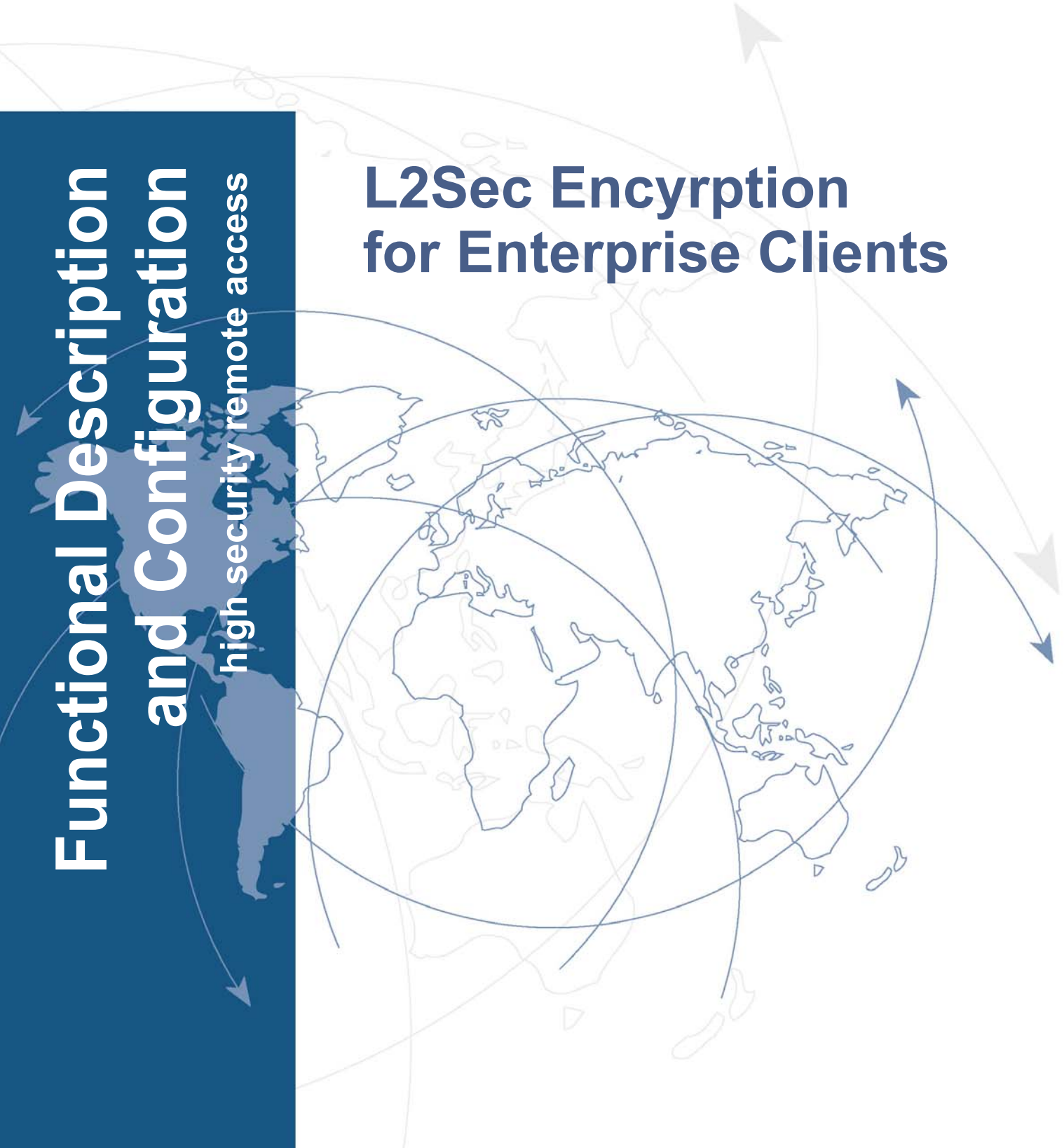


# Functional Description and Configuration

high security remote access

## L2Sec Encyrption for Enterprise Clients



# L2Sec Encryption for Enterprise Clients



This document describes the L2Sec Encryption, which is only supported by the Enterprise Client.

## Configuration Settings



In the parameter field **Security** all the configuration parameters for L2Sec and IPSec for the application in remote access environments are collected.



L2Sec can be used when **L2TP** has been selected as VPN protocol in the configuration field **VPN Tunneling**.

The security mode “L2Sec” was always used as the standard in earlier versions of the secure software. All security negotiations are carried out encoded and secure in an end-to-end tunnel (layer 2) between client and secure server.



## Encryption Type L2Sec (RFC 2716)

Experience with many VPN projects has shown that generally two situations must be accommodated. On the one hand there are a large number of distributed PC workstations to be connected to the central enterprise. On the other hand, in addition to IP; IX, SNA, and NetBios data packets (native) must be also transmitted.

Appropriate authentication of the communication participants is vital for the security of projected communication networks – especially during the establishment of the connection. Authentication becomes even more significant with the increase in the number of employees dialing into the enterprise over the Internet or other public networks from telecommuting workstations or mobile offices.

NCP implemented L2Sec in order to eliminate the weaknesses of IPSec and at the same time respond to enterprise demands regarding open systems. >From a security and communications perspective L2Sec constitutes the only real alternative to IPSec. L2Sec combines the advantages of L2TP with authentication and encryption in accordance with SSL (TLS). This protocol is specified in RFC 2716 (Microsoft). NCP was not only the first manufacturer to implement L2Sec long before the RFC was published, we also have successfully responded to the needs of countless major enterprises, organizations, and government agencies that were disillusioned with the inadequacies IPSec.

## L2Sec Functional Description

With L2Sec PPP security negotiations occur as soon as a channel is established to the central system, this is a Layer 2 connection with security. Layer 2 channels can be ISDN, B-channel, a modem-connection, or a tunnel (L2TP). With the NCP VPN Tunneling solution all negotiation steps are encrypted and secure in an end-to-end tunnel between the client and the VPN gateway.

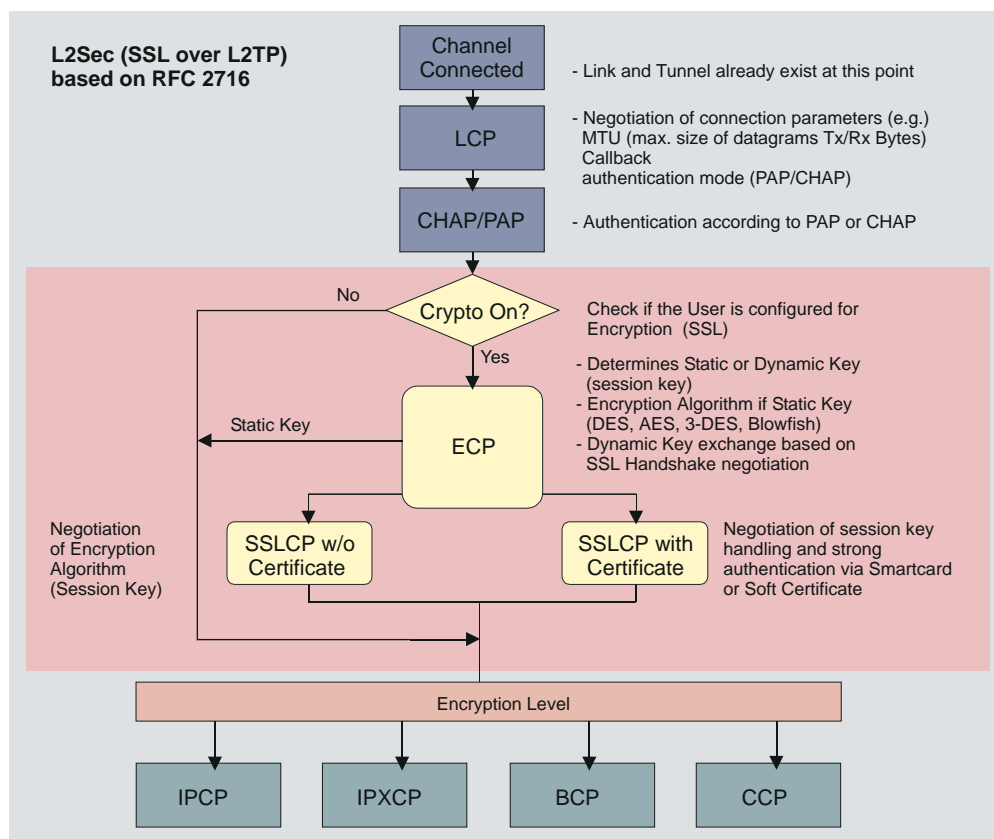
This assures that data communication via the end-to-end tunnel in a virtual private network is completely independent from the communications environment. The tunnel thus constructed offers the participants a secret passage through a public network running between the remote VPN client and the central VPN gateway.

The complete IP data packet, consisting of payload and IP header, is encrypted for the transmission and given a new heading. In other words even the original IP source and destination addresses undergo encryption, an enormous security benefit.

As many IP routers as desired from different manufacturers can be installed between the VPN client and the VPN gateway on the segment of the NCP end-to-end tunnel. These require neither data compression functionality nor tunnel protocols.

This represents a protection of your investment and a pure open architecture because network access servers from internet service providers as well as your installed routers and those of your business partners and of your business partners can be integrated in the virtual private network.

In this way NCP Secure Software offers a universal security infrastructure that permits the simple integration of your desired business applications. Also dependable encryption management is insured, as is the connection of Certificate Authorities (CAs).



LCP = Link Control Protocol

IPCP = Internet Protocol Control Protocol

CHAP = Challenge Authentication Protocol

IPXCP = Internetwork Packet Exchange Control Protocol

PAP = Password Authentication Protocol

ECP = Encryption Control Protocol

BCP = Bridge Control Protocol

SSLCP = Secure Socket Layer Control Protocol

CCP = Compression Control Protocol

L2Sec = Layer 2 Security functionally described in RFC 2716



## Copyright

*Considerable care has been taken in the preparation and publication of this manual, errors in content, typographical or otherwise may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP as desired.*

*NCP makes no representations or warranties with respect to the contents or use of this manual, and explicitly disclaims all expressed or implied warranties of merchantability or use for any particular purpose.*

*Furthermore NCP reserves the right to revise this publication and to make amendments to the content, at any time, without obligation to notify any person or entity of such revisions and changes. This manual is the sole property of NCP and may not be copied for resale, commercial distribution or translated to another language without the express written permission of NCP engineering GmbH.*

*All trademarks or registered trademarks appearing in this manual belong to their respective owners.*

© NCP engineering GmbH,  
March 2009

Network  
Communications  
Products engineering GmbH

GERMANY  
Headquarters:  
Dombühler Straße 2  
D-90449 Nürnberg  
Tel.: +49-911-99680  
Fax: +49 - 911 - 9968 299  
internet  
<http://www.ncp-e.com/en>  
E-mail: [info@ncp-e.com](mailto:info@ncp-e.com)