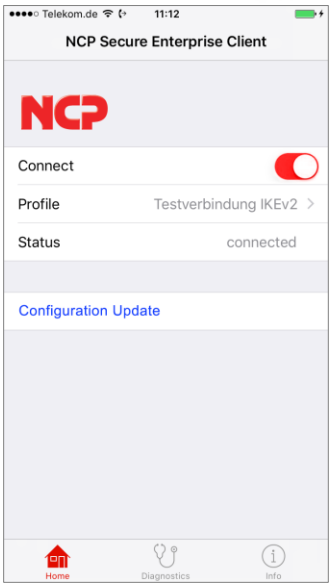
Data Sheet

NCP Secure Enterprise iOS Client

Centrally Administered
VPN Client for Apple iOS 9 & 10

- Central Management and central 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



Universally Applicable

The NCP Secure Enterprise iOS VPN Client enables a highly secure Virtual Private Network (VPN) connection to the corporate networks of companies or organizations. Access to multiple networks is supported, each connection has its own VPN profile.
Using standard IPsec protocols, connections can be established from tablets and smartphones to NCP VPN gateways.

NCP VPN Path Finder Technology enables remote access even when the device is located behind firewalls or proxies that would otherwise hinder the establishment of an IPsec tunnel.

Security

The strong authentication of the NCP Secure Enterprise iOS VPN Client provides comprehensive protection against access by unauthorized third parties. Data encryption: support for OTP (One Time Password) tokens and certificates in a PKI (Public Key Infrastructure).
Certificates that are stored in an exclusive area of the iOS key chain for the NCP Secure Enterprise iOS Client are supported.

In addition, establishing a VPN connection can be secured using authentication via the fingerprint sensor (Touch ID).
The embedded cryptographic module is validated according to FIPS 140-2 (Certificate #1747), Implementation Guidance section G.5.

Usability and Cost Effectiveness

The intuitive, graphical user interface not only makes NCP Secure iOS Clients "easy to use", but also keeps the user continuously updated on the state and security level of the connection, both while the VPN is established and while it is disconnected.
Detailed logs help to ensure rapid support from the helpdesk in the event of unforeseen problems. Usability, in turn, means cost savings as less training and documentation are required, and the load on the helpdesk is reduced.

Central Management

The NCP Secure Enterprise iOS VPN Client is optimized for management by NCP's Secure Enterprise Management (SEM). SEM incorporates extensive Endpoint Security capabilities which can be integrated, for example, in the central management and distribution of user configurations and certificate updates.

For the initial set-up the client is pre-configured with a minimum configuration and the individual configuration is deployed by SEM. After that, the user will not be able to gain access to the assigned configuration.

Americas: NCP engineering, Inc. · 678 Georgia Ave. · Sunnyvale, CA 94085 · Phone: +1 (650) 316-6273 · www.ncp-e.com
Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Fon +49 911 9968-0 · Fax +49 911 9968-299

Data Sheet

NCP Secure Enterprise iOS Client

Operating Systems	iOS 9.3 and above; NCP Secure Enterprise VPN Server 11.0; NCP Secure Enterprise Management Server 4.05
Central Management	Distribution of VPN configurations and certificates from the NCP Secure Enterprise Management
Virtual Private Networking	IPsec (Layer 3 Tunneling), RFC conformant; Event log; Communication only in tunnel; DPD; NAT-Traversal (NAT-T); IPsec Tunnel Mode
Encryption	*Symmetric processes:* AES-CBC 128, 192, 256 Bit; AES-CTR 128, 192, 256 Bit; AES-GCM 128, 256 Bit (only IKEv2); Blowfish 128, 448 Bit; Triple-DES 112, 168 Bit; SEED *Dynamic processes for key exchange*: RSA to 4096 bits; ECDSA to 521 bit; Seamless Rekeying (PFS); Hash Algorithms: SHA-256, SHA-384, SHA-512, MD5, DH Groups 1, 2, 5, 14-18, 19-21, 25, 26
FIPS Inside	The NCP Secure Enterprise iOS Client uses an embedded FIPS 140-2-validated cryptographic module (Certificate #1747) running on an Android platform per FIPS 140-2 Implementation Guidance section G.5 guidelines. 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 bits) ▪ Hash Algorithms: SHA1, SHA 256, SHA 384 or SHA 512 bits ▪ Encryption Algorithms: AES with 128, 192 or 256 bits or Triple DES
Authentication Process	IKEv1 (Aggressive and Main Mode) Pre-shared key, RSA, XAUTH IKEv2 Pre-shared key, RSA, EAP, Signature Authentication (RFC 7427), IKEv2 Fragmentation (RFC 7383)
Strong authentication	iOS Keychain for using User (Soft) Certificates Touch ID

Data Sheet

NCP Secure Enterprise iOS Client

VPN Path Finder	NCP VPN Path Finder Technology, Fallback IPsec /HTTPS (Port 443) when port 500 or UDP encapsulation cannot be used (prerequisite: NCP VPN Path Finder Technology required at the VPN Gateway
IP Address Assignment	DHCP; IKE Config Mode (IKEv1); Config Payload (IKEv2)
Line Management	DPD (Dead Peer Detection) with configurable polling interval; Timeout; VPN On Demand
Data Compression	Deflate
Other 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 Monitor **Intuitive GUI**	English, German; Configuration update; Connection control and management, connection statistics, log files; trace tool for error diagnosis; 3Touch
Download and trial	Download the NCP Secure Enterprise iOS Client for free at the Apple app store. For testing purposes please contact NCP engineering at ios-client@ncp-e.com.

FIPS 140-2 Inside

Next Generation Network Access Technology