



Enhancing VPN Security with Digital Certificates

A Baltimore Technologies[™] White Paper

No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly there from shall be given orally or in writing or communicated in any manner whatsoever to any third party being an individual firm or company or any employee thereof without the prior consent in writing of Baltimore Technologies, Ltd.

Written and published by Baltimore Technologies Ltd.

©2002 Baltimore Technologies plc. All rights reserved. Global e!security, the Baltimore logo, Baltimore SelectAccess, Baltimore UniCERT, Baltimore UniCERT Options, Baltimore KeyTools, Baltimore MIMESweeper, Baltimore SecureVPN and Baltimore SureWare are all trademarks of Baltimore Technologies plc. All other trademarks are the property of their respective owners. Users should ensure they comply with all national legislation regarding the export, import, and use of cryptography.

Contents

Introduction		1
Security and the Internet		1
Introduction to VPN Technology		2
VPN Implementations		3
IPSec VPN Security		4
IPSec Authentication Options		4
Shared Secrets		4
User Names and Passwords		4
Proprietary Tokens		4
Digital Certificates		5
Smart Cards and Smart Tokens		
Using Digital Certificates		5
Biometrics		5
Benefits of Using Digital Certificates within a VPN		6
Deploying your VPN with Digital Certificates		7
Using a VPN Service Provider or Building It Yourself		7
Outsourcing Your PKI or Developing It Yourself		7
Outsourced PKI Model		8
Summary		9
Glossary of Terms		10

Introduction

Corporations large and small are embracing Virtual Private Networks (VPNs) as a means to build networks that provide secure access for remote and mobile employees. The following discussion compares digital certificates issued from a Public Key Infrastructure (PKI) with the other IPSec authentication options and establishes that digital certificates are the better option for VPN authentication.

Security and the Internet

Existing methods used to route data through the open, public Internet leave data extremely vulnerable to a range of security risks such as spoofing, sniffing and session hijacking. Also, the lack of enforceable non-repudiation is an impediment to conducting contractual or monetary transactions over the Internet. Without comprehensive network security in place, a non-authorized user could access sensitive customer information or conduct fraudulent transactions anonymously. Mishaps like these can ruin companies; companies and individuals are demanding better security before exchanging information over the Internet.

Organizations need to secure communications between remote offices, business partners, customers and telecommuting employees. The Internet presents a cost-effective alternative to expensive private network connections. Transmitting messages over the Internet to these different entities poses an obvious risk, given the lack of protection provided by the existing public Internet. Virtual Private Network security with strong authentication plays a major role in preventing these risks from becoming a reality.

Digital certificates provide the four principal security functions that ensure secure data transactions:

- Confidentiality – to keep information private
- Integrity – to prove that information has not been manipulated
- Authentication – to prove the identity of the user or sender of a message
- Non-repudiation – to ensure the originator of a message cannot deny sending it

Lack of security is the number one barrier to implementing VPNs. Trust and confidence in the network systems greatly increases when all transactions are protected by these core functions of digital certificates.

Introduction to VPN Technology

A Virtual Private Network is comprised of existing dedicated networks, the Internet, or a combination of both, with an overlay of strong security to assure private communication over unsecured networks.

VPNs allow dispersed remote users to communicate securely via encrypted connections, known as tunnels. An enterprise owned and managed network solution using existing dedicated networks, the Internet, or a combination of both, to securely communicate information, VPNs are typically used in securing remote access for telecommuters to communicate with their corporate office, site-to-site network communication among branch and corporate offices, and corporate extranet access for business-to-business communication. Organizations are recognizing significant cost savings as they move their remote workers, branch offices and external constituents off expensive dedicated telephone lines and private networks to the Internet.

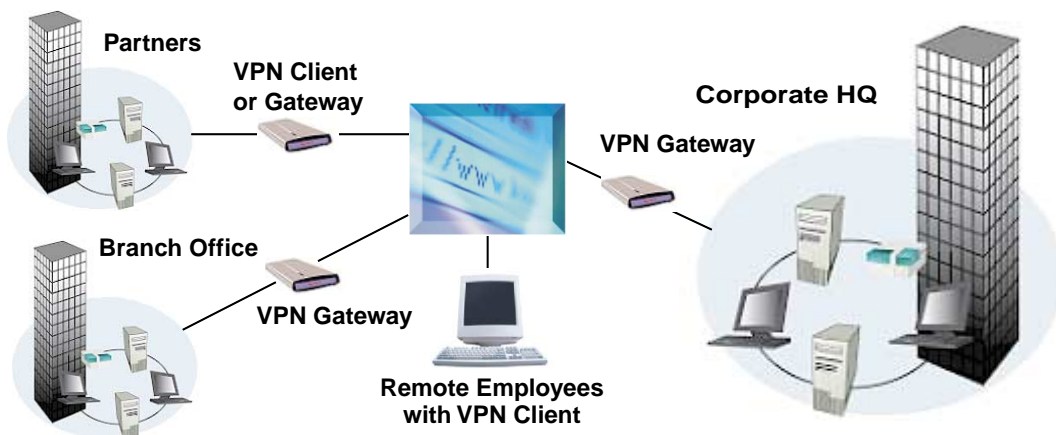
Control and management of security and access between the different entities in a company's business environment is of paramount importance. VPNs are set to revolutionize security on the Internet by offering a flexible, scalable and comprehensive information

security solution. VPNs provide the necessary data privacy, access control, data integrity and authentication services at a low level in the network and are independent of the applications using the network.

VPN providers differ in their product offerings. Solutions include:

- Embedded technology, such as that employed in routers
- Application level products installed on gateways and servers
- Desktop client applications providing security for dial-up and Internet connections
- Firewalls with VPN capabilities

Prominent tunneling technologies available to implement VPNs include PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), and IPSec. L2TP and PPTP provide security for any network layer technology including IP (Internet Protocol) and IPX (Internetwork Packet Exchange). IPSec provides strong cryptographic protection for IP. L2TP and PPTP offer weaker security compared to IPSec but are important for a small number of companies that use protocols other than IP. The public Internet is based on IP. IPSec was designed to secure the Internet and is accepted as the standard for Internet-based VPNs.



VPN Implementations

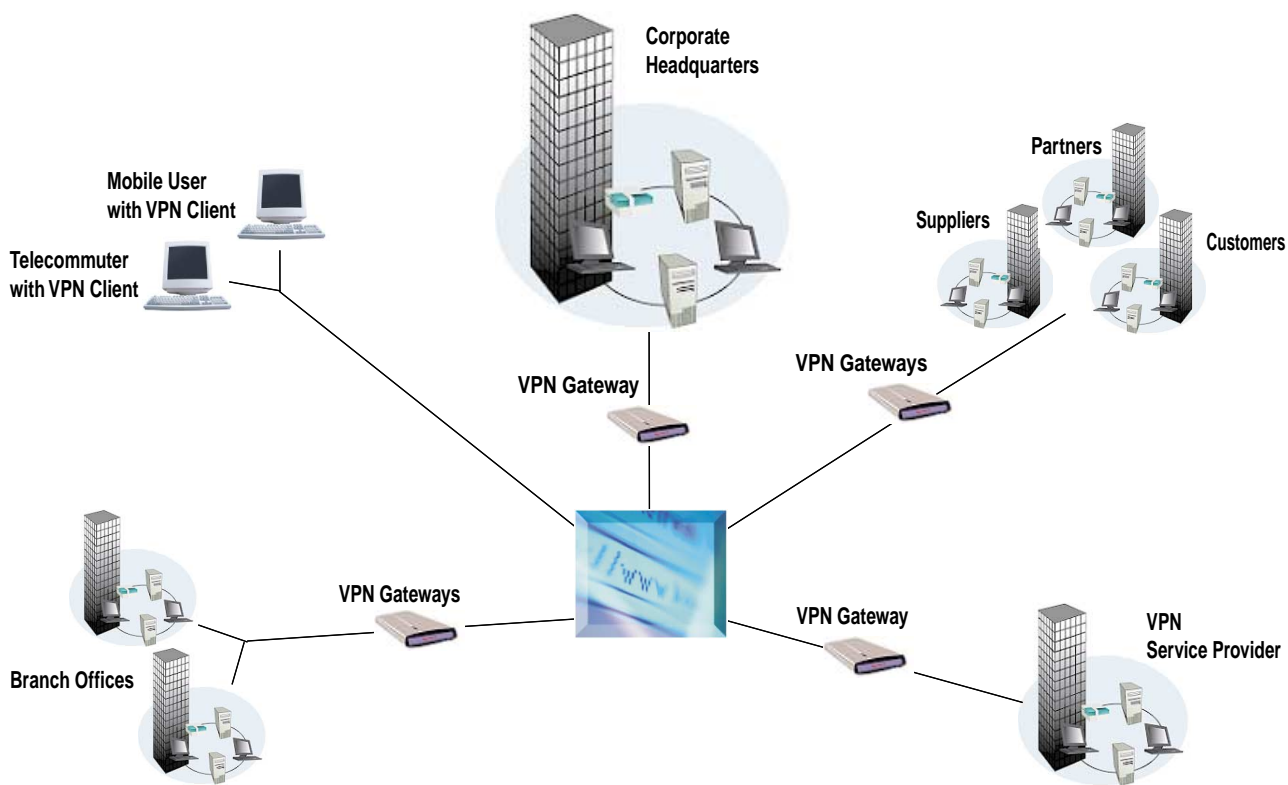
Companies are choosing to deploy VPNs in a variety of ways. Here are a few examples of the most popular VPN applications.

Remote Access

Remote User Access is the main reason companies choose to implement a VPN, as there is a significant cost savings compared to associates dialing directly into a corporate modem pool. Home office workers, pay a low monthly fee for fast Internet connectivity with a cable modem or DSL connection. Road warriors, like executives and sales representatives, have the option of using a local Internet connection or dialing a local number through an analog modem. The local connection is much cheaper than the long distance fees associated with dialing directly to the main office.

Business-to-Business Connectivity

VPNs increase communication and productivity with partners, customers, and suppliers by allowing them access to internal data and applications. Customers can place orders, suppliers can see inventories, and partners can access the critical and confidential information they need in real time. Again, by leveraging the public Internet, organizations can build extranets without an expensive private network.



Site-to-Site Connectivity

Using a VPN to connect branch offices to headquarters is less expensive and provides faster access to files and applications compared to leased lines that interconnect the LANs (Local Area Networks). Organizations purchase Internet connections that cost less and are faster than leased lines. The result is a secure, high-speed Wide Area Network (WAN) that interconnects branch offices and corporate headquarters.

Outsourced

Companies that do not wish to allocate the resources required to manage the VPN 24 hours a day and 365 days a year may find it convenient and cost-effective to trust a service provider with the management of their VPN. Most service providers provide this service on a per-month/per-user basis and can provide additional security levels which may not have been considered.

IPSec VPN Security

IPSec (Internet Protocol Security) is the accepted security standard for Internet-based VPNs. IPSec has earned wide support and popularity because it is specifically built to secure communications over the public Internet. It can truly secure all network transactions over the Internet, regardless of the application.

IPSec addresses the most important security concerns, including:

- **Confidentiality and Integrity** - ensuring that data exchanges over the Internet are private and protected against unauthorized tampering
- **Authentication** - verifying the identity of any entity on the network, whether it be a user, application, or gateway

IPSec compliant VPN's provide the above protection through the use of strong cryptography. VPNs adhering to IPSec standards provide secure, standards-based communications between different entities in a network. In their initial connection, each pair of entities negotiates the security policy that is to be used in their following communications. Issues decided in this negotiation include the form of authentication, whether encryption will be used and the key lengths that will be used.

IPSec Authentication Options

IPSec mandates use of at least one of a variety of authentication methods including shared secrets, user names and passwords, tokens and/or digital certificates.

Shared Secrets

Shared Secrets are primarily used in site-to-site VPNs; they can be used, but are not recommended, for remote access VPNs. A shared secret is a private passcode exchanged between two entities so that they can establish a secure VPN between them. Typically, a unique shared secret is required for each pair of parties communicating over a VPN. The problems of scale in distributing and managing these secrets multiply as the number of VPN users grows. Shared secrets are typically distributed manually, making them practical only in small VPN deployments or where communication is strictly limited to within a small enterprise.

User Names and Passwords

Most VPNs come standard with username and password authentication. Each user and device has its own unique user identification name and password to access the VPN and the network behind it. Users often forget their password, use easy-to-guess passwords, or leave their password in an insecure place. Remote Access VPNs using passwords for authentication require significant help desk support (approximately 40% of all calls) and are easily compromised.

Proprietary Tokens

There are proprietary tokens available that do not make use of digital certificates. They require a server to be installed at the customer location, and use a proprietary encryption algorithm to produce a numeric password every 60 seconds. These proprietary tokens can be software or hardware based; decision makers need to take into consideration that these tokens are proprietary, require the VPN gateway to have the server agent to be embedded and cannot be used for digital signatures. Digital signatures are required to provide security to e-

mail (via the S/MIME protocol) and e-business transactions. In contrast, digital certificates are based on the X.509 standard, allowing VPN vendors to be compliant to this one standard. Companies that employ digital certificates with an IPSec VPN are not locked in with a proprietary solution from a single vendor.

Digital Certificates

By using a digital certificate to access several applications, support desk staff will have time to focus on other important issues. Digital certificates act as user passports, authorizing use of the VPN. These "passports" are issued to users from a trusted party. Digital certificates provide the most secure and scalable way to implement a VPN by giving companies the power to control user access, bind contracts with digital signatures, and create digital audit trails.

PKI systems provide a scalable and policy-based method to provide strong authentication and non-repudiation. PKIs have quickly become the cornerstone of all e-commerce and enterprise security designs and are set to dominate the security landscape into the foreseeable future.

A PKI provides the VPN with the facility to use strong authentication techniques, certificate management and support for certificate life cycles through the use of Certificate Revocation Lists (CRLs). Support for policy management within a PKI allows the VPN to enforce strict policy control at a granular level throughout a network.

By implementing a VPN that makes use of PKI, you gain significant cost savings while maintaining the highest level of security - which means you maintain the peace of mind that comes from a well controlled network while you also vastly improve the bottom line.

Smart Cards and Smart Tokens Using Digital Certificates

There are two major types of smart cards and smart tokens, those that use digital certificates and those that use a proprietary algorithm for encryption. Combining smart cards and smart tokens with digital certificates provides one of the strongest levels of authentication. The private key is generated on the smart card or token and never leaves the card. Therefore, it can not be accessed by unauthorized users or copied to a server.

Smart cards look like a credit card with a small embedded computer chip, and require the use of a smart card reader. Smart tokens come in a variety of shapes and sizes and some store digital certificates. The most popular are the size of a key chain, and can be plugged directly into a laptop or desktop USB port.

Biometrics

Using finger printing, retinal scanning, and voice printing combined with the use of digital certificates will provide an almost impenetrable form of authentication. But requiring biometric authentication for VPN authentication is currently cumbersome and expensive. Biometric readers would need to be distributed to outside constituents like partners, customers, and suppliers and would need to be carried by executives and road warriors in order to access the VPN. The combination of biometrics and digital certificates holds a lot of promise for VPN security in the future.

Benefits of Using Digital Certificates within a VPN

Users Are Added Easily

Adding a new user to the VPN and PKI requires only that the user be granted a digital certificate. New users simply apply for a digital certificate which is then approved by a Certificate Authority (CA). The CA issues certificates based on your organization's approval instructions, keeping you in control of the issuance of digital certificates to end users within your VPN.

Keys Managed Easily

Key updates can be automated. Also, the IT manager can easily remove selected users or groups of users from the system by revoking their certificates, without disturbing the rest of the system. The withdrawn certificates are added to a CRL which immediately disables the certificate holder from accessing the network.

Portability

Users can store their certificates and the public key of their CA on a smart card or smart token, carry it with them, and log onto the network securely from any workstation running the VPN client software.

Cross Certification

Cross-certification, in which two CAs issue certificates to one another, is particularly useful for extranets in which a VPN is formed among trading partners that each have their own CA. Any node in a combined VPN served by cross-certified CAs can then authenticate the identity of any other node. As a result, any two nodes in the system can communicate securely, subject to access control.

Scalability

Users are added to and removed from the network quickly and easily as opposed to the exponential increase in security management required in a symmetrical key implementation. Optional automatic authorization can be added for deployments with high numbers of users.

Flexibility

Digital certificates work on multiple platforms, with several software applications, and a wide variety of hardware devices. In addition to VPN authentication, digital certificates can be used for encrypting e-mail and data files, S/MIME, and SSL. As new technologies emerge, PKI will grow with your network and security infrastructure.

Strong Authentication

Certificates provide the strongest level of authentication a corporation can use to enable trust between relying parties.

Easy to Use

With new VPNs developed to CAPI compliance, end users will enjoy the transparency of digital certificates as they securely connect to your internal network.

Easy to Administer

IT will enjoy the simplicity of deploying a VPN with digital certificates as well as the reduced on-going burden that comes with eliminating passwords and shared secrets.

Deploying your VPN with Digital Certificates

Using a VPN Service Provider or Building It Yourself

First you must decide on whether or not to outsource your VPN. There are significant cost and time savings associated with outsourcing—with additional PKI security often included in the service package. Most major service providers are offering VPN services to help their clients avoid management and administration costs associated with implementing a VPN on their own. The primary limitation is that you will be locked into certain VPN equipment and technologies pre-chosen by the vendor, although most Managed VPN Service Providers will offer popular standards based equipment and software.

You will need to evaluate the geographic coverage, security, price, and scope of the VPN services in your decision process. Also, check which standards and protocols are supported by the ISP to ensure compatibility with the corporate hardware and software. Finally, ensure that the service provider offers the necessary service level agreements and network availability guarantees from the company's remote access locations to the central site, even when crossing over multiple ISP networks.

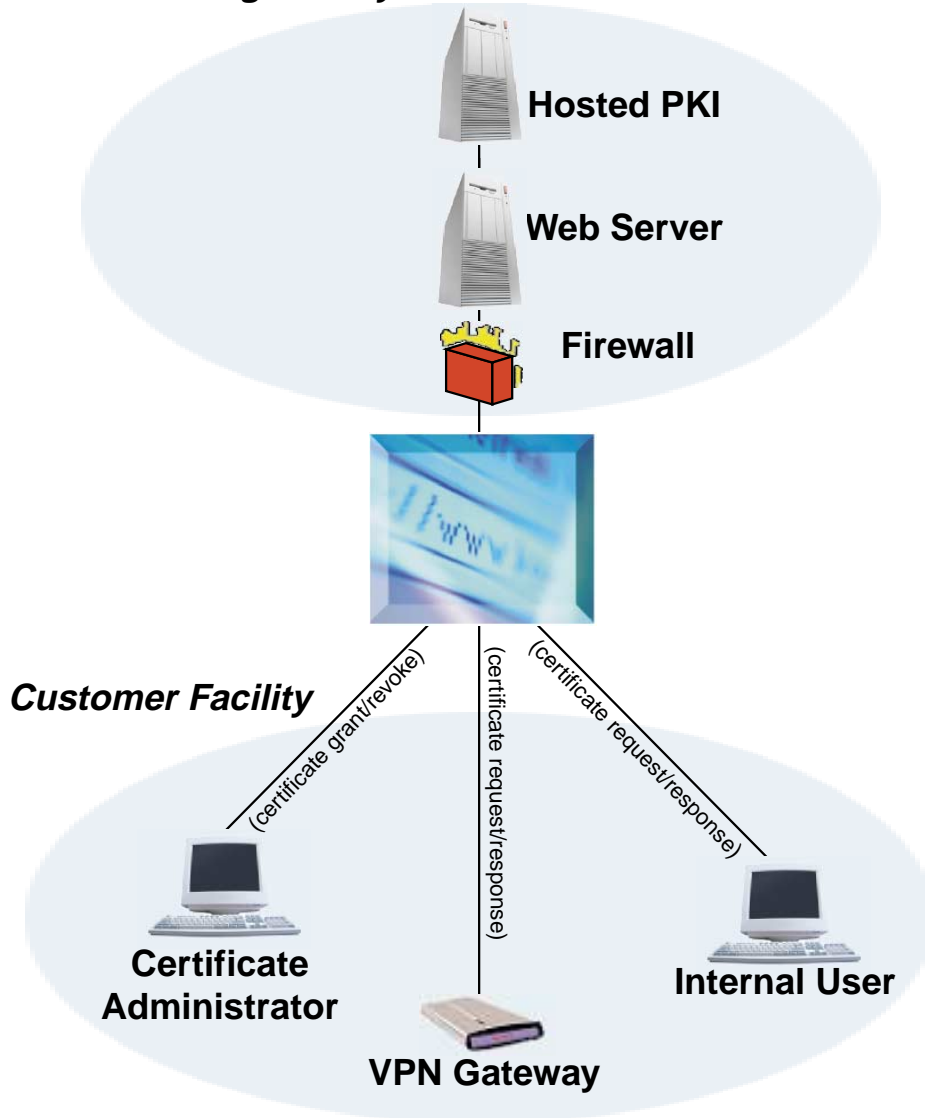
Outsourcing Your PKI or Deploying It Yourself

Next, decide on whether to outsource your PKI. Because PKI is a new technology to many IT managers, many are choosing to outsource it to Managed Security Service Providers (MSSPs) and PKI vendors. Compare the pricing models between a hosted PKI versus buying and deploying the software internally or against other security options. Also, evaluate the staffing requirements of all security options. Some companies prefer to start with their PKI hosted, and then plan to move the deployment in-house at a later date.

Not all PKI vendors offer their product as a managed service. For the benefit of customers wanting a low-cost and easy-to-manage PKI, a few PKI vendors and MSSPs offer an outsourced option that does not require the customer to implement any PKI component. The vendor or MSSP hosts and operates the PKI, but the customer controls how certificates are issued and revoked from a simple web interface. In many cases, an LDAP server will need to be deployed by the customer. The LDAP server is used for storing the CRLs. Often, the customer already has an LDAP server that can be used for this purpose. In some cases, the VPN device itself can be used to add and delete users, instead of using CRLs.

Outsourced PKI Model

Secure Hosting Facility



Summary

Organizations need secure communication lines between branch offices, remote employees, and outside constituencies. VPNs provide an inexpensive and convenient communication tool, and while VPNs provide basic encryption security, additional strong authentication is needed to ensure the right people are accessing your internal data resources.

With significant developments over the last few years, digital certificates are easier to deploy now than ever before into your VPN. You can develop and maintain both your VPN and/or PKI in house or outsource it to a vendor or service provider. New PKI standards make interoperability with your VPN easy, and the digital certificates are virtually transparent to the end user.

Digital certificates are the best authentication option for your VPN; shared secrets do not scale, passwords require significant support desk resources and are easily compromised, and proprietary tokens aren't as flexible. By implementing a VPN that makes use of digital certificates, you gain significant cost savings while maintaining the highest level of security - which means you maintain the peace of mind that comes from a well controlled network while you also vastly improve the bottom line.

Glossary of Terms

Term	Description
CA	Certificate Authority
CAPI	Microsoft's Crypto Application Programming Interface
CRL	Certificate Revocation List
DSL	Digital Subscriber Line
IP	Internet Protocol
IPX	Internetwork Packet Exchange
IPSec	Internet Protocol Security Standard
ISP	Internet Service Provider
IT	Information Technology
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Light Directory Access Protocol
MSSP	Managed Security Service Provider
PKI	Public Key Infrastructure
PPTP	Point to Point Tunneling Protocol
SCEP	Simple Certificate Enrollment Protocol
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network

Baltimore Technologies: Your Strategic Security Partner

Baltimore Technologies' products, services and solutions solve the fundamental security and trust needs of e-business. Baltimore's e-security technology gives companies the necessary tools to verify the identity of whom they are doing business with and securely manage which resources and information users can access on open networks. Many of the world's leading organizations use Baltimore's e-security technology to conduct business more efficiently and cost effectively over the Internet and wireless networks. Baltimore also offers worldwide support for its authorization management and public key-based authentication systems.

Baltimore's products and services are sold directly and through its worldwide partner network, Baltimore TrustedWorld. Baltimore Technologies is a public company, principally trading on the London Stock Exchange (BLM). For more information on Baltimore Technologies please visit

<http://www.baltimore.com>

www.baltimore.com