# Release Notes

# NCP Secure Entry Client (Win32/64)

**Service Release: 9.24 Build 84**
**Date: July 2011**

## 1. New Features and Enhancements

The following features and enhancements are included in this release:

### IKEv2 Implementation

As the Internet Key Exchange Protocol Version 2 (IKEv2), including the Mobility Extensions (MOBIKE), is now implemented in the Client's base, the Secure Client is now compatible with the latest versions of IPsec gateways such as Microsoft Windows Server 2008 R2.
Selection of the alternatives IKEv1 or IKEv2 is configured in the Client's profile settings under the rubric "IPsec General Settings / Exchange Mode". The options available via this pulldown-menu are:

- main mode (IKEv1) [this is the default value selected at profile creation]
- aggressive mode (IKEv1)
- IKEv2

If the Internet Key Exchange protocol version 2 (IKEv2) is selected, the Microsoft CHAP version 2 (MS-CHAP v2) authentication protocol is used.

### Evaluation of the Transferred Sub CA Certificate during IKE Negotiations

If the CA Certificate is transferred during the IKE negotiations, this is subsequently used in the certificate checking process. This means that this CA Certificate no longer has to be stored in the Client's installation directory. The Root Certificate must always be available at the Client.

### Evaluation of Extended Key Usages.

During an IKE negotiation the following Ext. Key Usages will now be accepted:

- id-kp-ipsecIKE (1.3.6.1.5.5.7.3.17) - RFC 4945
- anyExtendedKeyUsage (2.5.29.37.0) - RFC 4945
- IKEIntermediate (1.3.6.1.5.5.8.2.2) in acordance with draft-ietf-ipsec-pki-req-03

### Tolerance Behavior during Unstable Connections

If a wireless Internet connection (3G, Wi-Fi) breaks or is temporarily interrupted, the established VPN tunnel will be maintained until reconnection of the physical connection. This is indicated by means of a yellow Tunnel Status graphical field in the Client's monitor. The physical connection can only be interrupted for a period of time as long as the DPD Interval duration set in the gateway.
If the DPD functionality is disabled in the Client profile under "Advanced IPsec Options" the gateway also no longer sends DPD packets, meaning that the setting in the gateway no longer has any effect.

### Connection Establishment via Hotkey

Connections can be established and disconnected by using the Hotkey [Alt] + [c] (German [Alt] + [v]).

## 2. Problems Resolved

The following problems have been resolved:

### "Frozen" VPN Client after Standby Mode

When the computer was restarted from Standby, the NCP VPN Client was "frozen" - a deadlock had occurred. When the Client is restarted from Standby and "variable" Connection Mode is selected, the Client will attempt to re-establish a connection but this can be hindered by the recognition of 3G hardware in the Windows device manager.
The problem has been cured by delaying the start of connection establishment when the Client is configured in "automatic" or "variable" Connection Mode.

### Modem not found (VPN tunnel not established)

When the computer was restarted from Standby, the NCP VPN Client displayed "Modem not found‟ if 3G hardware was being used. Changes to the lower levels of the NCP VPN Client mean that the new 3G hardware is now supported. As negotiation of the Access Point Network (APN) takes place during connection establishment to the 3G network of the provider, a repeat negotiation of the APN during establishment of the 3G link can be omitted. Connection establishment to a 3G network is now a few seconds faster.

### DNS Request to the wrong DNS server

In order to ensure the correct functioning of the NCP VPN Client, the NCP network adapter must be the first to connect to the Windows Vista TCP/IP stack. After every start of the computer the NCP VPN Client checks the binding of the NCP adapter to the TCP/IP stack and, if necessary, puts the NCP adapter in the first position. However, this check does not takes place after the exit from Standby Mode, and, for this reason, despite deactivating Split Tunneling, a DNS request could bypass the VPN tunnel.

### Malfunction of Split Tunneling, Automatic Media Recognition and 3G

In profiles with Automatic Media Recognition and the 3G option, Split Tunneling was not carried out correctly and all packets were sent via the tunnel.

### Incorrect status display after VP connection established

The monitor of the NCP Secure Entry Client GUI uses animation to illustrate the status of connection establishment, and this establishment status is also displayed in the associated Tray icon. Although a VPN connection was already successfully established, a thin yellow line and a red lamp were displayed in the monitor and the Tray icon respectively. This malfunction occurred when a VPN profile required a connection to be established with an ISDN link. The animation has been corrected. Cause was the absence of the CAPI interface in the system.

### Malfunction during NAS Authentication

If a Client password of more than 19 characters was configured in a Client, the NAS Authentication would fail. The encryption function has been modified and enhanced with a conversion function.

**BSOD in Windows 7**

If the name of the service entered in the service part of the registry was longer than 64 characters, this caused a "Blue screen" during the NCP driver's scan process.

**The following problems associated with the use of certificates have been resolved.**

In the certificate assistant dialog, if a search for P11 modules found a P11 module without a manufacturer, this module could not be selected.

**VPN Tunneling when the Firewall is configured in "Basic Locked Settings"**

Setting the Firewall's "Basic Settings" to "Basic Locked Settings" is designed to be an easy way to open the Firewall exclusively to VPN Tunneling. A switch was included in the Firewall "Configuration" / "Firewall" / "Options" that globally permits (or inhibits) the passage of IPsec or VPN Path Finder traffic through the Firewall. However, the rule activated automatically in the background also permitted traffic from other tools (browsers, mail programs) to communicate via port 443. This rule has now been modified such that this is no longer possible.

## 3. Known Issues

None

## 4. Getting Help for the NCP Secure Entry Client (Win32/64)

To ensure that you always have the latest information about NCP's products, always check the NCP website at:
http://www.ncp-e.com/en/downloads.html

For further assistance with the NCP Secure Entry Client (Win32/64), visit:
http://www.ncp-e.com/en/about-us/contact.html

Mail: mailto:helpdesk@ncp-e.com?subject=A:%20NCP%20Secure%20Entry%20Client%20-%20Helpdesk%20message%20

## 5. Features

### Operating Systems

Microsoft Windows (32 & 64 bit): Windows 7, Windows Vista, Windows XP

### Security Features

Support of the Internet Society's Security Architecture for IPsec and all the associated RFCs.

#### Virtual Private Networking

- RFC conformant IPsec (Layer 3 Tunneling)
  - IPsec Tunnel Mode
  - IPsec proposals are negotiated via the IPsec gateway (IKE Phase 1, IPsec Phase 2)
  - Communication only in the tunnel
  - Message Transfer Unit (MTU) size fragmentation and reassembly
  - Network Address Translation-Traversal (NAT-T)
  - Dead Peer Detection (DPD)

#### Authentication

- Internet Key Exchange (IKE):
  - aggressive mode and main mode, Quick Mode
  - IKEv2
  - Perfect Forward Secrecy (PFS)
  - IKE Config. Mode for dynamic allocation of private IP (virtual) address from address pool
  - Pre-shared secrets or RSA Signatures (and associated Public Key Infrastructure)
- User authentication:
  - User Authentication via GINA/Credential Management
    - Windows Logon over VPN connection
  - XAUTH for extended user authentication
    - One-time passwords and challenge response systems
    - Authentication details from certificate (prerequisite PKI)
- Support for certificates in a PKI:
  - Soft certificates, Smart cards, and USB tokens: Multi Certificate Configurations
- Seamless rekeying (PFS)
- PAP, CHAP, MS CHAP v.2
- Pre-Authentication (Authentication before VPN establishment)
- IEEE 802.1x:
  - Extensible Authentication Protocol – Message Digest 5 (EAP-MD5): Extended authentication relative to switches and access points (layer 2)
  - Extensible Authentication Protocol – Transport Layer Security (EAP-TLS): Extended authentication relative to switches and access points on the basis of certificates (layer 2)
  - Extensible Authentication Protocol – Transport Layer Security (MS-CHAP v2): Extended authentication relative to switches and access points on the basis of certificates using IKEv2 (layer 2)
- Secure hotspot logon using HTTP or EAP
- RSA SecurID ready

## Encryption and Encryption Algorithms

| | |
|---|---|
| Symmetrical: | AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits |
| Asymmetrical: | RSA to 2048 bits, dynamic processes for key exchange |

Seamless Rekeying (Perfect Forward Secrecy)

## Hash / Message Authentication Algorithms

- SHA1, SHA-256, SHA-384, SHA-512, MD5
- Diffie Hellman groups 1, 2, 5, 14 used for asymmetric key exchange and PFS

## Public Key Infrastructure (PKI) - Strong Authentication

- X.509 v.3 Standard
- Entrust ready
- Support for certificates in a PKI
  - Smart cards and USB tokens
    - PKCS#11 interface for encryption tokens (smart cards and USB)
    - Smart card operating systems
      - TCOS 1.2, 2.0 and 3.0
    - Smart card reader systems
      - PC/SC, CT-API
    - Soft certificates
      - PKCS#12 interface for private keys in soft certificates
- PIN policy: administrative specification of PIN entry to any level of complexity
- Certificate Status Protocol (CSP) for the use of user certificates in the Windows certificate store
- Revocation:
  - End-entity Public-key Certificate Revocation List (EPRL formerly CRL)
  - Certification Authority Revocation List, (CARL formerly ARL)
  - Online Certificate Status Protocol (OCSP)
  - Certificate Management Protocol (CMP)[i]

## Personal Firewall

- Stateful Packet Inspection
- IP-NAT (Network Address Translation)
- Friendly Net Detection (Firewall rules adapted automatically if connected network recognized based on its IP subnet address, the DHCP server's MAC address or an NCP FND server[i])
- Supports secure hotspot logon feature
- Start application before or after VPN establishment
- Differentiated filter rules relative to:
  - Protocols, ports or IP addresses
  - LAN adapter protection,
- Protect VMware Guest systems

## Networking Features

### Secure Network Interface

- LAN Emulation
  - NCP Virtual Ethernet adapter with NDIS interface
  - Wireless Local Area Network (WLAN) support
  - Wireless Wide Area Network (WWAN) support

### Network Protocol

- IP

### Communications Media

- LAN
- Wi-Fi
- GPRS / 3G (UMTS, HSDPA), GSM (incl. HSCSD)
- xDSL (PPPoE)
- xDSL (PPP over CAPI, AVM)
- PSTN
- ISDN
- Automatic Media Detection (AMD)
- External Dialer

### Dialers

- NCP Secure Dialer
- Microsoft RAS Dialer (for ISP dial-up using dial-up script)

### Line Management

- Dead Peer Detection with configurable time interval
- Short Hold Mode
- Inactivity Timeout (send, receive or bi-directional)
- Channel Bundling (dynamic in ISDN) with freely configurable threshold value
- Wi-Fi Roaming (handover)
- Budget Manager
  - Separate management of Wi-Fi, GPRS/3G, xDSL, PPTP, ISDN and modem connections
  - Duration or volume based budgets
  - Management of GPRS/3G roaming costs
  - Separate management of multiple Wi-Fi access points

### IP Address Allocation

- Dynamic Host Control Protocol (DHCP)
- Domain Name Service (DNS): gateway selection using public IP address allocated by querying DNS server

### VPN Path Finder

- NCP Path Finder Technology

  - Fallback to HTTPS (port 443) from IPsec if neither port 500 nor UDP encapsulation are available [ii]

### Data Compression

- IPsec Compression: lzs, deflate

### Link Firewall

- Stateful Packet Inspection

### Additional Features

- VoIP prioritization
- UDP encapsulation
- IPsec roaming [ii]
- Wi-Fi roaming [ii]
- WISPr support (T-Mobile hotspots)

### Point-to-Point Protocols

- PPP over Ethernet
- PPP over GSM,
- PPP over ISDN,
- PPP over PSTN,
  - LCP, IPCP, MLP, CCP, PAP, CHAP, ECP

## Standards Conformance

### Internet Society RFCs and Drafts

Security Architecture for the Internet Protocol and assoc. RFCs (RFC2401 - 2409),

- Internet Key Exchange Protocol (includes IKMP/Oakley) (RFC 2406),
- Negotiation of NAT-Traversal in the IKE (RFC 3947),
- UDP encapsulation of IPsec Packets (RFC 3948),
- IKE Extended Authentication (XAUTH), IKE configure (IKECFG) and Dead Peer Detection (DPD)
- Additional Extended Key Usages:
  - id-kp-ipsecIKE (1.3.6.1.5.5.7.3.17) in accordance with RFC 4945
  - anyExtendedKeyUsage (2.5.29.37.0) in accordance with RFC 4945
  - IKEIntermediate (1.3.6.1.5.5.8.2.2) in accordance with draft-ietf-IPsec-pki-req-03

### FIPS Inside

The Secure Client incorporates cryptographic algorithms conformant to the FIPS standard. The embedded cryptographic module incorporating these algorithms has been validated as conformant to FIPS 140-2 (certificate #1051).

FIPS conformance will always be maintained when any of the following algorithms are used for establishment and encryption of the IPsec connection:

- Diffie Hellman Group: Group 2 or higher (DH starting from a length of 1024 Bit)
- Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit
- Encryption Algorithms: AES with 128, 192 or 256 Bit or Triple DES

## Client Monitor

### Intuitive Graphical User Interface

- Language support (English, German, French)
    - Monitor & Setup: en, de, fr
    - Online Help and License en, de
- Icon indicates connection status
- Client Info Center – overview of::
    - General information - version#, MAC address etc
    - Connection – current status
    - Services/applications – process(es) – status
    - Certificate Configuration – PKI certificates in use etc.
- Configuration, connection statistics, Log-book (color coded, easy copy&paste function)
- Integrated support of Mobile Connect Cards (PCMCIA, embedded)
- Password protected configuration and profile management
- Trace tool for error diagnosis
- Monitor can be tailored to include company name or support information
- Tip of the Day
- Hotkey connection establishment and disconnection

Notes

[i] If you wish to download NCP's FND server as an add-on, please click here:
http://www.ncp-e.com/en/downloads/software.html

[ii] Prerequisite: NCP Secure Enterprise Server V 8.0 and later

More information on the NCP Secure Entry Client (Win32/64) is available on the Internet at:
http://www.ncp-e.com/en/products/ipsec-client.html

Test it for free: download a free, 30-day full version of the NCP Secure Entry Client (Win32/64) from NCP's website:
http://www.ncp-e.com/en/downloads/software.html