net Detection

The Friendly Net Detection feature uses certificate-based authentication of the Friendly Net Detection Server in secure corporate or government networks to detect a secure network environment (Friendly Net). As a result, firewall rules configured in the VS GovNet Connector for the Friendly Net can be automatically activated when a friendly network is detected. This would be done, for example, to allow secure data exchange without a necessary VPN connection, or to allow administrative access to the device. Furthermore, the establishment of a VPN tunnel can be denied when the user is trying to do so from within the Friendly Network.

## Hotspot Logon

Often users are prevented from accessing Wi-Fi hotspots by security requirements that only permit communication through a VPN tunnel in insecure network environments, since this first requires accessing a login page via a web browser without a VPN tunnel.

This issue is resolved 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 via a dedicated, secure web browser together with 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). In principle, all settings in the NCP VS GovNet Connector can be locked by the administrator, preventing users from inadvertently or deliberately changing configurations. Beyond that, log files generated at the VS GovNet Connector, as well as the new audit log with all security-relevant incidents, are periodically transmitted to central management server for evaluation.

## Quality of Service

Through the Quality-of-Service feature, bandwidth for configured applications, such as Voice over Internet Protocol (VoIP), is reserved. The prioritization of selected data sources at the end user takes place for outgoing data transport in the VPN tunnel. For remote workers, this means stable VoIP communication through the VPN tunnel even with high data volumes.

## Custom Branding

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

| | |
|---|---|
| **Operating Systems** [1] | Microsoft Windows 10 (64-bit) version 1607 or later (x86-64)<br>Microsoft Windows 11 (64-bit) (x86-64) |
| **Security Features** | Support of all IPsec standards according to the RFC |
| Integrated Firewall<br>Firewall Configuration | Stateful packet inspection;<br>IP-NAT (network address translation);<br>differentiated filter rules for: Protocols, ports, applications and addresses, protection of the LAN adapter;<br>IPv4 and IPv6 support; central administration<br>Friendly Net Detection (automatic switchover of firewall rules when the connected network is detected using an NCP FND server [4]);<br>Secure Hotspot Logon;<br>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 tunnel despite disabling split tunneling. Alternatively, data communication outside the VPN tunnel can be permitted by the domain or destination address. |
| Virtual Private Networking [3] | IPsec (Layer 3 tunneling), RFC-conformant; IKEv1/ IKEv2;<br>Event log; Communication only in tunnel; MTU size fragmentation and reassembly;<br>DPD; NAT traversal (NAT-T); IPsec tunnel mode |
| Encryption [3] | Symmetric encryption:<br>AES 128, 192, 256 bits; Blowfish 128, 448 bits; Triple-DES 112, 168 bits;<br>Dynamic methods for key exchange:<br>RSA up to 8192 bits; Seamless Rekeying (PFS);<br>Hash algorithms:<br>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<br>IKE-Config mode for dynamic allocation of a virtual address from the internal address range (private IP); PFS;<br>PAP, CHAP, MS CHAP V.2;<br>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);<br>Support of certificates in a PKI: Soft certificates, smart cards, USB tokens and certificates with ECC technology<br>Multi-certificate configuration; one-time passwords and challenge response systems (including RSA SecurID Ready) |

| | |
|---|---|
| Strong Authentication [3] | X.509 v.3 Standard; biometric authentication<br>PKCS#11 interface for encryption tokens (USB and smartcards);<br>Smartcard Operating Systems: TeleSec TCOS 3.0 Signature Card Version 2.0 Release 1, Atos CardOS V5.3 QES, v1.0;<br>Smart Card Reader Interfaces: PC/SC, CT API; Microsoft CSP;<br>PKCS#12 Interface for private keys in soft certificates;<br>CSP for using user certificates in the Windows certificate store;<br>CSP for using smart cards via the manufacturer's API [7]<br>PIN policy; administrative specification for entering arbitrarily complex PINs;<br>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) |
| Network Access Control [5] | Endpoint policy: Checks current status of the virus scanner, existing hotfixes/service packs, services started, etc. |
| **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);<br>DNS [2]: Selection of the central gateway with dynamic public IP address by querying the IP address via 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);<br>Budget Manager (management of connection time and/or volume for GPRS/UMTS and WLAN, separate management for roaming abroad for GPRS/UMTS)<br>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) |

| | |
|---|---|
| **Quality of Service** | Outgoing bandwidth can be prioritized in the VPN tunnel. |
| **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 Secure VPN 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**<br>**Intuitive GUI** | Multilingual (German, English);<br>Client Info Center;<br>Configuration, connection control and monitoring, connection statistics, log files (colored display, simple copy and paste function);<br>Internet availability test tool;<br>Trace tool for fault diagnosis;<br>Display of connection status;<br>Integrated support for Mobile Connect Cards;<br>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:<br>• NCP Secure Enterprise Management Server version 6.00 or later<br>• NCP Management Console: Version 6.00 or later<br>• VS GovNet Connector Configuration Plugin: Version 2.10 or later<br>• License Plugin: Version 12.30 or later<br>• Firewall Plug-in: Version 12.30 or later<br>• PKI Enrollment Plug-in: Version 4.05 or later<br>• Endpoint Policy Plug-in: Version 4.00 or later |

[1] For VS-NfD-compliant operation, the BSI requirements regarding the operating system used must be observed.

[2] This feature is not part of the VS-NfD approval.

[3] For VS-NfD-compliant operation, only the algorithms provided for this purpose and BSI-compliant solutions for VS-NfD-compliant authentication may be used. For example by means of a smart card reader with an integrated PIN pad, such as the PURE 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 Secure VPN GovNet Server, NCP Secure Enterprise Management

[6] Prerequisite: NCP Secure Enterprise VPN Server, NCP Virtual Secure Enterprise VPN Server or NCP Secure VPN 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 Federal Office for Information Security (BSI) approved the NCP VS GovNet Connector 2.10 on November 30, 2021 (BSI-VSA-10599).*

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