Data Sheet

NCP Secure VPN GovNet Box

Secure Mobile Computing
According to VS-NfD Guidelines

- Hardened operating system
- Integrated firewall
- Transparent VPN tunnel
- Integrated smartcard reader
- Integrated capacitive PIN pad
- Optional data connections via LAN, Wi-Fi or mobile communication
- Support for Windows Domain Logon
- Easy to use and fast connection setup
- BSI certified (VS-NfD)

Bundesamt für Sicherheit in der Informationstechnik

Fraunhofer SIT

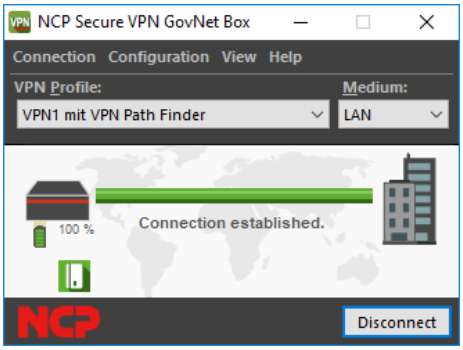
Universality and Communication

The NCP Secure VPN GovNet Box is a component of NCP's Next Generation Network Access Technology which is a comprehensive remote access VPN solution. Using a VPN connection, the box provides workstations handling classified information secure remote access to centrally stored applications and resources. The solution is suitable for use with information classified VS-NfD (classified material - for official use only).
Through a wired USB connection data is transmitted from the computer at the workstation to the NCP Secure VPN GovNet Box and from there to a configured remote station via secure VPN connection. For this VPN connection the NCP Secure VPN GovNet Box provides a connection optionally via LAN, Wi-Fi or mobile communication. All applications can be used such as Outlook or Voice over IP.

Since the data is not communicated through the Windows end device, the solution can be operated and maintained cost-effectively. The central remote side is the NCP Secure Enterprise VPN Server.

Security and Features

The NCP Secure GovNet box meets the highest security standards as well as the requirement of the German Federal Office for Information Security (BSI) for a "separation of security features from the client operating system". Additionally, the hardened operating system and a firewall protect both the box and the connected end device from cyberattacks. As the box is connected to the Windows system through USB, it can be bound using hardware attributes.



Caption: The NCP Secure GovNet Box monitor provides real-time information about connection and security status. Detailed log information ensures swift helpdesk support.

The VPN tunnel is managed through the USB connection in place, using an application which is

implemented on the user's computer: the NCP Secure VPN GovNet Box monitor. For strong user authentication before a VPN tunnel is established, the NCP Secure VPN GovNet Box is equipped with a smartcard reader and a capacitive keyboard ensuring that the PIN can be entered securely. The Windows domain logon is carried out by establishing a VPN connection prior to logon.

Central Management (in preparation)

Authentication, management and configuration are centrally performed with NCP's Secure Enterprise Management (SEM). Conveniently presented statistics inform IT administrators anytime about the status of the VPN connections.

Data Sheet

NCP Secure VPN GovNet Box

Supported PC operating systems	Windows 10, Windows 8.x, Windows 7
Operating system NCP GovNet Box	Hardened Linux operating system
Processor	Freescale i.MX53 CPU
PC interface	1 x mini USB interface for data transmission and power supply
Integrated internet interfaces	10 / 100 Mbit Base-T Ethernet interface Wi-Fi module (b/g/n standard) with 2.4 and 5 GHz 3G module (HSDPA+)
Smartcard interface	Integrated smartcard reader according to ID-1 standard (check card)
Supported smartcards	▪ Atos CardOS 5.0 ▪ G&D Sm@rtCafé Expert Version 5.0 ▪ Telesec TCOS 3.0 Signature Card Version 2.0
PIN pad	Integrated capacitive keyboard with backlight for PIN entry
LED panels	Integrated LEDs indicating the VPN, Wi-Fi or 3G connection status
Measurements and Weight	11 x 8 x 3.6cm and 250g
Accessories	LAN cable, power cable, USB cable
BSI certificate number	BSI-Z-VSA-10280, expires 07/2020
Conformity	CE, RoHS, WEEE

Security Features	
Personal Firewall	Stateful packet filter to protect the connected PC
Virtual Private Networking	IPsec (Layer 3 Tunneling) ▪ IPsec Tunnel Mode ▪ Transparent tunnel for the connected device (no NAT or routing required) ▪ Message transfer unit (MTU) size fragmentation and reassembly ▪ Network address translation traversal (NAT-T) ▪ Dead Peer Detection (DPD)

Data Sheet

NCP Secure VPN GovNet Box

Encryption	Symmetric: AES 128, 256 bit; Asymmetric: RSA 2048 bit, for dynamic key exchange Seamless rekeying Hash / message authentication algorithms: ▪ SHA-256 ▪ Diffie-Hellman Group 14 for asymmetric key exchange and PFS
Authentication Processes	Up-to-date Internet Key Exchange Protocol (IKEv2): ▪ Perfect Forward Secrecy (PFS) ▪ Dynamic assignment of IP address and DNS server ▪ RSA signature (with corresponding public key infrastructure) Automatic user authentication via smartcard (user name transmission by smartcard)
Secure Configuration	Configuration encryption at the device
Secure Domain Logon	The security measures of the GovNet Box take effect already during the booting process, even before the Windows logon. User ID and password for the domain controller can be entered directly via Windows Credential Provider without prior login at the local client. An encrypted VPN tunnel secures data transmission
PC Binding	Optionally, the GovNet Box can be used with a specified Windows end device
Client Monitor **Intuitive graphical user interface**	▪ User Interface: English, German ▪ Setup, online support and license: German, English Icon for the connection status indicator Password protected configuration and profile management Display of error messages and information Option of starting the monitor as full screen or icon after system start
BSI Certification	Certificate: Secure VPN GovNet Box, Version 10.11 BSI-VSA-10163