

# 6 Commonly Used Security Packages: PKI, VPN, SSL, PGP and Kerberos

6.1	INTRODUCTION.....	6-1
6.2	INTERRELATIONSHIPS BETWEEN TECHNOLOGIES, CONSUMERS, RESEARCHERS, AND SUPPLIERS.....	6-3
6.3	CERTIFYING AUTHORITIES AND THE PUBLIC KEY INFRASTRUCTURE (PKI) .....	6-4
6.3.1	<i>What is PKI and Why is it Needed?</i> .....	6-4
6.3.2	<i>Certifying Authorities (CAs)</i> .....	6-5
6.3.3	<i>PKI Versus CA Services – Practical Issues</i> .....	6-7
6.3.4	<i>Entrust – A Commercial PKI Product</i> .....	6-7
6.3.5	<i>Verisign – An Outsourcing Certificate Authority (CA)</i> .....	6-7
6.3.6	<i>Players in PKI – Standards and Technology Providers</i> .....	6-7
6.4	SECURE SOCKET LAYER (SSL) FOR WEB SECURITY.....	6-8
6.4.1	<i>What is SSL?</i> .....	6-8
6.4.2	<i>How SSL Works</i> .....	6-10
6.5	VIRTUAL PRIVATE NETWORKS (VPNS ) AND IPSEC .....	6-12
6.5.1	<i>Virtual Private Networks (VPNs)</i> .....	6-12
6.5.2	<i>IPSec</i> .....	6-13
6.6	PGP (PRETTY GOOD PRIVACY).....	6-16
6.7	KERBEROS .....	6-17
6.8	OTHER PACKAGES AND CONCLUDING COMMENTS.....	6-19
6.9	SHORT CASE STUDIES AND EXAMPLES .....	6-19
6.9.1	<i>Prudential/BT Managed PKI</i> .....	6-19
6.9.2	<i>Global Public Key Infrastructure (PKI) for Least Developed Countries</i> .....	6-20
6.9.3	<i>Utilities Choose PGP Encryption Over S/MIME</i> .....	6-21
6.10	SUGGESTED REVIEW QUESTIONS.....	6-22
6.11	PART II – NRW CASE STUDY REVISITED: CHOOSING ENABLING SECURITY TECHNOLOGIES AS COUNTERMEASURES.....	6-23

## 6.1 Introduction

In the previous two chapters, we discussed cryptographic and authentication, authorization, accountability and availability techniques. In reality, if you want to secure a system, you do not purchase individual technologies and then try to build a security solution. Instead, numerous security packages are commercially available at present that integrate different security technologies. The following list provides some examples:

- PKI (Public Key Infrastructure) is an extensive collection of security technologies (encryption, digital signatures, digital certificates) for a wide range of applications. However, due to its extensive capabilities, PKI is somewhat difficult to use.
- SSL (Secure Socket Layer) is the de facto standard for securing the traffic between Web clients and Web servers. SSL uses encryption, digital certificates, and digital signatures.
- IPSec is a standard used in Virtual Private Networks (VPNs) to encrypt and decrypt IP packets on the Internet. By using VPNs, customers can get a secure path over the public Internet by encrypting the IP traffic.
- PGP (Pretty Good Privacy) provides encryption and digital signature services. PGP is used commonly to protect email. Free and commercial versions of PGP are available.
- Kerberos is an open standard designed to provide strong authentication by using secret-key cryptography.

These packages provide slightly different security services and operate at different levels of the system. Figure 6-1 shows the various levels at which these packages operate. For example, many packages (PKI, PGP, Kerberos) are used to support security at the application level. SSL operates at the middleware level to support Web traffic, while IPSec and VPN protect the physical network traffic.

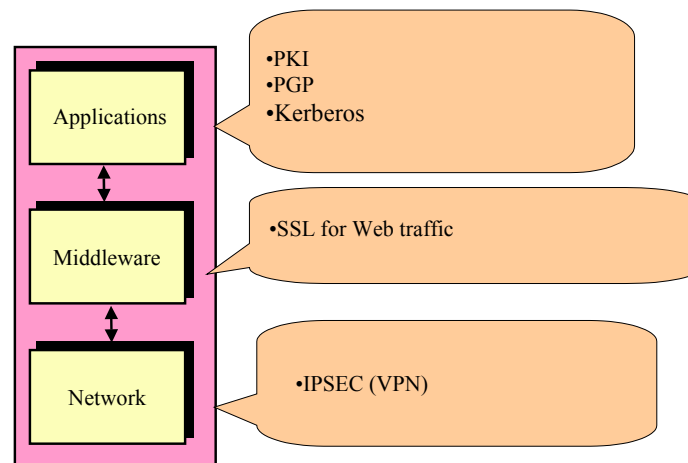


Figure 6-1: Security Technologies at Different Layers – A Starter Checklist

### Chapter Highlights

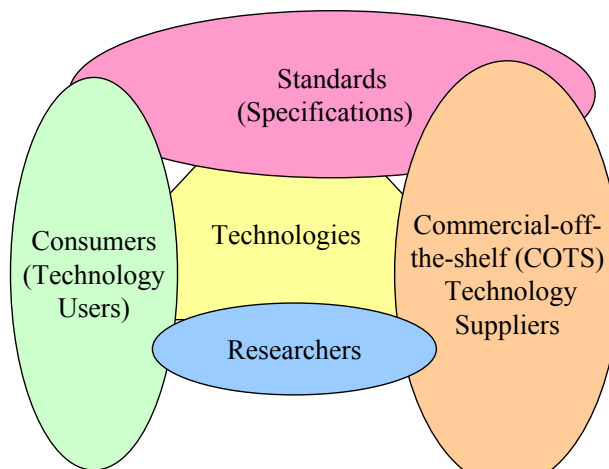
- Many security packages are commercially available to provide complete security solutions.
- Each provides its own strengths and weaknesses and operates at different levels.
- PKI (Public Key Infrastructure):
  - Extensive collection of security technologies (encryption, digital signatures, digital certificates) for a wide range of applications
  - Difficult to use, install and maintain

- If you need a certificate, you can choose an external certificate authority (CA) such as Verisign or install your own.
- The tradeoff is control versus effort.
- SSL (Secure Socket Layer):
  - De facto standard for securing the traffic between Web clients and Web servers
  - Uses encryption, digital certificates, and digital signatures
  - Client and server negotiate encryption scheme and key size (flexible). The choices are known as “cipher suites,” with different strengths.
  - When an SSL client connects to a server, both negotiate a cipher suite that is strongest and available on both sides
  - SSL has performance issues; but one can use SSL accelerators..
- IPSec is a standard used in Virtual Private Networks (VPNs).
  - Used to encrypt and decrypt IP packets in the Internet
  - Provides a secure path over the public Internet by encrypting the IP traffic
  - SSL can travel on top of VPN.
- PGP (Pretty Good Privacy):
  - Provides encryption and digital signature services
  - Used commonly to protect email and file transfers
  - Uses RSA to exchange the key (uses recipient’s public key to encrypt).
  - Free and commercial versions are available.
- Kerberos:
  - Open standard designed to provide strong authentication
  - Uses secret-key cryptography
  - Many free as well as commercial implementations

## 6.2 Interrelationships between Technologies, Consumers, Researchers, and Suppliers

To understand the different players in security technologies, it may be beneficial to briefly discuss how the various technologies become available to the consumers. As shown in Figure 6-2, technologies become available to the consumers in a variety of ways. In many cases, COTS (commercial off-the-shelf) technology providers build and sell technologies to consumers. We all use many products from Microsoft, IBM, and Oracle. An example in the security domain is SSL (Secure Socket Layer) that was developed by Netscape and is currently available in all Web browsers and servers.

Ideally, research efforts result in development of technologies that are “hardened” by the COTS suppliers and made available to the consumers. Examples are the encryption algorithms, such as RSA and SHA, that were developed by researchers and are currently available from many commercial vendors. In some cases, a few standards specifications are adopted and developed by COTS suppliers into products. Examples are IPSEC and S/MIME, which have been specified by the IETF and are now commercially available. Some technologies not adopted by COTS suppliers are provided by individual groups. Kerberos and PGP are such examples (now they have been adopted by suppliers and are available as commercial-strength products).



Technologies become available to the consumers in a variety of ways

- Some standards specifications are adopted and developed by COTS suppliers
- Some research efforts also result in COTS technologies
- Some technologies not adopted by COTS providers are provided by individual groups

Figure 6-2: Interrelationships between Technologies, Consumers, Researchers, and Suppliers

## 6.3 Certifying Authorities and the Public Key Infrastructure (PKI)

### 6.3.1 What is PKI and Why is it Needed?

A major problem with the public key cryptosystem is that it only works well if you know the public key of the recipient. Basically, you must be vigilant to ensure that you are encrypting to the correct recipient's key. How do you find out the correct public key of a recipient? If you freely exchange keys via public servers, *man-in-the-middle* attacks (as discussed in the cryptography chapter) are a potential threat. It is vital that you are assured that the public key to which you are encrypting data is in fact the public key of the intended recipient and not a forgery. In small settings, you could simply encrypt only to those keys which have been physically handed to you – e.g., on a diskette. But how do you exchange information with people you have never met; how can you tell that you have the correct key? Security and management of encryption keys is as important an issue in digital enterprises as is the protection of your house keys in your daily life (see the sidebar, “Key Management Issues”).

Although a variety of approaches can be developed, the most practical approach is that of using a trusted third party, called a “**certifying authority (CA)**.” Certifying authorities, along with several other support mechanisms to ensure a strong trusted environment, are known as the **Public Key Infrastructure (PKI)**. Simply stated, *PKI is not one technology but a family of technologies that are based on the public key cryptography and contain the facilities to store and manage certificates (i.e., the ability to issue, revoke, store, retrieve, and trust certificates)*. Specifically, PKI capabilities help create and manage

asymmetric cryptographic keys or public/private key pairs required by applications. The following major components are essential for a system to qualify as a PKI:

- **Encryption** based on the asymmetric as well as symmetric key cryptography.
- **Authentication Mechanisms** that may include a wide range of options such as user ID and password, one-time passtokens, digital certificates, and biometrics.
- **Certification Authority (CA)** is a commercial enterprise (e.g., Verisign) that vouches for the identities of individuals and organizations. A typical CA creates and signs digital certificates, maintains a list of certificates that have been revoked before the expiration date (certificate revocation lists), makes these certificates and revocation lists available, and provides an interface so administrators can manage certificates.
- **Registration Authority (RA)** evaluates the credentials and relevant evidence that a person requesting a certificate is who they claim to be. The RA approves the request for issuance of a certificate by a CA. CA and RA functions are provided by a wide range of PKI providers such as Tivoli SecureWay Public Key Infrastructure.
- **Directory Services** define and implement a common schema for users and groups. The directory service is the point of integration for user authentication in many security systems. A user can be defined once within an enterprise, and information about that user can be accessed in a consistent manner by multiple different applications. This reduces administrative costs and complexity. PKI directory services are usually based on the Lightweight Directory Access Protocol (LDAP).

#### **Key Management Issues**

- Protection of the keys that in turn are used to protect the assets is an important issue. These keys should be protected as diligently as you protect the keys to your house and car. Specifically:
  - Private keys and shared secrets, once acquired, must be protected.
  - End-to-end security must include consideration of the security of the end-user device.
  - Private keys stored on a personal computer disk file may be stolen via access to the file system or outright theft of the device.
- Security can be enhanced by
  - use of smart cards
  - use of a security chip embedded in end-user systems.
- Server-side hardware devices can provide tamper-resistant key storage. They can also provide assistance for encrypting and decrypting messages and public/private key operations that require heavy computational load

### **6.3.2 Certifying Authorities (CAs)**

A certificate is similar to a passport or driver's license. Basically, the main purpose of a CA is to produce such a certificate by binding a public key to a user. The CA is the authority whom everyone trusts, and no certificate is considered valid unless it has been signed by a trusted CA. Thus CA is similar to a government agency such as the passport

office or Division of Motor Vehicles (DMVs). There have been different standards for certificates – X509 is the best known (we discussed 509 in the previous chapter).

Trust is at the heart of CAs. To win trust, a CA is responsible for ensuring that prior to issuing a certificate, he or she carefully checks it to be sure that the public key portion really belongs to the purported owner. Anyone who trusts the CA will automatically consider any certificates signed by the CA to be valid. As mentioned previously, a CA's role is analogous to that of an office that issues passports (a passport is a certificate). A CA creates certificates and digitally signs them using the CA's private key, very much as a passport office creates a passport and then signs it by using secret stamps and codes that are difficult to forge.

To issue a certificate, the CA goes through the following steps (see Figure 6-3):

- The user first generates a public/private key pair.
- User keeps the private key and sends the public key to the CA with the user identification information (name, SSN, birthdate, etc.) in the form of a “certificate request.”
- The CA will verify the user identity through a procedure that may involve a telephone conversation or other mechanisms.
- If everything is verified, then the CA will issue a certificate with user name, email address, etc.
- The CA creates a signed certificate by creating a message digest and encrypting it with his private key. This makes sure that no one can modify this certificate.
- The certificate is returned to the user, with a copy kept by the CA.

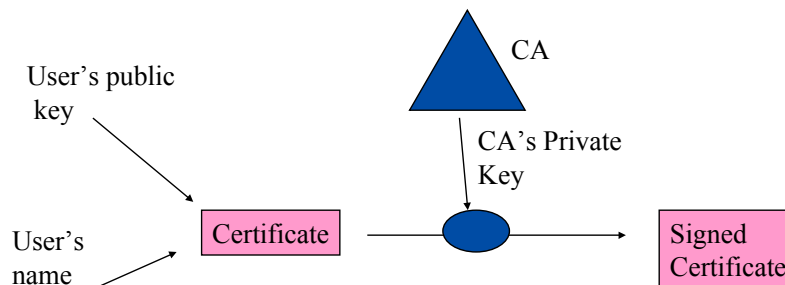


Figure 6-3: Certificate Authority (CA) and Creation of Certificates

Let us now assume that Joe wants to send a file to Pat. Before starting, Joe will ask Pat or the CA for a certificate. After receiving the certificate, Joe applies CA's public key to the certificate to verify correctness. If this works, then Joe can extract Pat's public key and send the file to Pat, after encrypting it with Pat's public key just obtained from the certificate.

CAs and signed certificates are core components of PKI systems. As we will see later, different types of certificates are maintained by current PKI systems. Basically a CA creates and manages certificates very much as authorities manage birth certificates.

### 6.3.3 PKI Versus CA Services – Practical Issues

PKI is an accepted standard for identifying people through certificates. It includes support for the entire life cycle of certificates and keys, ranging from creation to destruction of certificates and keys. Due to this, PKI-based solutions are expensive, complex, and not easy to administer and use. This has been the deterrent to widespread industrial use of the PKI – despite a great deal of press, PKI is used rarely in real-life environments.

Suppose you need a certificate that you can use for your Web server for a secure payment system. Then you have the following two choices:

- Outsource (rent) a CA service from an external agency. The agency will, for a fee, issue a certificate and then verify and certify that you indeed are the holder of the certificate whenever needed. Verisign ([www.verisign.com](http://www.verisign.com)) is such an agency.
- You buy your own PKI package, from a company such as Entrust, and install, maintain, and manage your own PKI system. This requires considerable effort.

The tradeoff is naturally control versus effort. If you need to support strong authentication by using certificates instead of ID and PW, but do not want to spend the time and effort to maintain the certificates, then an outsourced third-party CA is for you. However, if you do not trust a third party to serve as a CA, or want to control the certificates closely, then you should get your own PKI package.

### 6.3.4 Entrust – A Commercial PKI Product

Entrust.net, a subsidiary of Entrust Technologies, is a PKI provider that offers a portfolio of service solutions to securely manage e-business transactions. Solutions include secure e-business transactions from e-commerce Websites to interactive cell phones. Entrust also recently entered the secure transaction business for wireless transmissions. Entrust.net manages personal, Web and WAP (for wireless) certificates. In particular, the new WAP Server Certificates are digital certificates that enable WAP servers to establish Wireless Transport Layer Security (WTLS) sessions with mobile phones and micro-browsers that support the WAP standard. See [www.entrust.com/](http://www.entrust.com/) for additional information.

### 6.3.5 Verisign – An Outsourcing Certificate Authority (CA)

Verisign ([www.verisign.com](http://www.verisign.com)) is one of the best known third-party CAs. You can rent a variety of CA services from Verisign. It provides a wide range of security solutions for certificates, secure messaging, wireless systems, and payment systems. In addition, Verisign offers several industry-specific solutions for retail enterprises, telecoms, healthcare, and government agencies.

### 6.3.6 Players in PKI – Standards and Technology Providers

Many applications use cryptographic software to incorporate public-key cryptography for encryption and authentication. A number of such technologies exist under the general umbrella of PKI that have their origin in the standards bodies, research communities, and COTS (commercial off-the-shelf) technology providers (we discussed these issues in a

previous section). As stated previously, PKI is a family of technologies that are based on the public key cryptography and contain the facilities to store and manage certificates (i.e., the ability to issue, revoke, store, retrieve, and trust certificates). For a detailed discussion of PKI, see the book, *Understanding PKI*, by C. Adams and S. Lloyd (Addison-Wesley, 2003).

## 6.4 Secure Socket Layer (SSL) for Web Security

### 6.4.1 What is SSL?

Secure Socket Layer (SSL), also known as Transport Layer Security (TLS), is by far the most heavily used security technology for the World Wide Web. SSL provides encrypted communications between clients and servers, and also authentication of servers (optionally of clients also). At present, SSL is being packaged with almost all Web browsers (Netscape Navigator, Microsoft Internet Explorer) and servers (Apache, IIS). SSL technology was developed by Netscape Communications Corporation and has become the industry-standard method for protecting Web communications. SSL was introduced in the marketplace in 1994 with the first version of Netscape Navigator. Historically, a competing protocol (S-HTTP) was also introduced roughly at the same time. In addition, the cryptographic principles of S-HTTP and SSL were the same (digital envelopes, signed certificates, message digests, etc.). However, S-HTTP is rarely used at present.

SSL runs on top of TCP/IP and manages secure messaging on the network (see Figure 6-4). The SSL protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. Although SSL is used mainly for Web traffic, it can also be used to secure FTP transfers, emails, or any other service that uses TCP – this is a direct consequence of SSL residing on top of TCP.

SSL consists of software installed in browsers and on servers. All major browsers and servers today are “SSL capable.” If needed, SSL software can be obtained by subscribing to a Secured Service Provider such as [www.ssl.com](http://www.ssl.com), or by obtaining a Server Certificate from [www.ssl.com](http://www.ssl.com) and installing it on an existing secured server. The SSL protocol provides, as we will see, a wide range of encryption and authentication choices to ensure that communications between a client and a server remain private, based on user requirements. The cryptographic choices are known as “cipher suites.” A user can select a cipher suite when establishing an SSL session.

From an end-user point of view, the screen appearance of your browser with SSL is very similar to the one without SSL. To use SSL, you just need to type “https” instead of “http.” For example, the link (<https://www.fedex.com>) connects you to the Federal Express Website over SSL. If an SSL connection is successful, a lock appears in the bottom left part of your browser – the rest of your screen looks just about the same. If you want to know about the type of technologies and certificates (e.g., cipher suite) being used by your SSL session, just click on the lock and the browser will show you the SSL options being used. Once an SSL session is established, all Web server to client traffic (both ways) is encrypted. This includes:



- URL of the requested document
- Contents of the requested document
- Contents of any filled out forms
- Cookies sent from client to server
- Cookies sent from server to client
- Contents of the HTTP header

Thus SSL provides a great deal of confidentiality. However, you cannot hide that a particular browser is talking to a particular server. If this type of privacy is needed, then you should use a proxy server for anonymity.

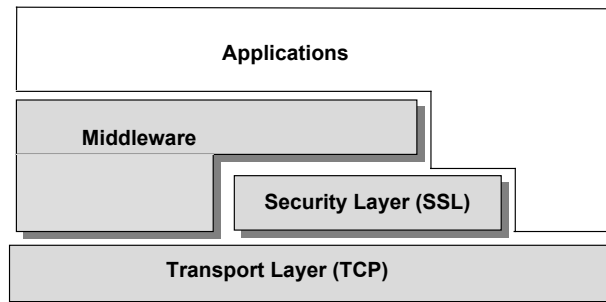
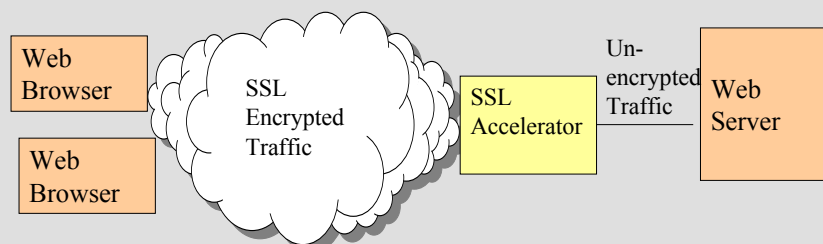


Figure 6-4: SSL

Although SSL is being described here as an instrument for Web security, SSL is not restricted to the Web. As depicted in Figure 6-4, *any* client/server application or middleware that uses TCP/IP can use SSL for secure transmissions. For example, CORBA security is based on SSL. In addition, J2EE and .NET security also rely on SSL. It can be seen from Figure 6-4 that applications have several choices to use SSL: a) directly use SSL by issuing SSL calls, b) use middleware such as CORBA or Web Services that uses SSL, or c) a mixture of the above two.

### SSL Accelerators

SSL adds considerable overhead to traffic, due to extensive encryption/decryption. Web servers are already quite busy handling requests from thousands of users. Encryption/decryption adds considerable overhead to this processing and reduces the number of users a Web server can handle. To reduce this overhead, SSL accelerators are used sometimes. An SSL accelerator is a separate appliance that decrypts/encrypts the SSL traffic before reaching the Web server, as shown below. While this handles overhead, it creates security risks because the traffic between the Web server and accelerator is un-encrypted.



### 6.4.2 How SSL Works

A secured server uses Secure Sockets Layer (SSL) technology to provide a safe way to transmit sensitive information, such as credit card numbers, online banking, email messages, surveys and other personal information. SSL client and server negotiate an encryption scheme and key size. SSL uses RSA (Rivest, Shamir, and Adleman) public encryption for key session negotiation and DSA (Digital Signature Algorithm) for session encryption. In reality, SSL gives users many cryptographic choices:

- Symmetric key (for encryption) can be DES, triple DES, or others.
- Asymmetric key (for authentication) can use the RSA public key and certificates.
- Message digest (for Integrity) can use the MD5 or SHA algorithms.
- Various key lengths are supported for conformance to different, especially overseas, secure websites.

These choices are known as “*cipher suites*” – each cipher suite has a different security strength. For example, the cipher suite “DES-RSA-MD5” in SSL 3.0 represents a security option with very high strength. Each Web browser and server supports several cipher suites. When an SSL client connects to a server, then both negotiate a cipher suite that is strongest and available on both sides. A common problem is that international websites have smaller key lengths (e.g., 40-bit). Thus the SSL session uses 40-bit keys even though higher key lengths are available on the Web browser.

Let us go through the information flow between a client and a server when a client clicks on, for example, <https://www.fedex.com>. Figure 6-5 shows the exchange of messages between the two parties to establish an SSL session and to display the lock at the bottom of the browser.

- 1. Send Client Hello.** The client (Web browser) opens a connection and sends its capabilities, i.e., the cipher suites it supports.
- 2. Respond with Server Hello.** The secure server responds to the client after determining the most suitable cipher suite. The server selects the strongest cipher suite that is supported by the client and the server. The server sends the selected cipher suite to the browser. The server also sends a session ID to be used. If a mutually agreeable cipher suite is not found, then the server sends the “handshake failure” message and disconnects.
- 3. Server sends certificate.** The server sends a signed X.509 site certificate to the client to identify itself. Almost all servers at present have signed certificates.
- 4. Server requests client certificates (optional).** This optional step is used if the client also has a signed certificate. Client-side certificates are gaining popularity slowly.
- 5. Send client certificate (optional).** This optional step sends the client-signed certificate to the server.
- 6. Send client key exchange message.** The client selects a suitable symmetric key for encryption. This key is used to encrypt/decrypt the messages. This key is encrypted by

using the server's public key (recovered from the server certificate) and sent to the server.

**7. Send a client certificate verify message (optional).** The client sends its certificate to acknowledge that it knows the symmetric key.

**8. Change cipherspec message.** The client as well as the server exchange this simple message to indicate that now they are ready to start communication.

**9. Send finished message.** The client and server send the MD5 and SHA hashes of all messages exchanged so far. This confirms that no messages have been compromised in this conversation.

**10. Exchange traffic.** The lock appears now and the two sides now start communication.

After step 9, an SSL session is established, and all Web server-client traffic (both ways) is encrypted by using the encryption key chosen in step 6. You also have the SSL icon (the famous lock) on the bottom of your screen. As indicated previously, all SSL communications are encrypted, including URLs of the requested document, contents of the requested document, contents of any filled-out forms, cookies sent from client to server, cookies sent from server to client, and contents of the HTTP header. Thus you can have secure Web communications.

It should be noted that SSL is not flawless. Several defects were found in the earlier versions of SSL and it was cracked a few times when it used only 40-bit keys. Most of these defects *appear* to have been fixed and longer key sizes are widely supported at present. I have not seen a recent story about SSL being cracked – so far so good.

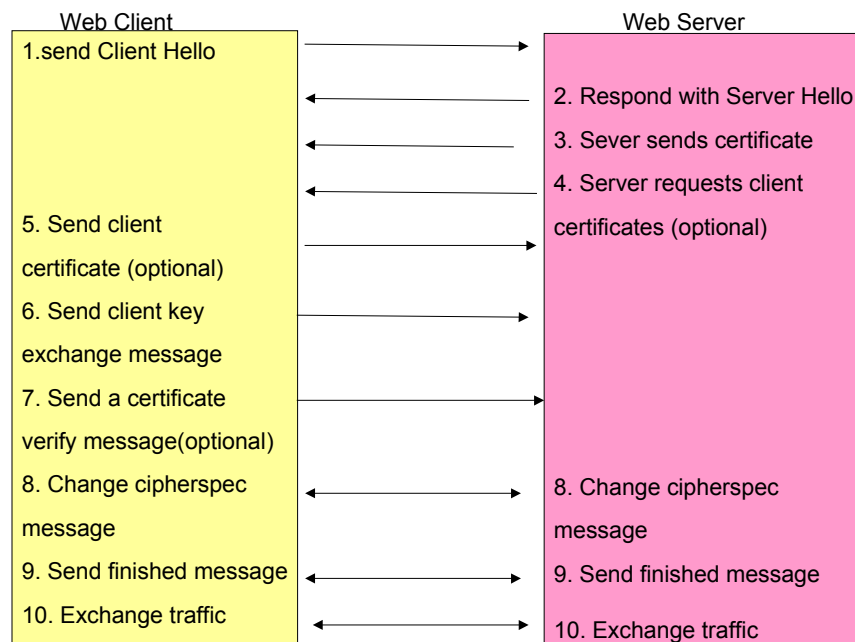


Figure 6-5: Flow of an SSL Session

## 6.5 Virtual Private Networks (VPNs ) and IPSec

Virtual Private Networks (VPN), as indicated above, are private networks (e.g. networks internal to corporations) that use public communication infrastructure. In other words, you set up a *private* network over a *public* network by using encryption. The main idea is that if your messages are encrypted, then the intruder cannot understand them even if he or she looks at them. Transportation of encrypted messages over a public network that spans a multitude of physical networks requires agreements and standards to avoid chaos. Currently available VPNs use IETF IPSec (RFC 2401) and related standards to transport encrypted messages over shared networks. VPNs and IPSec operate at a higher layer (layer 3) as compared to the network access (layer 2) because they encrypt packets that can be routed anywhere. An overview of VPNs and IPSec follows.

### 6.5.1 Virtual Private Networks (VPNs)

Simply stated, a VPN provides dedicated, secure paths, or tunnels, over a network that is shared by other users. VPN networks consist of authenticated and encrypted tunnels over a shared data network (typically, an IP network). The tunnels are set up between a point of presence (POP), also called a network access point (NAP), and a tunnel terminating device on the destination network. Shiva Corporation's LanRover Access Switch® is an example of a VPN POP. A POP encapsulates packets sent by the user so that the data travels securely over the shared network. A sample VPN is shown in Figure 6-6.

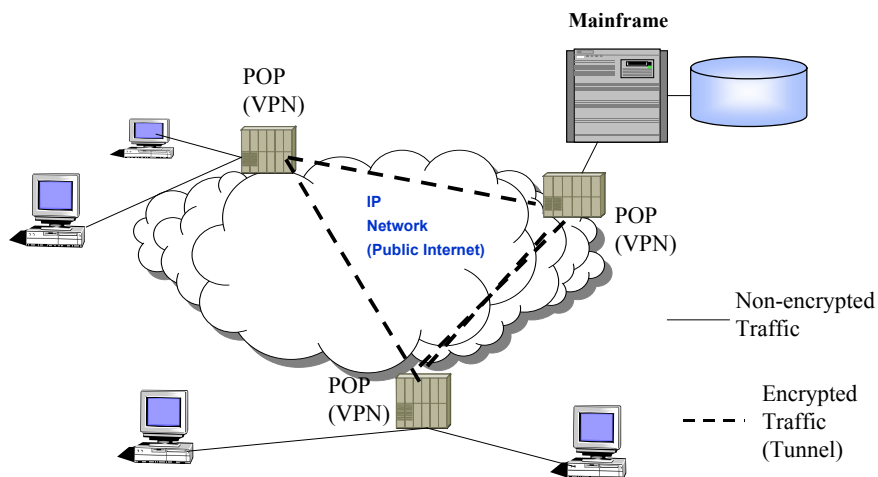


Figure 6-6: A VPN

Early attempts to provide VPN remote access involved simply encrypting every packet. Hardware was employed that encrypted and compressed data before it traveled on a shared data network. Current typical VPN configurations establish a secure tunnel between the POP server and a tunnel-terminating device on the local network. The POP server allows you to make a local call. An ISP or a network service provider may own a POP and add encryption/decryption service to provide VPN support. A user initiates a

dial-up session to a local POP, where a server authenticates the user and then establishes a tunnel through its Internet “cloud,” which terminates at the edge of the user’s corporate network. The IP packets are encapsulated in a tunneling protocol such as PPTP or L2F (see below), and these packets are, in turn, packaged by an IP packet containing the address of the corporate network – the packet’s ultimate destination. Note that in this case the POP assigns the user an IP address. The encapsulated packets can be encrypted end-to-end by using IPSec or an equivalent protocol. All packaging/unwrapping and encryption/decryption is transparent to the end user.

VPN users have basically two choices: install VPN software at their machine site or use the VPN capabilities of an ISP. With a VPN-enabled client, the users install software on their laptops and basically develop an end-to-end tunnel. The advantage of this *Internet service provider-independent* configuration is that mobile users can dial into any traditional POP to establish a VPN tunnel to a corporate network, independent of their contracted service provider. If the software is not embedded in the client, an *ISP-dependent model* is used, in which the participating ISPs are required to support VPN technology in the NAP server. The choice between the ISP-dependent and -independent models depend on port availability, backbone performance and client deployment. These considerations are beyond the scope of this book. Visit the VPN Consortium website ([www.vpnc.org](http://www.vpnc.org)) for a detailed discussion of the tradeoffs.

VPN POPs use protocols such as Point-to-Point Tunneling Protocol (PPTP) and Layer Two Forwarding (L2F) to encapsulate the data for Internet travel. PPTP is geared toward ISPs (Internet Service Providers) and has provisions for call origination and flow control, while L2F has less overhead and is suited for managed networks. The best features of both protocols have been combined into a new protocol called Layer Two Tunneling Protocol (L2TP). L2TP has provisions for flow control, call origination and secure tunnels across the Internet. The current protocols such as L2F and PPTP, and future ones such as L2TP, do not preclude the use of a Point-to-Point Protocol (PPP) client from having the tunnel-originating functionality embedded in it directly.

Currently, a large number of companies offer VPN services. Examples are Shiva, telecommunication companies (e.g., Southwestern Bell and Nortel), and network service providers such as UUNET. Additional information about VPN can be found at the VPN Consortium website ([www.vpnc.org](http://www.vpnc.org)). Although VPN is a favorite choice for physical network security, some issues with VPN security still exist, mainly because of multiple VPN implementations in the marketplace. In addition, many IPSec products in the marketplace are proprietary, with poor interoperability. In addition, many of the proprietary extensions have security flaws. A list of Web links to the security analyses of VPN protocols as well as to the IETF standard of IPSec is given in the sidebar “VPN and IPSec Information Sources.”

## 6.5.2 IPSec

Most of the currently available VPNs are based on the IETF IPSec (RFC 2401) and related standards to transport encrypted messages over shared networks. IPSec is not, however, restricted to VPNs – a corporate LAN within a building can use IPSec by installing IPSec-compliant software on various routers. IPSec-compliant software encrypts and signs Headers and/or Data parts of an IP Packet and specifies security at the packet level, instead of the application level. It thus provides security without requiring

changes to applications and is especially suitable for VPNs (see Figure 6-7). IPSec was developed for the next generation of IP (IPv6) but is flexible enough that it is being used in the current versions of IP (IPv4).

The principal feature of IPSec is that it can encrypt and/or authenticate all traffic at the IP level. Thus all applications that use IP (email, Web access, file transfer, etc.) can be secured. IPSec encompasses the following functional areas at the IP level:

- Authentication: Assures that the received packet is, in fact, transmitted by the party identified as the source in the packet header. In addition, this mechanism assures that the packet is not modified in transit.
- Integrity: Assures that the data is not modified in transit.
- Confidentiality: Encrypts messages to prevent eavesdropping by third parties.
- Key management: Assures secure exchange of keys.

To provide privacy and authentication services at the IP layer level, IPSec is typically implemented at the network router level or a “firewall” that serves as the main entry point into a system. When implemented in a firewall, IPSec provides strong security that applies to all traffic crossing the firewall. If the firewall is the *only* way to enter the system, then you have very strong protection by making the firewall IPSec enabled. In addition, since IPSec runs below the TCP/UDP layer, no change is needed on the application software for added security. In large-scale systems this is very valuable because *all* applications can be secured without any changes. This does not address the different security needs of different applications. For example, email may not need the same level of security as a corporate retirement system. Those special needs have to be addressed at the application level.

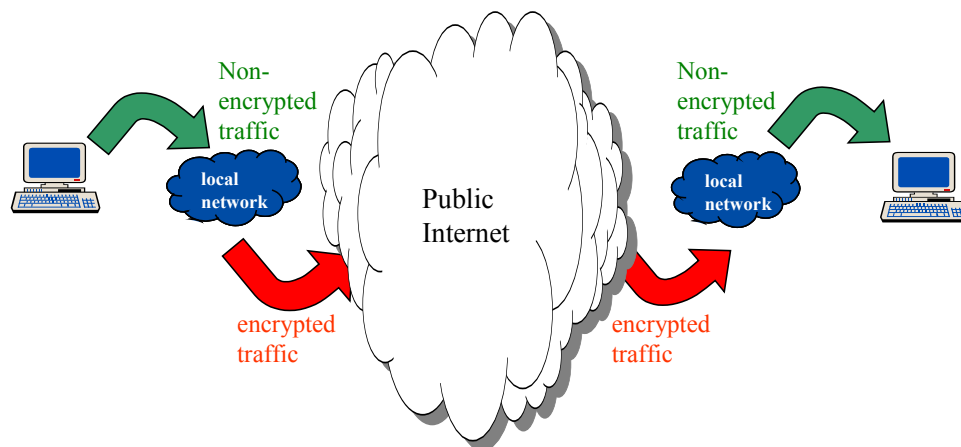


Figure 6-7: IPSec Conceptual View

Figure 6-8 shows a more detailed view of how IPSec can be used in enterprise networks. The IPSec-compliant software is installed in a set of network devices (routers). In addition this software can be directly installed in a user workstation. The main purpose of this software is to generate and process the encrypted packets that have the following format:

- IP Header – this indicates the regular IPv4 or IPv6 header that shows the origin and destination addresses.

- IPsec Header – this header is generated by IPsec software and itself can consist of two headers: an Authentication Header (AH) used to describe the authentication to be used, and an Encapsulating Security Payload (ESP) to describe the encrypted payload. AH and ESP headers will be described later.
- Secure IP Payload – this is the actual data that has now been encrypted

LAN1 and LAN2 in the following figure generate the regular IP traffic with packets that contain the IP Header and the the IP Payload. These packets are transformed by the IPsec-enabled devices (routers) into IPsec packets by adding a new header (IPsec Header) and encrypting the payload. These packets are then sent over the public Internet (treated as a VPN) or over a private network. The IPsec-enabled workstations directly generate and interpret the IPsec packets.

A great deal of information, in the form of several documents, has been produced by the IETF (see Figure 6-9).

### IPsec Versus SSL

A commonly asked question is: how does IPsec differ from SSL? Although we will discuss SSL later, it is good to note here that IPsec differs from SSL in that it creates a secure channel between two TCP/IP *hosts* over which *multiple* TCP/IP connections can be established. Each TCP/IP session itself may or may not use SSL. This also implies that IPsec can authenticate machines but not users because it is too low-level.

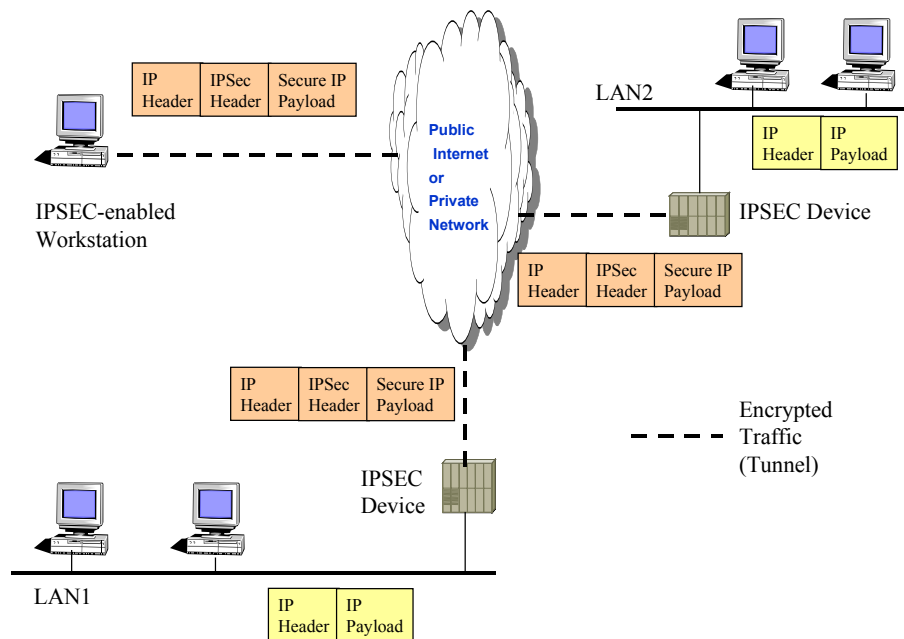


Figure 6-8: A More Detailed View of IPsec (based on [Stallings 2000])

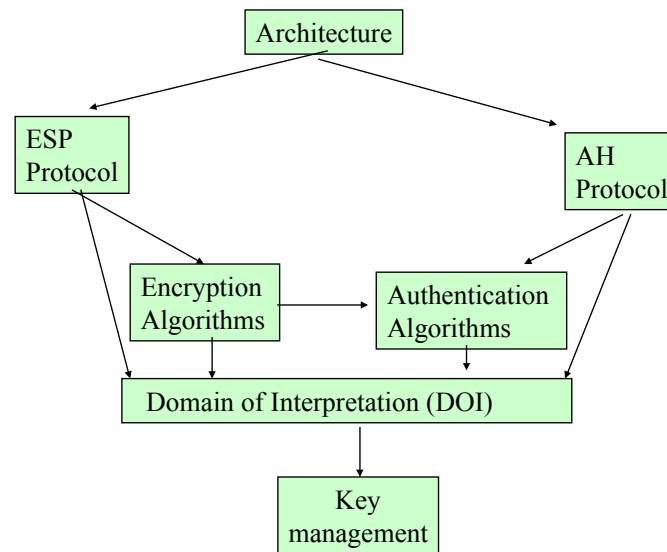


Figure 6-9: IPSec Documents

## 6.6 PGP (Pretty Good Privacy)

PGP is a popular program, available on the Internet, that uses public-key cryptography to authenticate users to each other without the use of certificates. PGP was developed by Philip Zimmerman to provide encryption and digital signatures. It does not introduce any new technology, but merely packages several encryption technologies into a product. PGP is used heavily in group communications (among individuals). The security mechanisms are implemented in software that is free for individual use. The main characteristics of PGP are:

- It uses symmetric as well as asymmetric encryption.
- For symmetric encryption, PGP uses a block cipher with a 128-bit key to encrypt files or messages.
- A “session key” is generated automatically for files and messages based on a random number generator.
- The session key is encrypted by using the asymmetric encryption. PGP uses RSA to encrypt and exchange the session key. It uses the recipient’s public key to encrypt.
- PGP can also be used to encrypt files for storage and messages for transmission.

To illustrate how PGP works, let us assume that Pat wants to send secure email to Joe. Pat encrypts her email by using the PGP-generated session key  $K$ . Pat then sends the email. To send the session key  $K$ , Pat gets Joe’s public key ( $E_j$ ) and encrypts  $K$  by using  $E_j$ . The encrypted  $K$  is now sent to Joe.

When Joe receives the email, he does the following. First he decrypts the session key  $K$  by using his private key ( $D_j$ ). He then uses the decrypted key  $K$  to decrypt Pat’s email.

PGP keeps on evolving with new features to overcome new problems. In particular, several vulnerabilities of PGP have been found in the late 1990s. These problems have been fixed in newer releases.



A great deal of information about PGP, including tutorials and downloads, can be found at the Website: [www.pgpi.com](http://www.pgpi.com).

## 6.7 Kerberos

Kerberos is primarily an authentication protocol based on secret-key encryption. Developed at MIT, Kerberos uses a third-party authentication server to grant cryptographic “tokens” that authenticate users for a given service. Kerberos is an open standard designed to provide strong authentication by using secret-key cryptography. Used for secure interoperation of existing systems, Kerberos is primarily used for user authentication.

Kerberos has gone through several evolutions. It is currently on version 5 and includes a very wide range of security technologies such as the following:

- the venerable user-ID and password
- certificate-based public key systems
- asymmetric-key cryptography
- certificates
- token cards
- smart cards

Although primarily intended for authentication, the Kerberos security system possesses capabilities that cover many aspects of PIA4:

**Privacy:** Secure and private channels are supported through encryption. Kerberos incorporates asymmetric-key cryptography, such as elliptic-curve cryptography. It provides all of the basic security services using shared secrets and symmetric-key cryptography. The ability to use symmetric-key cryptography guarantees undisturbed use of performance-sensitive applications, such as high-volume transaction-processing systems, where each transaction is individually authenticated.

**Integrity:** Hashing functions and message digests support integrity.

**Authentication:** Kerberos provides strong authentication by maintaining a high level of assurance that the principal’s claimed identity is genuine. Also, Kerberos provides mutual authentication; i.e. the identity of both client and service can be assured. Completing authentication before the beginning of the conversation, although very important, is not enough to assure the client that later the conversation will not be subverted. Kerberos provides the cryptographic “session keys” needed to establish a secure channel that keeps the conversation protected after the completion of the initial authentication procedure.

**Authorization:** A common mechanism to represent the authorization includes access control lists (ACLs) and capabilities. Although Kerberos doesn’t provide an ACL-based authorization system, it provides all of the underlying services such a system requires. Also, Kerberos provides the facilities necessary for capability-based authorization and delegation processes.

**Accountability and non-repudiation:** These are not fully supported by Kerberos.

Let us illustrate the operations of Kerberos through an example. Let us suppose that an employee, Joe, needs to access payroll. The principal database has the secret keys  $K_p(\text{payroll})$  and  $K_j(\text{Joe})$ . Figure 6-10 shows the flow of information:

1. The client asks for Joe's ID request. He identifies himself as Joe and indicates that he wants to access payroll. This information is sent to KDC.
2. KDC Authentication Server (AS) constructs two replies and sends them to the client:
  - Service ticket: This includes the following information: Joe, payroll, and a session key (random). The service ticket is encrypted by  $K_p$ .
  - Client ticket: This is the service ticket but it is now encrypted by  $K_j$ .
3. The client decrypts the client ticket by using  $K_j$ . If this does not happen, then something is wrong.
4. Client constructs a service request. This consists of the service ticket + request (print check).
5. Client sends the service request to the payroll server. The payroll server decrypts it by using  $K_p$ .

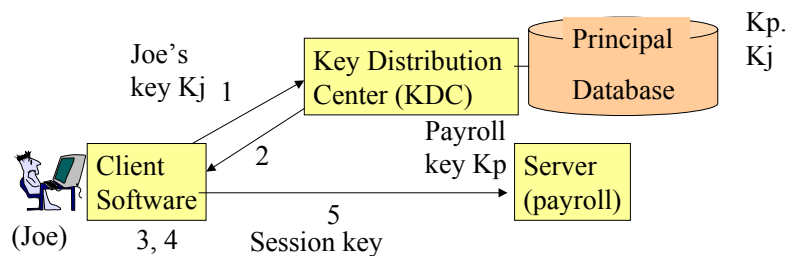


Figure 6-10 : Conceptual View of Kerberos

Kerberos has been adopted as one of the IETF standards. Many free as well as commercial implementations of Kerberos exist at present. Examples of products that use Kerberos are:

- OSF DCE (Open Software Foundation's Distributed Computing Environment): integrated into a product (mid-1990s)
- GSS-API (Generic Security Service API): hides underlying technology
- Microsoft SSPI: very similar to GSS-API
- SSL: uses public key for network security
- IPSEC: encrypts packets
- RADIUS (Remote Access Dial-in User Service)
- Token cards: user gets a key, types; host side synchs
- Smart cards: micro-processor with IDs, etc.



A great deal of information about Kerberos can be found at the website (<http://www.mit.edu/kerberos/>).

## 6.8 Other Packages and Concluding Comments

A number of public-key-based cryptographic infrastructure tools are available, such as the Microsoft and Netscape Certificate Servers, which allow for the inclusion of public-key certificates in various applications. Examples of other packages include:

- Tivoli ([www.tivoli.com](http://www.tivoli.com)) started as a systems management company (managing performance and faults) but was bought by IBM. It provides a set of security services under the Tivoli Access Manager that controls both wired and wireless access to applications and data, keeping unauthorized users out. It also integrates with e-business applications to deliver a secure personalized experience for authorized users. Recent versions of Tivoli integrate security for key CRM, ERP, and SCM e-business solutions with enhancements for security in the current J2EE and .NET environments.
- Microsoft's Passport Service is a PKI system for the .Net environment. This service is used in .Net applications.

We have reviewed a few of the common packages that are used in modern environments. The purpose here is to highlight the main players. Parts III and IV of this book will show how these packages are actually used to protect IT assets. Additional packages that are used for specific situations will also be discussed in later chapters.

## 6.9 Short Case Studies and Examples

### 6.9.1 Prudential/BT Managed PKI

Many corporations have adopted PKI for secure operations. This is a short illustrative example of how the Prudential group in the UK chose and implemented PKI.

Prudential is one of the largest financial services providers in England, with total funds under management of around £150 billion. Prudential recognised the need for a secure and trusted environment when it launched its extranet, enabling IFAs (Independent Financial Advisers) to work more efficiently and effectively. IFAs traditionally contacted Prudential with new business quotations, policy valuations and application-tracking enquiries. The extranet was developed to allow the bulk of interaction between Prudential and its IFAs to take place over the Internet.

There was an obvious need for a *trusted environment* for both Prudential and IFAs to conduct business without fear or concern for safety of information. The main security challenge for the extranet was that it had to allow access to hundreds and potentially thousands of financial advisers, while allowing Prudential to manage the level of access privileges IFAs receive. In addition, IFAs had to be sure they were using a highly secure system because their client details would be entered onto the extranet.

After an analysis, Prudential chose digital certificates rather than user names and passwords to meet the security challenges. Passwords and user names can be costly to set up and maintain in large settings. Passwords and user names also carry a security risk since they can be guessed or cracked by the adversaries. It can also be very difficult for

IFAs to remember passwords and user names, especially if they deal with a range of companies who all give them different user names and passwords to enter secure areas.

Using digital certificates has several benefits. Each IFA can be issued a unique digital certificate and Prudential can identify each individual IFA by simply interrogating their certificate each time they enter the extranet. In addition, personalized content can be delivered based on the information contained in the digital certificate as the extranet recognizes and validates the identity of the IFA on an individual basis. This can allow an entirely personalized service for each IFA. For instance, one IFA might have a focus on investment products, while another specializes in group pension schemes. So the content delivered via the extranet could reflect those activities by using the entries in the certificates (a certificate could show what services are typically used by the IFA).

The Verisign-Managed PKI from BT was chosen for implementation, as it allowed Prudential to operate as a customized Certification Authority (CA), without the additional work of establishing a secure environment in which to operate a certificate service. Verisign Managed PKI from BT gives Prudential the ability to issue digital certificates to authorized users while outsourcing all the technical work. Prudential chooses who to issue certificates to, while BT manages the database, administers the server, backs up the system daily, and performs all other overhead activities associated with a certificate service. Prudential decided to offer the product as a free 30-day trial before launching the system. The demo facility was particularly useful to see how the service would work in a real-life situation.

Verisign-Managed PKI from BT was also chosen for its six data fields. Three data fields are pre-defined to guarantee the same level of security regardless of application or company – the other three are user-defined fields, allowing Prudential to customize their certificates. This feature also gives Prudential the ability to treat each IFA as an individual and provide personalized service.

The process for registering online as an extranet user is straightforward. The IFA fills in a registration form with their details, which is then passed to an administrator who checks and verifies those details. Once Prudential is confident that the IFA is legitimate, an email is automatically generated and sent to the IFA with their pin number and a link to the extranet, where they can collect their digital certificate and install it.

The project has been very successful. In the Independent Financial Adviser market, the standards body ORIGO has approved digital certificates as the chosen method of access to a provider's extranet services. A company called OSIS has been established to act as the Certificate Administrator. If an IFA has an OSIS certificate, then it can access the services of all participating providers. BT Trust Services has been selected to provide the certificates for OSIS.

**Source:** <http://www.btglobalservices.com/en/products/trustservices/inform/scot.html>, May 2002.

### **6.9.2 Global Public Key Infrastructure (PKI) for Least-Developed Countries**

G77 is the title given by the United Nations to the 134 Least Developed Countries (LDCs) in the world. G77 believes that the Internet can be used by the LDCs to lift their

economies through international trade. G77 also recognizes the necessity to establish a secure foundation for international trade over the Internet. KPMG Consulting has been retained since March 1999 to establish this secure trading infrastructure through digital certificates. An incubator has been established in KPMG Consulting's site, from which the G77 PKI is operated together with a trading database storing trade opportunities posted from amongst the G77 participants. The organization chosen by the G77 to work within this endeavor is the Chamber of Commerce, which is very strong in most LDCs. It is expected that eventually this business exchange will encompass the developed countries and become global in scope. Besides trade, health and education exchanges are also planned.

KPMG Consulting has financed the G77 PKI (based on SpyruS PKI technology) and trading database (based on Digerati Trade Tracker). KPMG Consulting will be repaid on a per certificate basis, so selling more certificates is a critical success factor. The global root is held by G77 and operated by KPMG Consulting, which is also the Certification Authority (CA). Registration Authorities (RAs) are distributed amongst the participating countries, where local Chambers of Commerce operate the RA. KPMG eSecurity consultants developed appropriate certification policy and participated in training workshops in different sites. It is expected that as the project grows, the national chambers or governments will sponsor and manage their own CAs.

More than 15 countries have participated in this project: Brazil, Costa Rica, Trinidad-Tobago, Romania, Malta, Nigeria, Cameroon, Ghana, Kenya, Mauritius, Senegal, Uganda, Pakistan, India, and Singapore. The first sales of certificates embedded into trading software commenced in June 2000 in Pakistan, with India and Brazil following shortly after.

Source:

[http://www.spyrus.com/content/irc/case\\_studies/KPMG/G77\\_SETI\\_KPMG\\_case\\_study.asp](http://www.spyrus.com/content/irc/case_studies/KPMG/G77_SETI_KPMG_case_study.asp)

### **6.9.3 Utilities Choose PGP Encryption Over S/MIME**

The Gas Industry Standards Board (GISB) is one of the major groups that chose PGP (Pretty Good Privacy) encryption and authentication technology rather than the more popular S/MIME (Secure/Multipurpose Internet Mail Extension) standard developed by RSA. The GISB's decision to adopt PGP impacts its 165 corporate members which include Amoco, Exxon, Mobil, Con Edison and Pennsylvania Power & Light Co. This adoption is a major endorsement for PGP. PGP was chosen because it allows encryption for email exchanges as well as for data stored in files. The group also felt that PGP was better suited for its requirements, which include data privacy, integrity, authentication and nonrepudiation. While S/MIME also supports these core functions, it is intended only for email encryption.

The GISB has been experimenting with PGP since 1996, before S/MIME became a standard. GISB wanted to send encrypted EDI files, using HTTP as a transport. Although SSL could be used for this purpose, SSL was owned by Netscape at that time. GISB did not want to pick one specific Web server and browser. In addition, GISB wanted file protection. PGP will help the GISB member companies secure more than 37 different types of business transactions, from ordering space in a pipeline, to moving gas, to paying for it once it reaches its destination.

Based on GISB's choice of PGP, the Federal Energy Regulatory Commission (FERC) has mandated that all members of the gas industry implement PGP 2.6 or greater to secure electronic transactions. Network Associates, which acquired PGP Inc. in 1998, is making the product compatible between various versions. Although PGP has emerged as a de facto standard for data encryption among consumer users and individuals, it has not been adopted by many large companies at an enterprise level. Under the auspices of Network Associates, PGP is evolving into a more flexible, robust product with support for RSA encryption and X.509 digital certificates. PGP also supports other standards, such as SSL. Network Associates offers an integrated suite, called PGP Enterprise Security.

Source: R. Yasin, "Utilities Choose PGP Encryption Over S/MIME," Internetweek.com, August 16, 1999.

## 6.10 Suggested Review Questions

- 1) Why do so many packages exist for security? Why can't one security package do it all?
- 2) What are digital certificates and how are they related to certifying authorities?
- 3) What are the key players in PKI and how are they interrelated to each other?
- 4) When would you install your own PKI, as opposed to renting CA services from a service provider?
- 5) Compare and contrast GP with Kerberos. What are the similarities and differences?
- 6) Can SSL be used to encrypt everything? Specifically, can you use SSL to encrypt IP packets?
- 7) Develop a table that compares and contrasts PKI, Kerberos, PGP, SSL, and VPN in terms of #

## 6.11 PART II – NRW Case Study Revisited: Choosing Enabling Security Technologies as Countermeasures

Figure 6-11 shows the conceptual model of NRW that was introduced in earlier chapters (chapters 1 and 3). As shown, the NRW corporate website consists of a user interface that connects to an Accounts Balance Program (ABP) that allows customers to view, update, and modify account information; a customer database that contains information about customers; an investment database that contains investment data; and other typical corporate applications and databases for payroll, accounts payable/receivable, etc. A corporate network will operate in the building, connected to the public Internet. A firewall protects the internal corporate resources. This simple model will be sufficient to get us started. NRW will establish some key attributes of the security architecture for the Accounts Balance Program (ABP) to address the risks identified previously at the end of part I (chapter 3). These high-level as well as low-level risks were identified through attack trees and other risk-analysis measures. We now need to do an overall assessment of what type of security technologies can be employed to address these risks. More detailed evaluation and selection of these techniques will be discussed at the end of parts III and IV to address specific protections needed for networks and the IT assets. At present we will do a high-level and general evaluation.

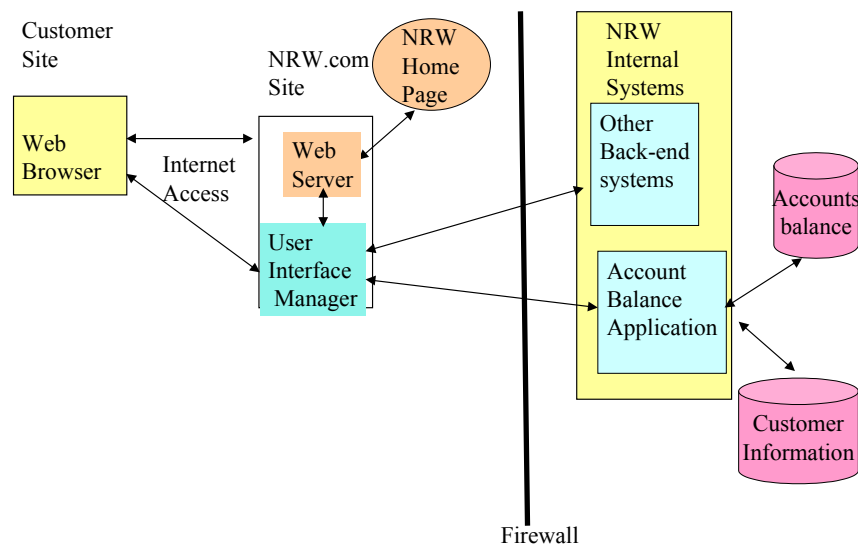


Figure 6-11: NRW System Conceptual View

The main elements of the countermeasures are the use of encryption, Virtual Private Networks (VPNs), firewalls, authorization, and general attempts to minimize the points of access to critical databases and applications. All external users, customers, remote employees, global partners, and suppliers should receive certificates in order to access

the corporate information. Specifically, the countermeasures should include the following:

- Modern cryptographic techniques should be employed by NRW for the encryption/decryption of its data between customers. Specifically, NRW should use symmetric key encryption. For asymmetric encryption, digital signatures and integrity through message digests, NRW may also want to explore using Public Key Infrastructure (PKI) as a means for encrypting/decrypting data from its applications. Packages such as PGP or Kerberos may be employed. A wide range of security technologies ranging from public/private key encryptions to digital certificates and ACLs are currently available to address the authentication, protection, authorization, and accountability aspects of security. Table 6-1 shows a mapping of various security technologies to security needs (e.g., which technologies address which needs).
- The platform for NRW's extranet system has to be highly controlled. This means that only NRW's data center personnel have physical access to NRW's application server and network equipment. If a business partner owns a piece of equipment, it is to be shared between both organizations.
- Firewalls will be used to localize the different areas of the firm's security architecture. The firewall will separate the corporate website from the ABP, the customer database, and the investment databases.
- Secure network connectivity has to be provided using a dedicated line or Virtual Private Network (VPN). VPNs provide encryption and authentication features over public networks for secure communications. Before a NRW VPN device communicates with another, it first must establish a password. Authentication systems like NRWs are based on digital certificates that are more secure than a password-based authentication. NRW would want to ensure that its network is semi-private, meaning that only business partners have access to the network. NRW would want a network effectively capable of detecting intrusions.
- Access to applications should be private. Users must be authenticated and authorized to perform operations depending on their rights. Application users have to be uniquely identified using adequate authentication techniques. Accountability can be accomplished by identifying and authenticating users of the system and subsequently tracking actions on the system to the user who initiated them.
- SSL should be used to protect Web-based operations, and PGP may be needed for highly secure emails.
- There should be single user name and logon. Once a person is logged on to the NRW system, they will not have to log on again.
- NRW will use authentication and authorization. The NRW security architecture must enforce user accountability. At the network level, it is very difficult to achieve this due to the proxy servers, application gateways, firewalls, and address translation.
- The users' authorization to the network will be stored in a Web server/directory server. The NRW users' rights to what files and directories they can access will all be located and accessed from this server. This is sufficient for static Web content security. The application will provide further authentication and authorization once the network access has been granted to the NRW employee.
- Authorization rights have to adhere to the least-privilege principle. This principle is the practice of restricting a user's access (DBMS updates or remote administration) or type of access (read, write, execute, delete) to the minimum level necessary to perform a job. It is a conservative approach to granting user rights.



- NRW should also take Non-repudiation (NR) into consideration. Non-repudiation is the ability to provide proof of the origin or delivery of data. NR protects both senders and recipients in a data interchange. A receiver (NRW) cannot say that he or she never received the data, and the sender (customer) cannot say that he or she never sent any data.
- For quality of service, NRW should ensure availability, latency, bandwidth and response time of its extranet system. Quality of service should not be compromised in any security system. Servers should be physically secured and back-up power sources should be available.
- For increased availability that does not violate security, FRS should be used for the critical resources.

**Table 6-1: Security Considerations - Mapping Technologies to Needs**

Technologies	Privacy	Integrity	Authentication and Authorization	Accountability (Non-repudiation)	Availability and Denial of service
Encryption	X		X		
Password protection	X		X		
Digital signatures		X	X		
Message Digest		X			
Digital certificates	X	X	X		
ACLs			X		
Audit trails				X	
Redundancy and FRS					X