

WHITEPAPER



SECURE COMMUNICATIONS ■

PRESENTS

AN INTRODUCTION

To

SECURE VIRTUAL PRIVATE NETWORKING

Important Notice

The information in this document is furnished for informational use only and is subject to change without notice.

NCP assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

No part of this publication may be reproduced, published, stored in an electronic database, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, for any purpose, without the prior written permission of NCP.

Trademarks

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

Executive Summary

This document is intended to provide an overview of the NCP Secure Communications Virtual Private Networking solution.

For those who may be unfamiliar with the concept of VPN, a VPN (Virtual Private Network) is a private connection between two or more machines that sends private data traffic over a shared or public network, for example the Internet. This technology enables organizations, for example, to extend their network to branch offices and remote users by creating a private WAN (Wide Area Network) via the Internet.

The appeal of a VPN is the global presence of the Internet. Communication links can be made quickly, cheaply, and safely across the world. An especially attractive feature is that an organization can have all the services except for guaranteed Quality of Service, and avoid the need to install and maintain a global infrastructure.

A recent article in America's Network magazine made the following comment. "One of the fastest growing trends in remote access is outsourcing all or part of a corporate network via service providers' virtual private network (VPN) services. VPNs are in the early stages of adoption, but provide tantalizing benefits to customers and carriers—among them, security features, quality of service (QoS)-like protocols, and significant cost savings over pure leased lines."

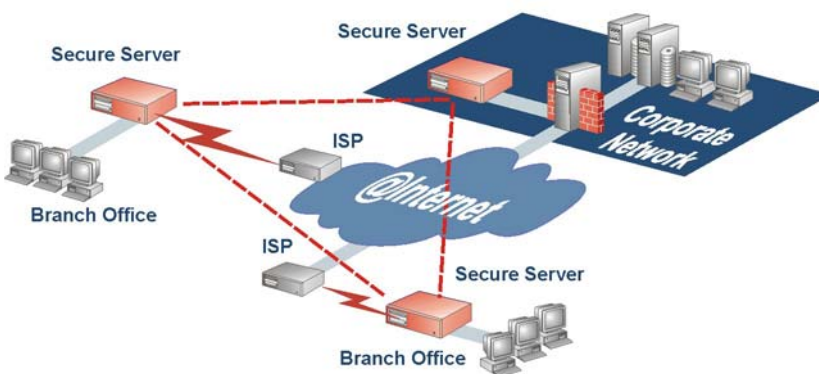
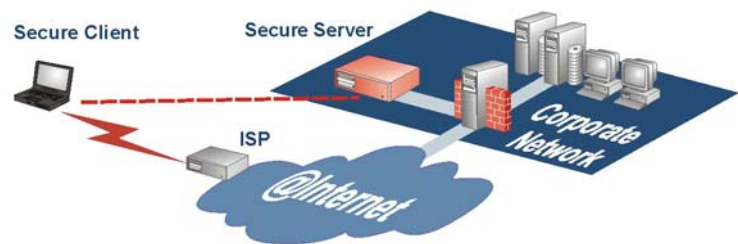
The adoption rate in the US market where traditionally communication costs are much lower than in Europe is exploding. According to the November 2nd 2000 issue of Internet World, the "U.S. market for IP-based virtual private network (VPN) services is expected to sky-rocket from \$224.1 million this year to more than \$13 billion in the year 2004."

The Frost & Sullivan report on VPNs cited "cost savings, the ability to set up networks quickly, and increased IP expertise as reasons for the growth of IP VPNs in the near term." However one of the most interesting statements in the report states: "Later on, advancements in security software and improved tunneling standards will further boost VPN sales, according to the report."

The Application Of Virtual Private Network Technology

VPN technology can be applied in many different models, tailored to an organization's specific needs. One of the most common applications is the provision of remote access to business resources over the Internet, as shown below.

Instead of calling directly into a central site, the user calls a local ISP. Using the connection to the local ISP, a second, virtual connection is established to the central site, which will be connected to the Internet.



Another very common model is to build a VPN to interconnect business locations. This will be done using either dedicated connections such as leased lines, or dial-up connections, depending on the type of connectivity required.

The motivation for deploying VPN technology will vary according to the organization, for example cost saving by eliminating the need to maintain costly long-distance connections, alleviating

management tasks by outsourcing the network backbone maintenance to a third party, improving performance through the utilization of “end-to-end” techniques such as data compression, and security through the use of authentication techniques, and encryption.

A VPN must therefore provide certain fundamental features such as:

- **Authentication.** The means whereby a user's or an organization's identity is protected, and VPN access is restricted to authorized users only. Included in this must be auditing and accounting functionality.
- **Data Encryption.** Data that is being transported on public networks must be secured against the “man-in-the-middle” attacks, and be unreadable to unauthorized organizations or individuals.
- **Key Management.** When Authentication and Data Encryption are being used, effective Key Management is essential to ensure that security is not compromised.
- **Multi-protocol Support.** The VPN should be capable of supporting the common protocols used in today's corporate environment, such as TCP/IP and IPX/SPX, but also support more exotic protocols such as SNA, NetBEUI, and NetBIOS.

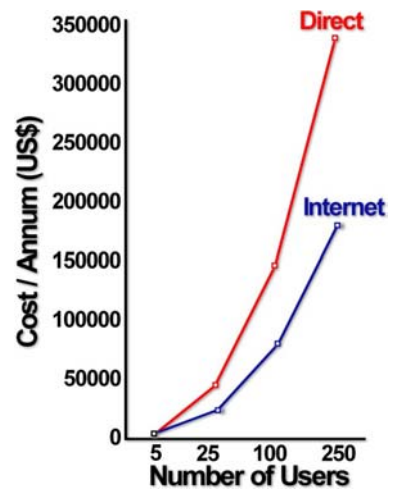
Private Networks and The Internet

Although private networks would appear to offer better security, this has more to do with the users' perception than reality. This however is a totally false sense of security since whether on private leased lines, or the Internet, unsecured data is visible to the Service Providers, be they the Internet Service Providers (ISPs), or the traditional Telcos.

Private networks are often used to provide the organization with the capability of enhancing performance, using facilities such as data compression, callback, managing access control, and also the freedom to transport data that is to a large extent protocol independent. Many corporate networks still use protocols such as Novell's IPX/SPX, Microsoft's NetBIOS, NetBEUI, and IBM's SNA/SDLC, LU6.2, in addition to TCP/IP which is the platform on which Internet connectivity is built.

Meanwhile the Internet offers significant saving in operating costs. Take, for example the situation as shown here in the graph of the annual communication costs, which represents dial-up costs for companies in Europe. The figures are based on actual PTT tariffs between two cities in one European country, and these tariffs are relatively similar throughout Europe.

Using the Internet for corporate traffic will result in major savings, even taking into account the initial investment required in VPN technology. Even companies with 10 or more teleworkers could expect to see an ROI within 6 to 9 months of operation.

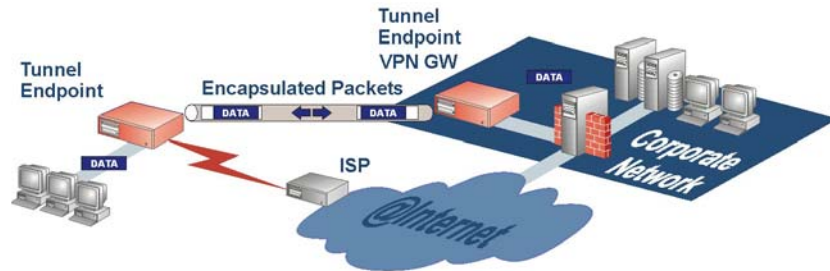


What Is A Virtual Private Network

Before proceeding to taking a closer look at the NCP's position, it is perhaps useful to first look at some of the terminology, and goals of VPNs.

A virtual private network (VPN) maintains privacy through the use of a tunneling protocol and security procedures.

Tunneling allows the use of an existing infrastructure to transfer data for one network over another network (carrier). The data being transferred can be frames or packets from the same protocol that forms the basis of the carrier



network, or another protocol. The data from the originating device is encapsulated in the tunnel protocol, and an additional header provides the necessary routing information so that the carrier network can deliver the encapsulated data to the required endpoint.

Encapsulated packets are routed between tunnel endpoints over the carrier network. The logical path the encapsulated packets travel through is called a tunnel. When the encapsulated frames reach their destination on the carrier network, the frame is unencapsulated and forwarded to the final destination. Tunneling thus provides for the entire process (encapsulation, transmission, and unencapsulation of packets).

The carrier network can be any public network, for example the Internet, the example that is most often used as the real world example, but in reality can be any value added network service.

The concept of tunneling is not new. Many Router manufacturers have supported tunneling for many years, with numerous examples of SNA and IPX protocols being tunneled in many networks. During the past few years, a number of new tunneling protocols have been introduced.

Layer 2 Forwarding (L2F) – RFC 2341

L2F was a technology proposed by Cisco, and still used in many environments, particularly Cisco networks. L2F permits the tunneling of the link layer (i.e., HDLC, asynchronous HDLC, or SLIP frames) of higher-level protocols. Using such tunnels, it is possible to divorce the location of the initial dial-up server from the location at which the dial-up protocol connection is terminated and access to the network provided.

Layer 2 Tunneling Protocol (L2TP) – RFC 2661

L2TP is a combination of PPTP and L2F. The objective was to integrate the best features of PPTP and L2F. The protocol encapsulates PPP frames to be sent over carrier networks. When configured to use IP as its carrier transport, L2TP can be used as a tunneling protocol over the Internet. L2TP can also be used directly over various networks, such as Frame Relay, without an IP transport layer.

Over IP carrier networks, L2TP uses UDP and a series of L2TP messages for tunnel maintenance. L2TP also uses UDP to send L2TP-encapsulated PPP frames as the tunneled data. The data is encapsulated in PPP frames, and can be encrypted and/or compressed.

IPSec – RFC 2401-2409

Short for IP Security, IPSec defines a set of protocols to support secure exchange of packets at the IP layer. It is designed to provide security for IP traffic, for example to secure a TCP connection, and is designed with network routers, and gateways in mind. A complex security negotiation is performed between the tunnel endpoints through the Internet Key Exchange (IKE), normally using PKI certificates for authentication.

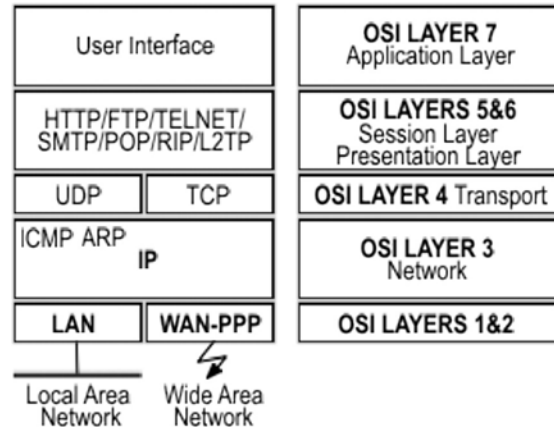
One of the major strengths of IPSec is that it is the first tunneling protocol that specifically addresses the issue of encryption and authentication, based on international standards. IP packets sent by an

IPSec host to a protected network are encrypted and delivered to the security gateway for that network. For IPSec to work, the sending and receiving devices must share a public-key, which allows the receiver to obtain a public-key and authenticate the sender using digital certificates.

IPSec uses packet headers, called Authentication Headers (AH), to validate users and Encapsulating Security Payloads (ESP) to encrypt data, and supports multiple concurrent remote-access links, so that a user can maintain one connection to the corporate LAN and another to the public Internet.

Extensible Authentication Protocol (EAP) – RFC 2716

EAP is an IETF-proposed extension to PPP that allows for arbitrary authentication mechanisms for the validation of a PPP connection, the standard basis by which most devices connect to the Internet. EAP was designed to allow the dynamic addition of authentication plug-in modules at both the client and server ends of a connection. This allows vendors to supply a new authentication scheme at any time. EAP provides the highest flexibility in authentication uniqueness and variation. EAP is implemented in Microsoft Windows 2000 and onwards.

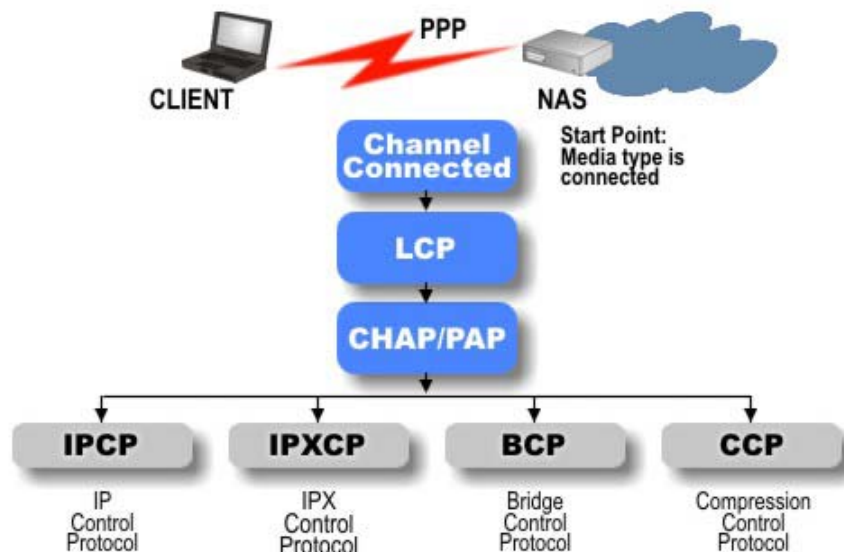


The Point-To-Point Protocol (RFC 1661)

To try and put all these standards in perspective, and to understand how it all fits together, it is useful to look at the PPP protocol.

Today, connection to the Internet, regardless of the device used, is governed by a protocol called PPP, or Point-to-Point Protocol.

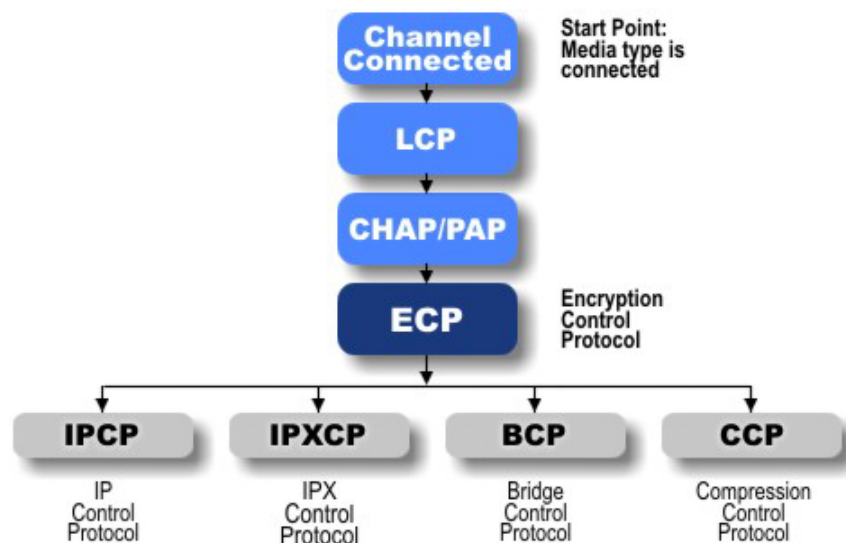
The Point-to-Point Protocol is designed for simple links, which transport packets between two peers. These links provide full-duplex simultaneous bi-directional operation, and are assumed to deliver packets in order.



The PPP encapsulation provides for multiplexing of different network-layer protocols simultaneously over the same link, for example, IP, IPX, SNA, and others.

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP also defines an extensible Link Control Protocol (LCP), which can be used to negotiate authentication methods, as well as an Encryption Control Protocol (ECP), used to negotiate data encryption over PPP links, and a Compression Control Protocol (CCP), used to negotiate compression methods.

Additionally PPP provides many other functions, such as Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP, an encrypted authentication mechanism that avoids transmission of the actual password on the connection, Callback Control, Network Address Translation (NAT), Multilink, and other features.



Encryption Control Protocol (RFC 1968)

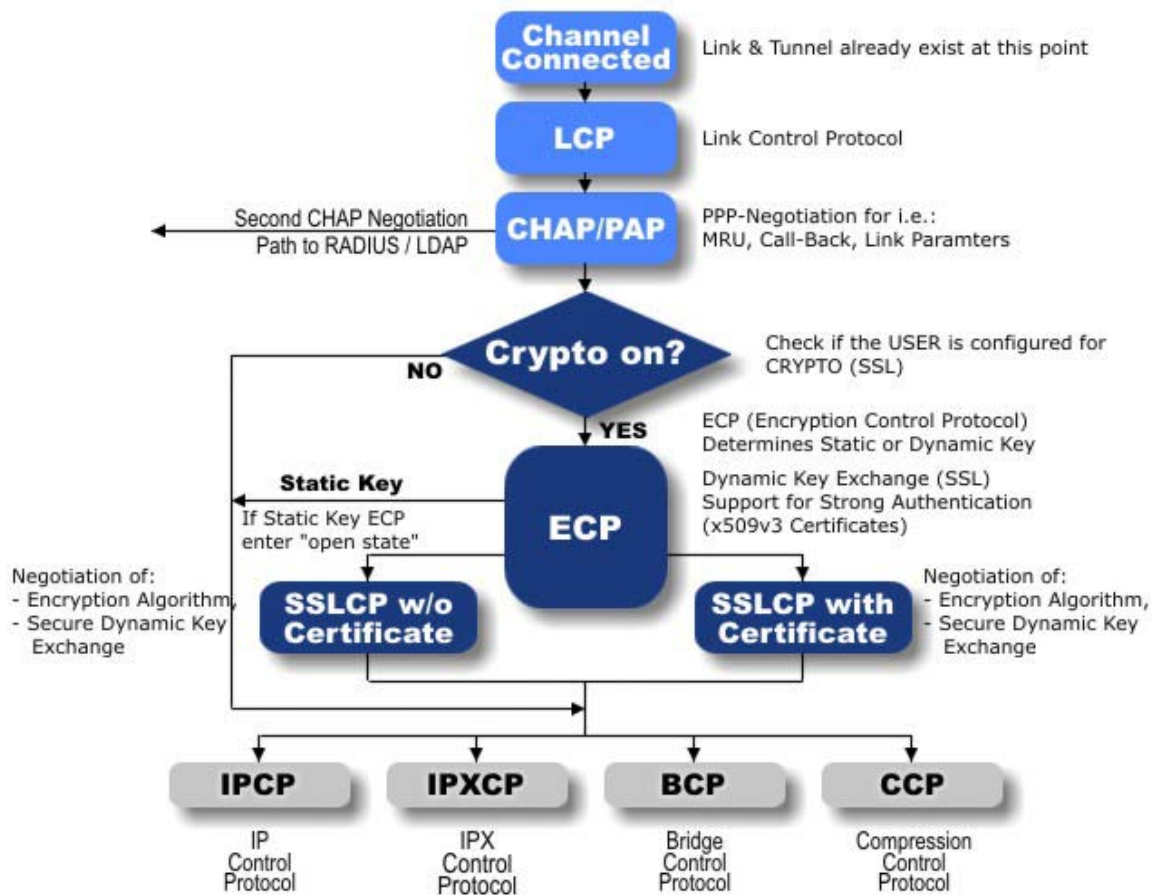
In order to establish communications over a PPP link, each end of the link must first send LCP packets to configure and test the data link during the Link Establishment phase. After the link has been established, optional facilities may be negotiated as needed.

The Encryption Control Protocol (ECP) is responsible for configuring and enabling data encryption algorithms on both ends of the point-to-point link.

PPP EAP TLS Authentication Protocol (RFC 2716) – L2Sec

Transport Level Security (TLS), based on the SSL 3.0 Protocol Specification as published by Netscape, provides for mutual authentication, integrity-protected cipher suite negotiation and key exchange between two endpoints. EAP-TLS has been submitted to the IETF as a draft proposal for a strong authentication method based on public-key certificates. With EAP-TLS, a client presents a user certificate to the dial-in server, and the server presents a server certificate to the client. This approach follows the standard, which has become the de-facto in the application world, more commonly known as a Public-Key Infrastructure.

See illustration on the following page.



Which Approach?

In our view, the overriding concern in today's market is security, followed by performance. One only has to consider the support being received by IPsec to realize that the market demands security. Studies conducted by Internetweek Research (<http://www.internetwk.com/VPN/VPNcharts.htm>), showed that 90% of IT Managers responding, rated Security as their primary concern, followed by 79% rating Performance. The remaining concerns or criteria in descending order where, Management Tools, Configuration Tools, Ability to use Existing Management Tools, Client Deployment, and finally Interoperability.

Within the industry there is an ongoing discussion related to IPsec. For example in an article in America's Network magazine, VPN industry leaders express very different opinions. "The vendors that are IPsec alone are going to be left in a very difficult spot.", Greg Marcotte, Altiga Networks; "IPsec is the ideal. For one thing, it's a standard.", Robert McKinney, GTE; "IPsec is great for security, but as far as dealing with native IP addresses and some of the issues with regard to address management—address translation and so forth – the technical answer is that L2TP and PPTP are better in those types of environments." Jonathan Cohen, AT&T.

According to Robert Moskowitz, co-chair of the IETF's IPsec Workgroup, speaking about the keep-alive problem, (this results in one IPsec VPN device not detecting the loss of connection with another VPN device, and continue to broadcast data), was quoted as saying that during recent meetings "Other issues, such as proper configuration of IPsec clients and network address translation, took precedence", and in reference to the keep-alive problem, he stated: "The answer is that we don't know

the best way to do it." (<http://www.idg.com.au/network/>). Additionally incompatibilities between IKE and NAT, mean that passing IPsec through typical NATs cannot be implemented.

Having said that, PPTP and L2TP don't measure up either. The PPTP protocol is only really of any use in a Microsoft environment, and L2TP in spite of its flexibility in terms of network integration and protocol support offers no effective answer for security. The result then is that if anything IPsec, rather than solving the issue, in the short term, of standardization of VPN technology, has generated a frenzy of inventions, whether IPsec over L2TP or vice-versa.

Comparing technologies

Where does it all stand today? In some of these cases, work is in progress where the feature is not supported, particularly in the IPSec arena.

Feature	Description	PPTP	L2TP	IPSec	L2Sec
User Authentication	<i>Can authenticate the user that is initiating the communications.</i>	Yes	Yes	No	Yes
NAT Capable	<i>Can pass through Network Address Translators to hide one or both end-points of the communications.</i>	Yes	Yes	No	Yes
Multiprotocol Support	<i>Defines a standard method for carrying IP and non-IP traffic.</i>	Yes	Yes	No	Yes
Dynamic Tunnel IP Address Assignment	<i>Defines a standard way to negotiate an IP address for the tunneled part of the communications.</i>	Yes	Yes	N/A	Yes
Encryption	<i>Can encrypt traffic it carries.</i>	Limited	No	Yes	Yes
Uses PKI	<i>Can use PKI to implement encryption and/or authentication.</i>	No	No	Yes	Yes
Packet Authenticity	<i>Provides an authenticity method to ensure packet content is not changed in transit.</i>	No	No	Yes	Yes
Multicast support	<i>Can carry IP multicast traffic in addition to IP unicast traffic.</i>	Yes	Yes	No	Yes
NCP Secure Communications	<i>Support Status.</i>	No	Yes	Yes	Yes

PKI – The Missing Link

The discussion which has focused the attention of VPN suppliers, and Service Providers - which VPN technology is the best – has until now avoided confronting a key issue, namely Public-Key Infrastructure (PKI). A fundamental component of both IPsec, and EAP-TLS is the use of certificates in the authentication and encryption process.

Cryptography

In order to better understand PKI, a quick introduction to cryptography is needed. Cryptography, i.e. encryption of information for protection and decryption of information to make it intelligible to applications and people, is the basis for all four of the basic security services. There are two kinds of cryptography in common use: *symmetric* and *public-key cryptography*.

Symmetric cryptography, in which a single key is used both to encrypt and decrypt information, offers the advantage of a conceptually simple architecture: Just distribute a key to both ends of the connection. However, distributing symmetric keys raises a “chicken and egg” problem: how to implement strong security for key distribution, when strong security depends on having keys.

Public-key cryptography uses pairs of keys, each pair consisting of one public-key and one private key. Information encrypted with one key in the pair can only be decrypted with the other key. Thus, to have a secure connection to a VPN Gateway, the VPN Client must encrypt the data with VPN Gateway’s public-key. The VPN Gateway then decrypts the data with its private key, which only it has access to. Public-key cryptography solves the key distribution problem because public-keys are not secret and can be distributed over non-secured networks, while private keys do not need to be distributed. Since only the owner of a private key needs to have it, the private key can be generated on the machine where it is used. NCP’s mission is to enable secure and efficient VPN transactions by complementing standard PKI solutions through a combination of leading-edge technology, extensive systems integration skills and industry partnerships. NCP’s early sales and partner successes confirm the company’s ability to deliver a reliable, robust security solution that enables banks, and other private and public enterprises, to conduct business securely over the Internet.

Public-Key Infrastructure (PKI)

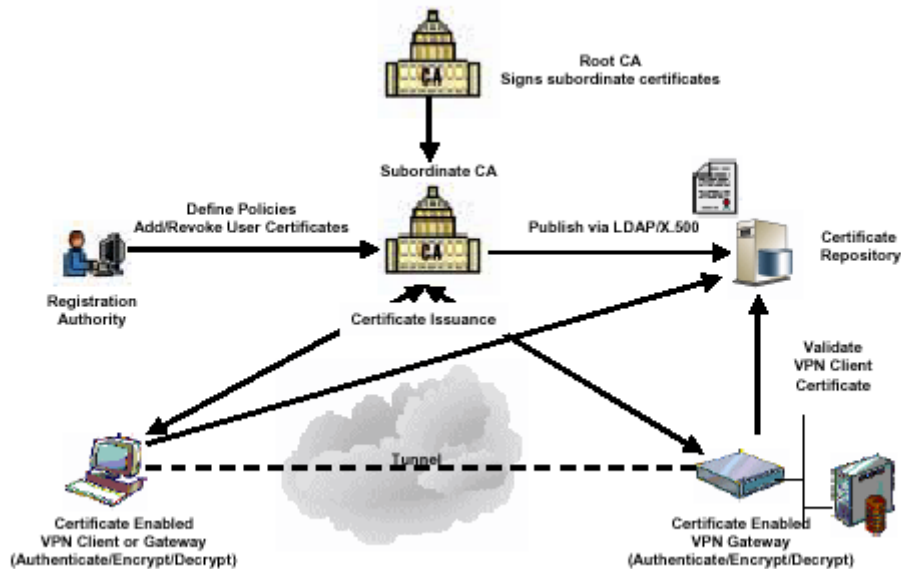
Public-key cryptography requires a means of validating public-keys, that is, proving that a particular public-key belongs to a particular user. For instance, if a message is encrypted with the wrong public-key, a user other than the intended recipient will be able to decrypt it, and the intended user will not be able to decrypt it. *Certificates* provide the validation function, which links a particular public key to a particular user. There are two types of certificates: *soft certificates* that are stored on magnetic media, such as hard disks, and *hard certificates* that are stored in hardware devices, such as smartcards or USB cryptographic devices.

The infrastructure that provides the necessary components for managing (e.g. issuing, revoking, validating) public-keys and certificates is called a public-key infrastructure (PKI). There are three core PKI components:

The *Certification Authority (CA)* issues certificates. The CA function can be provided either by in-house servers running X.500 directory software from a vendor such as Baltimore, Entrust, RSA or even Certification Services in the Windows 2000 Advanced Server, or externally by a third party service provider such as VeriSign, Globalsign or DST. The CA is responsible for storing the certificate and guaranteeing its validity, much like an issuer of an ID card or driver’s license. As part of the certificate validation function, the server checks a certificate revocation list (CRL) to make sure that the administrator has not revoked the certificate.

The *Registration Authority (RA)* facilitates user registration and accepts requests for certificates, which it forwards to the CA. The RA may be implemented as part of the CA, or it may be a separate piece of software. There can be multiple RAs for a single CA. Conversely, a single RA can access multiple CAs. The idea with the RA is to keep the validation process close to the user, while forwarding only certificate signing requests to a central, secure CA.

The *repository* stores public-keys, certificates and Certificate Revocation Lists (CRLs). It is usually based on a Lightweight Directory Access Protocol (LDAP)-compatible directory service. Using LDAP results in a more scalable and access-friendly directory service than a native X.500 directory.



Thus, the PKI provides the essential services for managing digital certificates and encryption keys for the people, programs and systems that use public-key cryptography. On top of the PKI are layered applications, such as VPN, client-based security devices such as smartcards, tokens and biometrics.

It is possible to manage a small number of passwords and encryption keys manually, without a PKI. However, as the number of passwords and keys grows, manual management becomes burdensome, and the need for a PKI becomes apparent. VPN applications in an Internet-based community requiring authentication and encryption services may also argue strongly for a PKI. The PKI makes it possible to manage just one public/private key pair and one certificate per user for all applications. Without a PKI, each user typically has a password/key for each application, and passwords and keys must be managed from within each application. Multiple passwords, keys and user interfaces tend to be burdensome. For instance, they make it more difficult to renew or revoke a given user's credentials.

Thus, in order to scale a system based on public-key cryptography, companies typically build or outsource a PKI. Initially, this involves either setting up an in-house CA or else establishing a relationship with a commercial CA service provider such as VeriSign or Globalsign.

When IPSec, and EAP-TLS tunnels are created, the VPN endpoints can authenticate each other with digital certificates. The use of digital certificates is considerably more scalable than shared secrets. It is no longer necessary to issue a unique pair of secrets for every pair of VPN devices. Each device has just one digital certificate. In addition it is also not necessary to reconfigure all other devices every time a new device is added to the VPN. Instead, by making certificates available to every device through a public directory such as Lightweight Directory Access Protocol (LDAP), it means that if companies want to interconnect VPNs, the existing certificates, issued by different CAs can cross-certify each other.

NCP's Approach

NCP's approach has been to support a range of tunneling protocols, particularly L2F (historical), L2TP, IPSec, and since early 1999, what we refer to as L2Sec, but more commonly referred to as RFC2716, fully integrated in a PKI environment.

In common with most IPSec vendors, we support a standard mode and a NCP proprietary mode, in order to alleviate the shortcomings of the specification. Based on the market requirements, we agree with the pragmatic approach of the market that is to say that it is pointless at this stage to become religious about one or the other.

The NCP VPN & PKI suite enables the highest level of security, i.e. user authentication based on PKI, which protects VPN communications, encryption based on international standards, with no restrictions, and no compromise in performance.

The NCP VPN functionality is best described as a multi-layer security with built-in PKI encryption technology. This means everything passing through the VPN is encrypted, regardless what protocol is being used. NCP VPN supports TCP/IP protocols as well as layer 2 protocols, such as IPX, NetBEUI, and SNA. This secure multi-layer connectivity makes NCP VPN one of the most complete security products on the market today.

Software Only

The NCP Secure Communications suite consists of two different products: NCP Secure Client Software and NCP Secure Server Software. Both products can be obtained in three security levels: Standard Security, Advanced Security, and Strong Security. The Client Enterprise version and the Server Bridging module provide the additional communication protocols NetBEUI and SNA.

The Products

NCP Secure Client (Remote Client for ISDN/PSTN/GSM/Ethernet/Broadband access)

- Based on Ethernet LAN emulation and supports TCP/IP and IPX/SPX protocols *)
- Support for LDAP and RADIUS authentication
- Remote Configuration and Monitoring

The NCP Secure Enterprise Client includes the same features but is

- Based on Token Ring LAN emulation and supports TCP/IP, IPX/SPX, SNA, and NetBEUI protocols

NCP Secure Server (Remote Access Server)

- Support for LDAP/RADIUS authentication
- Supports TCP/IP, IPX/SPX, SNA, and NetBEUI protocols
- Supports communications via ISDN, PSTN (modem), GSM V.110, UMTS, Ethernet, Broadband
- Authentication and encryption based on CHAP/PAP, 3DES, Blowfish, AES128/192/256, SSL (RFC2716)
- SNMP (& SNMP over SSL) based GUI for remote administration and configuration
- SNMP Compliant – managed via Tivoli, HP Openview, etc. (MIB II files provided)

The Security Levels

Both the Client and the Server can be obtained in three security levels:

NCP Standard Security

- Authentication and encryption based on CHAP/PAP, 3DES, Blowfish, AES128/192/256, SSL (RFC2716)

NCP Advanced Security

- Authentication and encryption based on CHAP/PAP, 3DES, Blowfish, AES128/192/256, SSL (RFC2716)

- Includes support for VPN tunneling: L2F, L2TP, EAP-TLS and IPSec

NCP Strong Security

- Authentication and encryption based on CHAP/PAP, 3DES, Blowfish, AES128/192/256, SSL (RFC2716) with Certificate exchange
- Includes support for VPN tunneling: L2F, L2TP, EAP-TLS and IPSec
- Dynamic revocation checking – X.509 based. Supports all commercial CA products and TTPs
- Support for smart cards and USB cryptographic devices (PKCS#11 compliant)
- CRL and OCSP Support