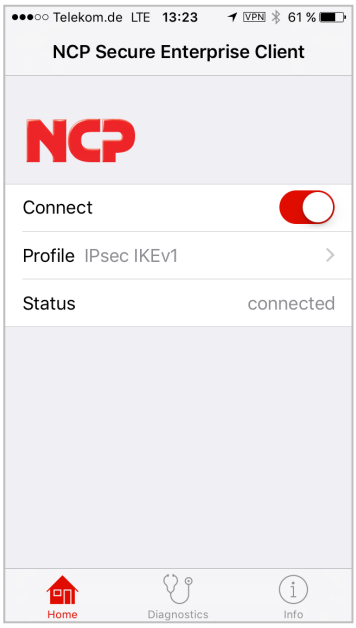
Data Sheet

NCP Secure Enterprise iOS Client

Centrally managed VPN client for Apple iOS

- Central configuration and certificate rollout via NCP Secure Enterprise Management
- NCP load balancing support
- Fallback IPsec / HTTPS (VPN Path Finder Technology)
- iOS keychain support
- FIPS Inside
- Strong Authentication, Touch ID support
- VPN On Demand



Universal integration and secure communication

The NCP Secure Enterprise iOS Client enables a highly secure VPN connection to the central data networks of companies and organizations. It can access multiple data networks, each with their own VPN profile. VPN On Demand sets up the VPN tunnel automatically and ensures that it is used exclusively for communication.

NCP VPN Path Finder Technology facilitates remote access even behind firewalls or proxies that block VPN traffic.

Enhanced security

The strong authentication of the NCP Secure Enterprise iOS Client offers comprehensive protection against remote access by unauthorized third parties. It uses certificates that are stored in an exclusive area of the iOS keychain for the NCP Secure Enterprise iOS Client. VPN connections can also be secured to require authentication via fingerprint sensor (Touch ID). The cryptography module is certified in accordance with section G5 of the Implementation Guidance for FIPS 140-2 (certificate #1747).

Efficiency

The NCP Secure Enterprise iOS Client is designed for excellent usability. Details on connection status, certificates, network environment and a log export feature are clearly displayed in the client UI. This efficiency is reflected in low training costs, less user documentation and quick support.

Central Management

The NCP Secure Enterprise iOS Client is optimized for central administration with NCP Secure Enterprise Management (SEM). User configurations and certificate updates can be managed centrally with SEM. Clients are set up with a minimal configuration for connecting to SEM and can then download custom configurations and certificates from SEM. The user is not able to view the assigned configuration.

Prerequisites	iOS 11.x and higher; NCP Secure Enterprise VPN Server 11.0; NCP Secure Enterprise Management Server 4.05
Central Management	Distribution of VPN configuration and certificates via NCP Secure Enterprise Management
Virtual Private Networking	IPsec (Layer 3 tunneling), RFC-conformant; Event log; Communication only in tunnel or split tunneling; DPD; NAT traversal (NAT-T); IPsec Tunnel Mode
Encryption	*Symmetric encryption:* AES-CBC 128, 192, 256 Bit; AES-CTR 128, 192, 256 Bit; AES-GCM 128, 256 bits (IKEv2 only); Blowfish 128, 448 bit; Triple-DES 112, 168 bit; SEED *Dynamic methods for key exchange:* RSA up to 4096 bits; ECDSA up to 521 bits; Seamless Rekeying (PFS); Hash algorithms: SHA, SHA-256, SHA-384, SHA-512, MD5, DH group 1, 2, 5, 14-21, 25-30
FIPS Inside	The NCP Secure Enterprise iOS client integrates cryptographic algorithms based on the FIPS standard. The cryptography module that includes these algorithms is certified in accordance with section G5 of the Implementation Guidance for FIPS 140-2 (certificate #1747). FIPS conformance will always be maintained when the following algorithms are used for set up and encryption of a VPN connection: ▪ DH Group: Group 2 or higher (DH starting from a length of 1024 bits) ▪ Hash algorithms: SHA1, SHA 256, SHA 384 or SHA 512 bits ▪ Encryption algorithms: AES 128, 192 and 256 bits or Triple DES
Key exchange procedure	IKEv1 (Aggressive and Main Mode Pre-shared key, RSA, XAUTH IKEv2 Pre-shared key, RSA, EAP-MS CHAPv2, EAP-MD5, EAP-TLS, EAP-PAP, signature authentication (RFC 7427), IKEv2 fragmentation (RFC 7383)
User Authentication	XAUTH or EAP with optional input of user name and password before manual VPN tunnel setup; User certificate in iOS keychain; Touch ID for user authentication before manual VPN tunnel setup.
VPN Path Finder	NCP Path Finder Technology fallback to HTTPS from IPsec (port 443) if neither port 500 nor UDP encapsulation are available
IP Address Assignment	DHCP; IKE Config mode (IKEv1); Config Payload (IKEv2)

Line Management	Dead Peer Detection (DPD) with configurable time interval; Timeout; VPN On Demand sets up the VPN tunnel automatically and ensures that it is used exclusively for communication.
Data Compression	Deflate
Optional Features	UDP encapsulation;
Internet Society RFCs and Drafts	RFC 4301 (IPsec), RFC 4303 ESP, RFC 3947 (Nat-T negotiations), RFC 3948 (UDP encapsulation), IKEv1, RFC 3526, ISAKMP, RFC 7296 (IKEv2), RFC 4555 (MOBIKE), RFC 5685 (Redirect), RFC 7383 (Fragmentation), RFC 7427 , 3279 Section 2.2.3, 3447 Section 8 (Signature Authentication), RFC 5903, 6954, 6989, 4754 (ECC), RFC 2451, 3686 (AES with ESP), 5930 (AES-CTR), 4106 (AES-GCM), 5282, 6379 (Suite B), RFC 3447 Section 8 (Padding)
Client GUI Intuitive UI	German, English; Configuration update; Profile selection; Connection control and monitoring, connection statistics, log files; Fault diagnosis export; Network information, 3D touch
Download	Download NCP Secure Enterprise iOS Client for free from Apple's App Store. Please contact us at ios-client@ncp-e.com if you would like to test the software.

FIPS 140-2 Inside

NCP engineering GmbH
Dombühler Straße 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