

Virtual Private Networks  
and  
The Automotive Network Exchange

by

Ronald G. Wolak  
wolakron@scis.nova.edu

A paper submitted in fulfillment of the requirements  
for DISS 840

School of Computer and Information Sciences  
Nova Southeastern University

January 1999

An Abstract of a Paper Submitted to Nova Southeastern University  
in Fulfillment of the Requirements for DISS 840

Virtual Private Networks  
and  
The Automotive Network Exchange

by  
Ronald G. Wolak

January 1999

Electronic commerce, industry supply-chains, and the use of virtual private networking are three complementary initiatives whose value has stimulated rapid growth. In recognition of this, the automotive industry, led by the Automotive Industry Action Group (AIAG), created the Automotive Network Exchange (ANX) in 1995. As proposed, the ANX will be the world's largest virtual private network (VPN) or "extranet." It will ultimately connect more than 10,000 automotive businesses. The ANX reached production status in January 1999. In the following pages, this paper began with a discussion of the rapid growth of business-to-business electronic commerce. The electronic commerce (e-commerce) initiatives of DaimlerChrysler, Dell Computer, and Ford Motor Company were examined. These were followed by a discussion of the use of extranets and virtual private networks (VPNs) as secure methods of conducting e-commerce. Current VPN protocols (i.e. SOCKS v5, PPTP/L2TP, and IPSec) were compared relative to their levels of security, industry acceptance, interoperability, and ease of implementation. Three VPN technology scenarios were also explored. These included intranet VPNs, remote access VPNs, and extranet VPNs. Following this general discussion of VPN networks and protocols, the paper proceeded with an in depth investigation of the ANX. Topics included ANX organizational structure, the ANX overseer, ANX certified service providers, ANX certified exchange point operators, ANX certified VPN/IP security companies, and ANX certification authority service providers. The paper concluded with a discussion of ANX trading partners, ANX vertical expansion, ANX global expansion, and ANX banking.

## Virtual Private Networks and The Automotive Network Exchange

Electronic commerce, industry supply-chains, and the use of virtual private networking are three complementary initiatives whose value has stimulated rapid growth. In recognition of this, the automotive industry, led by the Automotive Industry Action Group (AIAG), created the [Automotive Network Exchange \(ANX\)](#) in 1995. The automotive industry's creation of the ANX demonstrates its intention to exploit the benefits derived from the combination of these three initiatives.

As proposed, the ANX will be the world's largest virtual private network (VPN) or "extranet." It will ultimately connect more than 10,000 automotive businesses. The ANX reached production status in January 1999. In the future, the ANX project will expand electronic commerce in both the automobile industry and other worldwide markets. Procedures, guidelines, models, and technologies developed during its implementation will provide a basis for future growth in electronic commerce.

In the following pages, this paper begins with a discussion of the rapid growth of business-to-business electronic commerce. The electronic commerce (e-commerce) initiatives of DaimlerChrysler, Dell Computer, and Ford Motor Company are examined. These are followed by a discussion of the use of extranets and virtual private networks (VPNs) as secure methods of conducting e-commerce. Current VPN protocols (i.e. SOCKS v5, PPTP/L2TP, and IPSec) are compared relative to their levels of security, industry acceptance, interoperability, and ease of implementation. Three VPN technology scenarios are also explored. These include intranet VPNs, remote access VPNs, and extranet VPNs.

Following this general discussion of VPN networks and protocols, the paper proceeds with an in depth investigation of the ANX. Topics covered include ANX organizational structure, the ANX overseer, ANX certified service providers, ANX certified exchange point operators, ANX certified VPN/IP security companies, and ANX certification authority service providers. The paper concludes with a discussion of ANX trading partners, ANX vertical expansion, ANX global expansion, and ANX banking.

### Business-to-Business E-Commerce

Electronic commerce is projected to grow at staggering rates in the near future and a significant part of that growth will occur in the business-to-business segment. Fueling this growth is the Internet, which is proving to be an inexpensive and reliable vehicle for business communication and supply-chain transactions (Wilder, Dalton, & Davis, 1998). Use of the public Internet produces substantial savings over the use of private networks. As a result, a growing number of U.S. companies, including DaimlerChrysler, Dell Computer, and Ford Motor are expanding their Internet business links with both domestic and overseas suppliers, customers, and trading partners.

[DaimlerChrysler](#), for example, is stepping up its efforts in business-to-business e-commerce. Separate from the company's ANX efforts, Daimler is adding overseas companies to suppliers of maintenance, repair, and operational (MRO) goods via [GE Information Services' TradeWeb](#) (Wilder, Dalton, & Davis, 1998). TradeWeb uses the Internet to transport EDI data such as invoices, purchase orders, purchase-order changes, and remittance advances. Daimler plans to buy from more than 3,000 suppliers via TradeWeb by early 1999.

[Dell Computer](#) is another company with plans to link its overseas suppliers into a companywide effort to manage its entire supply-chain on the Web. Dell is conducting several pilots that will link its internal management systems to suppliers overseas. Unlike the automakers, Dell plans to use standard Internet technology to put its entire supply-chain online.

[Ford Motor Company](#) is also moving quickly into business-to-business e-commerce with its plans to convert most of its \$16 billion-a-year MRO purchases to the Internet by the end of 1999 (Temkin, 1998). Ford chose [Intelisys Electronic Commerce](#) (a software company specializing in procurement solutions) to create an Internet-based purchasing environment.

Ford will require its vendors to follow a proprietary implementation of the Open Buying on the Internet (OBI) standard. Intelisys offers three options to help Ford suppliers become compliant: 1) attach plug-in software to an existing Net catalog; 2) sign up for an off-the-shelf, hosted catalog; or 3) engage Intelisys partners like iCat and Open Market to build new custom catalog systems. Ford's adoption of the Intelisys solution will ensure that more than 3,000 of its vendors will be able to conduct business over the Internet by the end of 1999. The next step will occur when these suppliers extend their on-line capabilities to other business customers, creating a ripple effect that will eventually extend to tens of thousands of buyers.

While companies like Dell plan to employ standard web technology to link their supply-chains over the Internet, other businesses are looking to extranets as a more secure and reliable transport solution. In fact, as much as 40 percent of business-to-business e-commerce applications will be replaced by extranets before 2002, predicts Geri Spieler, a research analyst for [Gartner Group](#) (Horowitz, 1998). Eighty percent of the companies currently using e-commerce are expected to use extranets within five years.

## Extranets and Virtual Private Networks

The Gartner Group defines the term "extranet" as intranet-based applications and services that employ extended secured access to external users or enterprises. This is accomplished through passwords, user IDs, and other application-level security mechanisms. Therefore, an extranet is the extension of two or more intranets with a secure interaction between them. The extranet maintains control of access to those intranets within each enterprise in the deployment.

According to an online survey conducted by [InformationWeek Research](#), one in four businesses have created an extranet (Chabrows, 1998). Half of these businesses and nonprofit organizations provide extranet access to all customers. In addition, a study conducted in July 1998 by [Forrester Research](#) found the demand for extranets is derived primarily from marketing departments and customers. "Extranets have the potential to take over most business-to-business communications," says Barbara Ells, an analyst at [Zona Research](#) (Horowitz, 1998). Extranets save companies money. [Cisco](#), for example, saves money by speeding purchase order processing to a few hours, down from about a week, according to Richard Palmer (director of marketing in Cisco's Internet service provider unit).

The term "extranet" is usually found in business-oriented discussions while the similar term "virtual private network" is often found in technology-oriented discussions (Covill, 1998). The two terms have come to mean the same thing--namely, using Internet technology to communicate, and share information with a specific set of trading partners both inside and outside the enterprise. Specifically, a virtual private network (VPN) is a private data network that uses the public telecommunication infrastructure.

A VPN takes information (originally designed to travel across a proprietary network and therefore has a proprietary wrapper) and compresses it, encrypts it, and places it in a TCP/IP wrapper. This allows the information to travel or "tunnel" across the Internet. At the destination, the information is unwrapped, decompressed, decrypted, and used in some business setting. VPNs enables corporations to open their Intranet web sites to suppliers, contractors, and customers. The network that results from the opening of proprietary web sites to a limited set of outsiders in order to share information and collaborate is called an extranet.

## **VPN Protocols**

Although VPN security products are still quite young, a handful of protocols have emerged as the leading choices for building VPNs. The following protocols are currently the most widely deployed (Kosiur, 1998).

### *SOCKS v5.*

The [Internet Engineering Task Force](#) (IETF) originally approved SOCKS v5 as a standard protocol for authenticated firewall transversal. When combined with Secure Sockets Layer (SSL), it provides the foundation for highly secure VPNs. SOCKS v5 is best applied in applications requiring the highest security levels, since access control is its strength. SOCKS v5 was developed in 1990 by David Koblas and has received widespread support from companies such as Microsoft, Netscape, and IBM.

SOCKS v5 controls the flow of data at the session or circuit layer. This maps approximately to layer five of the OSI networking model. Consequently, SOCKS v5 provides more detailed access control than protocols operating at lower layers. SOCKS v5 establishes a virtual circuit between a client and a host on a session-by-session basis

and provides monitoring and strong access control based on user authentication without the need to reconfigure each new application.

SOCKS v5 is unique in its use of directed architecture. Directed architecture protects destination computers by proxying traffic between source and destination computers. When used in conjunction with a firewall, data packets are passed through a single port in the firewall (port 1080 by default) to the proxy server. Another advantage of SOCKS v5 is that the client is non-intrusive. It runs transparently on the user's desktop and does not interfere with networking transport components.

Since SOCKS v5 adds a layer of security by proxying traffic, its performance is lower than that of lower-layer protocols. Though it is more secure than VPN protocols located at the lower network layers, the extra security requires sophisticated policy management. Also, client software is required to build a connection through the firewall to transmit all TCP/IP data through the proxy server.

#### *PPTP/L2TP.*

One of the most widely known VPN security choices is Point-to-Point Tunneling Protocol (PPTP) from Microsoft. It is embedded in Microsoft Windows NT v4.0 and is used with Microsoft's Routing and Remote Access Service. PPTP operates at the datalink layer (i.e. layer two of the OSI model). It encapsulates PPP with IP packets and uses simple packet filters to provide access control. PPTP and its successor, Layer Two Transport Protocol (L2TP) extend the PPP dial-up infrastructure supported by Microsoft and most ISPs.

L2TP evolved from the combination of Microsoft's PPTP protocol and Cisco System's Layer 2 Forwarding (L2F). It supports multiple, simultaneous tunnels for a single client. When using L2TP, a remote user, dials up a local ISP without encryption. The ISP then creates an encrypted tunnel back into the secure destination. Both PPTP and L2TP have received broad support from companies such as Cisco, Bay Networks, 3Com, Shiva, and Microsoft, because they are an effective way for these companies to migrate their existing dial-up products to Internet-based tunneling.

Most VPNs only secure TCP/IP traffic, but PPTP and L2TP support additional networking protocols such as Novell's IPX, NetBEUI, and AppleTalk. They also support flow control and enhance network performance by minimizing dropped packets. One limitation of PPTP and L2TP is their maximum of 255 concurrent connections. In addition, end users are required to manually establish a tunnel before connecting to the intended resource. Also, the selection of authentication and encryption standards is very limited. Currently strong encryption and authentication are not supported.

#### *IPSec.*

IP security (IPSec) is a security protocol from the IETF that provides authentication and encryption over the Internet. IPSec evolved during the development of IPv6. IPSec is a broad-based, open solution for VPN security that facilitates interoperability between VPNs. It can be configured to run in two distinct modes (i.e. tunnel mode or transport

mode). In tunnel mode, IPSec encapsulates IPv4 packets within secure IP frames to secure information from one firewall to another. In transport mode, information is encapsulated in such a way that it can be secured from endpoint to endpoint. The security wrapper does not obscure the end routing information as it does in the tunnel mode. Tunnel mode is the most secure method for deploying IPSec. However, this security results in significant overhead on a per-packet basis.

One advantage of IPSec is that it defines a set of standard protocols for authentication, privacy, and data integrity that are transparent to the application and the underlying network infrastructure. Unlike PPTP, IPSec supports a variety of encryption algorithms, such as DES (Data Encryption Standard), Triple DES, and IDEA (International Data Encryption Standard). It also checks the integrity of transmitted packets to make sure they have not been tampered with en route.

IPSec is designed to provide security between multiple firewalls and routers. This makes it well suited for LAN-to-LAN VPNs. IPSec client-to-server configurations require a public key infrastructure (PKI). In addition, IPSec implementations require a known range of IP addresses or fixed IP addresses to establish identity. This makes IPSec impractical in dynamic address environments.

### **VPN Technology Scenarios**

At a minimum, a VPN should encrypt data over a virtual connection over the Internet in order to protect the information from being understood if intercepted. Beyond this basic requirement, VPNs customarily include tools for authentication, integrated access control, and authorization. Strong authentication and encryption are relatively simple to deploy and verify. Access control, on the other hand, is complex because tied directly to every other security tool. The security of a VPN is a function of how closely authentication, encryption, and access control are connected (Kosiur, 1998)

VPN configurations typically incorporate a firewall, router, proxy server, VPN hardware and software, or all the above. In addition, VPNs may be deployed as three internetworking types. These include secure connections:

1. between a corporation and its branch offices (i.e. intranet VPN),
2. between a corporation and remote or traveling employees (i.e. remote access VPN),
3. and between a corporation and its trading partners (i.e. extranet VPN).

#### *Intranet VPNs.*

Intranet VPNs are defined as semi-permanent WAN connections over a public network to a branch office. This type of LAN-to-LAN connection is assumed to carry the least security risk because companies trust their branch offices and consider them an extension

of the corporate network. In this case, the corporation controls both the source and destination nodes.

When endpoints of a data channel are trusted, companies typically decide on a VPN solution that focuses on performance over security. Security in this case is limited to the strength of encryption and authentication methods between routers. High volumes of data are typically exchanged between LANs on an intranet VPN and a premium is placed on speed and interoperability.

In companies concerned with security threats from within, an alternate VPN solution would control the information flow on an authenticated, user-specific policy level rather than on a trusted subnet basis. In this type of highly secure intranet VPN, only certain employees at the branch office have access to corporate resources (each with a different set of permissions). Data transferred across the Internet is encrypted and authenticated all the way to the endpoints, not just to the network perimeter.

#### *Remote Access VPNs.*

Remote Access VPNs are more affordable than traditional direct dial-up remote access methods. Corporations, incurring the expense of maintaining large modem pools and the expense of long distance charges, are finding remote access VPNs less expensive and easier to implement and maintain than the alternatives (Gasparro, 1997). Most remote access VPNs are configured under the assumption that a corporation trusts the person using the link (typically a remote salesperson). This translates to a "transparent access" policy. In other words, remote employees are able to access all resources normally available to them when directly connected to the corporate LAN.

In this scenario, encrypting the data in transit is the priority. Most VPNs meet this basic security requirement. Typically, a remote user logs onto the Internet through a local ISP and establishes an encrypted tunnel between his or her desktop and the perimeter of the corporate network. User identity is unknown, only the IP address of the computer is identified.

An alternate scenario is one in which highly secure remote access is required, the VPN is configured so that remote employees have tightly controlled access to specific resources on the network. Resource permissions are dependent on the employee's job function. Secure policy-driven VPNs of this type; authenticate individual users, not just IP addresses. Consequently, a corporation knows which employee is gaining access to the network. Authentication is accomplished through common passwords, digital certificates, token cards, smart cards, or biometrics (e.g. fingerprint or iris scanning). Once an employee has authenticated to the corporate VPN server, he or she is granted a certain level of access depending on his or her profile.

#### *Extranet VPNs.*

Unlike intranets that are isolated, extranets are required to reach trading partners, customers, and remote employees. Extranet VPNs provide a hierarchy of security, with access to the most sensitive data placed under the tightest security control. Typically,

extranet VPNs secure all applications, including TCP and UDP applications, such as Real Audio, FTP, etc.; corporate vertical applications, such as SAP, BAAN, PeopleSoft, and Oracle. Corporate VPN solutions must be extremely versatile and interoperable with multiple platforms, protocols, and authentication and encryption methods.

In an extranet VPN, security elements (i.e. encryption, authentication, and access control) are tightly integrated with some type of perimeter security. Companies usually place a VPN proxy server behind an impenetrable firewall that blocks all unauthenticated traffic. Any traffic that is allowed to pass is funneled through a common portal directly to the VPN server. This server filters the traffic according to company policy.

The most secure extranet VPNs are built around a "directed" architecture, as opposed to a bi-directional "tunneled" method. Directed VPNs transmit encrypted information to a higher level in the networking protocol stack than tunneled VPNs. Security and control increase as functionality moves up the network hierarchy. Directed VPNs act as proxy servers (i.e. they do not open any direct connections into corporate networks. This prevents IP addresses from being "spoofed" or mapped. Tunneling hides information in IP packets at the packet level, exposing them more easily to attack. Since all data is proxied in directed VPNs, network administrators are able to determine who has been trying to gain access to the network.

Unlike tunneled VPNs, directed VPNs protect connected networks from each other's security flaws. Directed VPNs do not assume a trusted relationship between connecting parties. If security is breached in the directed model, only the attacked network is exposed. In the tunneled model, when one network is attacked, each successive network is susceptible to the same attacker. The directed model allows each company to set its own access privileges and not expose its network to unknown security problems.

When companies conduct business transactions over the Internet, simple encrypted tunnels are not adequate. Extranet VPNs should use the highest encryption available (i.e. 128 bit). In addition, the VPN should support multiple authentication and encryption methods since business partners, suppliers, and customers have varying network infrastructures and platforms. Perhaps the best example of this type of highly secure extranet VPN is the Automotive Network Exchange (ANX).

### AIAG's ANX Project

The [Automotive Industry Action Group](#) (AIAG) is a nonprofit trade association of North American automobile manufacturers and suppliers (AIAG, 1998). The association's members include the Big Three along with over 1200 automotive supplier companies. The mission of the AIAG is to improve the global productivity of the North American automotive industry. This is accomplished by providing an organization that:

- Fosters cooperation and communication among trading partners to improve and reduce variation in business processes and practices.

- Addresses existing and emerging common issues and applies new and current technology to increase the efficiency of the industry.
- Promotes a sense of urgency in adopting developed business practices.
- Cooperates and communicates with other industry, government, and technical organizations.

The AIAG organization consists of a board of directors, an executive director, associate directors, a full-time staff, and volunteers serving on project teams. The executive and associate directors are executives on loan from member companies.

AIAG member committees focus on business processes and supporting technologies. These committees research, develop, and provide training on standard business practices in a variety of areas. These include automatic identification, CAD/CAM, EDI/electronic commerce, continuous quality improvement, materials and project management, returnable containers and packaging systems, and transportation/customs. Key AIAG projects are Auto-STEP, MAP, Quality/QS-9000, Autochain Online, Year 2000, and ANX.

In 1994, the AIAG published the document "Trading Partner Data Telecommunications Protocol Position." This document recommended that TCP/IP become the standard for transport of automotive trading partner electronic information. The ANX project was launched shortly thereafter in December 1995. The project was the result of the AIAG's decision (in the second quarter of 1995) to adopt the document's recommendations. The TCP/IP endorsement was in recognition of market trends (i.e. the explosive growth of the Internet) along with the rising use of Internet technologies for applications running within AIAG member companies. The initial goal of the ANX project was to develop a plan to implement data communication links between trading partners and to deliver a functioning extranet as the end result.

The ANX is an IP-based virtual private network for managing the automotive industry supply-chain. GM, Ford, Chrysler, and their suppliers and dealers support it. Initially, three implementation options were considered for the ANX. These included the public Internet, private network expansion, and virtual private network services. A fourth option - the ANX model - was finally adopted. The ANX model consists of:

- Multiple service providers certified by an ANX Overseer company.
- All certified providers required to interconnect with each other.
- Pricing to be comparable to existing VPN services.

The goal of the ANX project is to save \$1 billion annually or \$70 per car. This will be accomplished by optimizing information flow within the supply-chain by reducing information lead-time. Direct savings will be derived from the following:

- Consolidation of multiple communication links.
- Elimination of transaction-based charges.
- Elimination of carrier management cost of multiple links.
- Reduced maintenance costs and staff expenses.
- Reduced hardware and software costs.

Indirect savings include the ability to:

- Carry out business strategy more effectively.
- Service new customers more quickly.
- Support strategic partnerships more readily.

In short, the ANX will replace the intertwined web of connections that currently connect automotive suppliers and manufacturers with a single, secure IP-based network.

### **ANX Organizational Structure**

The AIAG Implementation Task Force (ITF) and the Telecommunications Project Team (TPT) are responsible for the ongoing operation of the ANX Network. The ANX Business Manager is a full-time agent of the ITF and is responsible for network planning and operational issues. The ANX Business Manager also reports the appropriate AIAG manager for AIAG-related administrative functions.

The ANX Overseer (ANXO) company directs all operations and management responsibilities of the ANX. The ANXO is under contract to the AIAG, and it reports indirectly to the ITF and the AIAG via the ANX Business Manager. ANX Certified Service Providers (ANX CSPs) and ANX Exchange Point Operators (ANX CEPOs) provide the technical and physical infrastructure for the network. Every ANX CSP interoperates with all other ANX CSPs. ANX CSPs and CEPOs are independent business entities that manage their own services and facilities. Before certification, both must commit to very specific services level agreements with ANX subscribers. Their compliance with these objectives is closely monitored by the ANXO.

### **ANX Overseer**

[Bellcore](#) was selected as the ANX Overseer (ANXO) in May 1998 (ANX Press Release, 1998). Bellcore is a leading provider of communications software, engineering, consulting, and training services. As ANXO, Bellcore provides administrative services such as security certificate handling, trouble handling, dispute resolution, and ANXO

help desk services. In addition, Bellcore administers certification services for service providers and registration services for automotive trading partners.

To become an ANX CSP or an ANX CEPO, service providers must sign a contract with Bellcore. The process is as follows:

1. A service provider requests an ANXO Service Provisioning Package from the ANXO. This package includes the terms and conditions of certification, a fee schedule, registration form, and application form.
2. Service providers purchase ANX Release 1 Document. This document specifies service quality requirements in eight categories.
3. Service providers need to pass ANX registration, ANX certification assessment, and ANX certification verification. Bellcore administers and works with each service provider throughout this certification process.

The ANX Release 1 Document also outlines Bellcore's role in registering automotive trading partners. The process is as follows:

1. Trading partners first obtain sponsorship from an Authorizing Trading Partner (e.g. DaimlerChrysler, Ford, or GM).
2. Once sponsored, trading partners contract with the ANXO and obtain an ANXO Service Provisioning Package for Trading Partners. This package includes the terms and conditions for ANX registration and subscription.
3. Trading partners must pass through ANX registration and subscription. Bellcore is responsible to assist each trading partner throughout this process.

### **ANX Certified Service Providers**

ANX certified service providers (ANX CSPs) are ISPs that have demonstrated compliance with ANX-specified requirements for network service features, interoperability, performance, reliability, business continuity, disaster recovery, security, customer care, and trouble handling (Bradner, 1998). ANX CSPs are also connected to one or more ANX certified exchange points. Security is perhaps the most important of the many service features that the ANX requires an ANX CSP to offer.

All ANX CSPs must be part of a public-key certificate hierarchy that is administered by the ANX. This certificate hierarchy is used to enable the ANX-wide use of the IP Security set of functions to protect and authenticate transactions between trading partners. Since each ANX CSP must have an approved public-key certificate (used in real time to authenticate the CSP), the ANX is able to decertify CSPs that are unable to maintain network quality of service standards. Before de-certification, the ANX will provide a structured set of warnings.

Recently, the AIAG approved the first three certified service providers (Pappalardo, 1998). [Ameritech](#), [Bell Canada](#), and [Electronic Data Systems](#) (EDS) were certified after passing the service-level tests. Trading partners can now connect to the ANX via their services. The ANX's stringent performance tests were in part responsible for a delay in the ANX's rollout. For example, CSPs must provide support with:

- A minimum latency of 125 msec from network edge to edge.
- A maximum of 10 lost packets for every 10,000 sent.
- A network uptime of 99.5 percent

Other ISPs currently in the process of obtaining CSP certification include [MCI](#), [Concentric Network](#), and [AT&T](#). However two large ISPs, [UUNET](#) and [GTE Internetworking](#), have stated they are not seeking certification at this time.

Gaining AIAG certification is important for ISPs because the AIAG plans to make ANX VPN available to other vertical industries, such as health care, insurance, and finance according to Karl Schohl, ANX Business Manager. It is also anticipated that the list of approved ANX CSPs will soon become the approved ISP list for many organizations that are unrelated to the automotive industry.

Recognizing the value of ANX certification, Ameritech's began its AutoVAN service (Dalton & Davis, 1998). AutoVAN provides businesses with all equipment and service required to access the ANX network. AutoVAN services include managed router service and either frame relay, switched multimegabit data services (SMDS) or asynchronous transfer mode (ATM). Access speeds range from 56 Kbps to T3 (45 Mbps). Ameritech also offers managed firewall service, IPSec devices, configuration, and other consulting services. Trading partners are also able to use AutoVAN service to access the public Internet and the private Electronic Business eXchange, another extranet connecting essential business partners who are not ANX members.

Similar to Ameritech's AutoVAN service, Bell Canada's competing product is [AutoLinx](#). In conjunction with the AIAG, Bell developed the concept behind ANX and was involved with the ANX design team since 1995. Bell developed the first Canadian extranet, an IP automotive network connecting one of the original equipment manufacturers to its trading partners. This extranet provided the vision for the ANX.

During the five month ANX pilot process, EDS, another ANX CSP, also played an important role (Capps, 1998). EDS worked with five major automotive original equipment manufacturers (OEMs) and 35 trading partners scattered across the U.S. and Canada. Instead of using "test data" for the pilot, EDS moved production data across the network. According to GM's Manager of Corporate Networks, Arvind Sabharwal, EDS played an integral role in the movement of production data across the network during the pilot. "GM was able to get a true sense of how information migration will work," said

Sabharwal. During the pilot process that ended in November 1998, EDS maintained availability of more than 99 percent.

### **ANX Certified Exchange Point Operators**

ANX Certified Exchange Point Operators (ANX CEPO) provide ATM-based network services to interconnect ANX CSPs. Certified exchange point operators must demonstrate 100 percent compliance to ANX Service Quality requirements for (1) interoperability, (2) performance, (3) reliability, (4) business continuity and disaster recovery, (5) security, (6) customer care, and (7) trouble handling.

In December 1998, the AIAG and Bellcore certified Ameritech Advanced Data Services as the ANX's first CEPO (Simmons, 1998). As the first CEPO, Ameritech's role in the ANX is expanded to provide connections between ANX CSPs. Ameritech's exchange points house the required high-speed electronics and software to allow CSP connections to interoperate or peer. "With the certification of Ameritech as the first ANX CEPO, the ANX network is operationally ready to significantly reduce current and future communication costs throughout the automotive supply-chain," said Richard T. Simmons, AIAG executive director.

During the ANX pilot phase, Ameritech acted as the network's exchange point operator. In that role, it determined the technologies and architecture needed to meet the needs of ANX CSPs. Those needs included migration to an ATM-based exchange point, network redundancy requirements, CSP bandwidth considerations, routing and directory information storage and services, and quality of service documentation.

Finally, the ANX's goal is to bring the benefits of the electronic commerce revolution to the automotive industry. The ANX service will deliver the reliability, performance, and security required of a business quality network while supporting all automotive applications. ANX service will shortly become the universal method for automotive trading partners to access each other's business applications. The ANX provides the opportunity to solve the data communications problem once instead of one trading partner and application at a time. New applications will be deployed faster, and eliminating redundant connections will reduce communications costs. The ANX's mission is to create an environment that maximizes the ability of each trading partner to compete efficiently.

### **ANX Certified VPN/IP Security Companies**

In addition to signing up with a certified service provider and the AIAG, trading partners must also choose one of eight approved IP Security (IPSec) vendors (Pappalardo, 1998). Working with the AIAG, the International Computer Security Association (ICSA) conducted extensive testing that resulted in the certification of [Axent](#), [Check Point Software Technologies](#), [Cisco](#), [IRE Secure Solutions](#), [Network Associates](#), [Radguard](#), [TimeStep](#), and [VPNnet](#) as interoperable IPSec gateways. The testing also certified that the

gateways complied with the pending IETF IPsec standard. IPsec is a security protocol that provides authentication and encryption over the Internet.

The ICSA began testing VPN products for the AIAG in May 1998 (Saunders, 1998). The VPN products were tested for compatibility with competitor offerings, as well as for their cryptographic abilities, according to Don Krysnaowski, ICSA lab director. ICSA took over testing from the AIAG, which had run a series of in-house "bake-offs" with several VPN companies to see how well different products worked together. The eight VPN companies currently certified have products that range from firewall management to comprehensive VPN systems.

VPN Technologies (a VPN pioneer) was one of the eight VPN companies chosen to support the ANX (Clark, 1998). VPN Technologies was founded in 1995 and is based in San Jose, California. The company develops, manufactures, and markets high performance VPN products. All of the company's domestic products support Triple DES encryption. DES is a National Institute of Standards and Technology (NIST) standard secret key cryptography method that uses a 56-bit key. Triple DES is an enhancement of DES that provides considerably more security than standard DES.

"The ANX project represents one of the best objective validations of VPN technology," said Raymond Keneipp, principal analyst, carrier infrastructure, at [Current Analysis](#). "Since the ANX project represents one of the largest, if not, the largest extranet in the country, the VPN products in this test must lead the industry in security and scalability. VPN Technologies is one of the pioneers of VPNs and was among the first vendors to deploy working solutions in real business applications." In fact, a number of industries have established "ANX Certification" as a requirement for their approved VPN products.

### **ANX Certification Authority Service Providers**

One important piece of the IPsec standard is the use of digital certificates for authentication. All ANX users are required to use X.509 digital certificates to authenticate and identify users before establishing an encrypted session over the ANX VPN. The AIAG is using [Digital Signature Trust](#) (DST) as its Certificate Authority Service Provider (CASP). Interoperability issues among certificate authorities have led the AIAG to use only Digital Signature Trust. Other certificate service providers will be added as interoperability issues are worked out.

DST is one of the key providers of trusted Public Key Infrastructure (PKI) solutions for secure communications and electronic commerce. DST (a subsidiary of Zions First National Bank) was formed in 1996 in response to the nation's first digital signature law, the Utah Digital Signature Act (FAQs, 1998). DST manages the central ANX Repository in which ANX Certificate Policy, ANX Certificate Profile, all ANX Certificates, and ANX Certificate Revocation Lists (CRLs) are stored. This online database provides real-time ANX certificate validation.

Working closely with the AIAG and Bellcore, DST developed the legal and policy infrastructure governing the use of the digital certificates used to secure the network. This work included:

- Creating the world's first industry-wide certificate policy.
- Developing the IPsec certificate used in phase one of the ANX rollout.
- Building a certificate registration process for trading partners to request ANX certificates.

DST launched the ANX certificate program September 1998 and issued the first IPsec certificate in the ANX production environment. Through its TRUST source plus certification authority services, DST issues certificates to ANX trading partners and manages all facets of the certificate life-cycle. Users seeking to verify a certificate's status access DST's TRUST eXchange (managed repository for ANX certificates). TRUST eXchange enables users to communicate over the ANX network with total assurance of the identity of the sender and the privacy and integrity of their transactions.

### **ANX Trading Partners**

As of November 1, 1998 (ANX's full production launch date), 3,699 automotive trading partners were ANX sponsored. ANX sponsorship is the first step in connecting to the ANX network. Trading partners next become contracted, registered, and finally subscribed. Currently, 14 companies are ANX subscribed. They are Borg-Warner, Caterpillar, Chicago Rawhide, Dofasco, Ford, Freudenberg-NOK, GM, Interautomation, Magna, Methode Electronics, MSX, Seeburn, Taylor Steel, and United Technologies Automotive.

[Taylor Steel](#) is among the list of ANX subscribed companies. Taylor is a Stoney Creek, Ontario automotive supplier that receives large coils of sheet steel from mills and cuts them down to narrow coils (Anonymous, 1998). These coils are then shipped to stamping companies. The company communicates with customers via a dial-up EDI connection. This dial-up connection is slow and in cases where customers are located a few minutes away, the truck usually arrives before the electronic order does.

During its participation in the ANX pilot implementation, Taylor demonstrated the ability of the ANX to eliminate this problem. Since Taylor and one of its customers, [Dofasco](#), were both ANX pilot members, they began using the ANX to replace the slow dial-up connection. Consequently, Taylor now receives Dofasco's EDI orders in half the time and the truck arrives after the ANX message. Also, ANX use reduced Taylor's phone charges by 75 percent.

[DaimlerChrysler](#) is another trading partner committed to the success of the ANX. According to Thomas Stallkamp, DaimlerChrysler President, the company is committed to use the ANX as it enters the production stage this year. Daimler's plans include

migrating e-mail, interactive CAD, EDI, and the majority of its other applications to the ANX. The ANX will be used at Daimler to electronically route product shipment schedules, order information, CAD files for product designs, purchase orders, and other financial information.

The improved exchange of information will result in new business practices between Daimler and its vendors. "They'll be holding information rather than inventory" stated Laura Migliore, a Daimler process control specialist. Daimler also hopes the ANX will help it alleviate chronic design cycle problems by allowing it to collaborate in real time with its suppliers (Merkow, 1997). Daimler's ANX connection will enable simultaneous engineering using multiple workstations or graphics terminals to run finite element analysis software, solid modeling CAD packages or even high-speed prototyping. The network will provide the guaranteed bandwidth, not just for CAD/CAM but also for applications such as advanced videoconferencing and three dimensional virtual reality design sessions. Connection to the ANX will cut Daimler's cost of doing business and aid in reducing the current five-year product design cycle down to less than three years.

[American Axle and Manufacturing](#) (AAM) is a trading partner that is registered to become a subscribed ANX member. AAM (headquartered in Detroit, Michigan) is a growing, multi-billion-dollar manufacturer of automotive driveline systems. Unlike the trading partners described above, AAM decided only recently to connect to the ANX. Following that decision, AAM chose EDS to be its certified service provider. EDS was also contracted to integrate the ANX into AAM's existing WAN infrastructure. Together the two companies developed the following three-phase implementation plan (Daum, 1998):

#### Phase I - Initial Implementation

- Support AAM with planning and design expertise.
- Assist AAM with completion of ANX subscription requirements.
- Assist with ANXO subscription assessment testing.
- Establish T-1 connection to EDS ANX Services.
- Access Router - installed, managed, and configured by EDS ANX Services.
- DNS Services - Primary housed on AAMPUB1, secondary housed by EDS.
- Configure and install AAM DMZ and public segments.
- Register IP Addresses and domain name registration for AAM DMZ.

- Remote access dial-up services provided by EDS ANX services.
- Establish naming conventions and name advertising for DMZ devices and servers.

#### Phase II - Extend Connectivity to Include the Internet

- Internet access provided by EDS ANX services, routing performed at CSP.
- DNS servers updated to include Internet addressing.
- Router tables updated to include Internet routes.
- Establish Internet use policy guidelines.
- Setup proxy rules on DETFW1 to manage Internet and ANX usage by user/group.

#### Phase III - Integration of ANX Services

- Install and configure AAM public network server.
- Install and configure Exchange SMTP gateway server.
- Install and configure WWW/FTP server on DMZ.
- Plan to integrate outside supplier connection requests to use their existing ANX connection.
- Develop plan for making internal application data available via ANX.
- Design and implement a secure VPN based on ANX IPsec and firewall devices to connect AAM locations in Japan and Mexico.

Recently AAM and EDS completed the first two phases of their ANX implementation plans. Phase three is underway, and select AAM users are currently able to access the Internet via the companies dedicated ANX link. Phases one and two took 90 days to complete. Phase three has a planned completion date in the last quarter of 1999. The fast ANX implementation thus far at AAM is evidence of the AIAG's success in producing a viable production network.

#### **ANX Vertical Expansion**

The AIAG plans to make ANX available to other vertical industries. One example is a group of health care organizations that are holding talks with the AIAG about becoming

ANX participants (Wallace, July 1998). Health care organizations would use the ANX to verify patients' insurance coverage, submit claims, and gather administrative data. Once privacy and security concerns were addressed, confidential patient medical information would be transported.

In addition to networking with other in the health industries, health care organizations would be able to link with the automakers and other partners on the VPN. "It would be a plus for us and the health care people by expediting transactions and cutting cost," said Wally Mashini, project leader for health care and safety at Ford Motor. "There would be a dynamic exchange of data instead of it taking a month or more to get information."

Barbara Horwitz, a member of the Michigan Health Management Information Systems group, recently piloted a health care standard whereby hospitals check patient coverage eligibility over the ANX instead of by phone calls. In the pilot, the process that used to take between 30 seconds and 20 minutes was shortened to 15 seconds. In addition, the cost per transaction dropped from a range of 50 cents to five dollars to only four to six cents.

### **ANX Global Expansion**

The ANX is also planning to become a global service. Although existing ANX quality metrics and production development are based on North American requirements, future releases are planned to include areas such as Europe, South America, Australia, and Japan. AIAG executives confirmed recently that the group is actively working to expand the ANX globally (Wallace, September 1998). The AIAG is pursuing a cooperative agreement with the European auto association and the Japanese Auto Manufacturers Association to extend the ANX globally. The network is currently limited to the U.S. and Canada. "We're trying to make ANX a global network that the entire industry can take advantage of," said Don Hedeem, ANX director. Hedeem's next step is to extend the ANX into Mexico and the many automotive manufacturing installations there.

In 1997, the AIAG developed a formal ANX Memorandum of Understanding (MOU) to share information and jointly develop the ANX service in Europe with the European auto association called the Organization for Data Exchange by Tele-Transmission in Europe (ODETTE). There are currently three ANX European national projects underway in Europe (i.e. France, Germany, and the United Kingdom). Projects are beginning in Italy and Spain. Details of projects in Europe and the rest of the World are as follows:

- Italy - The national organization ODETTE Italy is leading the adaptation of ANX for Italy. Meetings have been planned.
- Spain - The national organization ODETTE Spain is leading this national effort. A working group comprised of Dalphi Metal, Fasa Renault, Fiat, Michelin, Sogedac, Telefonica, Teleinformatica, and VW-Gedas is investigating the ANX concept. A pilot is under consideration.

- France - The national organization Groupement pour l'Amelioration des Liaisons dans l'Industrie Automobile (Galia) recently developed an ANX concept and potential pilot in France. The pilot will be called Project Rapides (Pilot Automotive Network for Secure Exchanges). Trading partners include Cockerill Sambre, Eurostyle, Labinal, Michelin, PSA, Renault, Sollac, and Valeo. Project work groups are currently working to analyze the opportunity offered by ANX technology, adapt it to the French environment, and assure global interoperability.
- United Kingdom - The national organization ODETTE U.K. and the Society of Motor Manufacturers and Traders (SMMT) have developed an ANX concept. A pilot, which began in late 1998, includes Automotive Parts, British Telecom, Ford, GM, Perkins, Rover Group, Toyota, Unipart, and Worldcom (UUNet). Pilot objectives include the determination of national service quality requirements.
- Germany - The national organization Verband der Automobilindustrie (VDA) has developed the Automotive Network (ANET) concept and architecture. In addition, the VDA has developed country-specific quality metrics based upon ANX Release 1. An ANET pilot service was recently begun. This pilot includes trading partners Audi, Behr, Bosch, BMW, DaimlerChrysler, Deutsche Telekom AG Draxlmeier, Ford, Freudenberg NOK, Hella, Opel-GM, Siemens, Volvo, and VW. Issues to be addressed include the internetworking of global exchange points, security implementation considerations, and a global ANX Overseer (GANXO). This new global overseer will ensure consistent administration and management of the network.
- South America - AIAG and ODETTE are in the process of identifying interested national organizations. MOUs with country-specific automotive groups will be established.
- Japan and the Pacific Rim - Informal ANX information transfer has been established between the AIAG and the Japan Automobile Manufacturers Association (JAMA). In anticipation of a migration to ANX, Japanese automaker Mitsubishi is replacing its 10-year-old proprietary FDDI-based system that runs its plant floor operations with TCP/IP-based networking (Frook, 1998).
- Australia - The national organization Federal Chamber of Automotive Industries (FCAI) is leading the national effort. An Australian ANX committee was established in mid-1998. This committee is comprised of Ford, FAPM, Holdens, Mitsubishi, MTAA, and Toyota representatives.

Expanding the ANX overseas will be very beneficial to U.S.-based automakers. Every major automotive company is a global player with global supply-chain issues. Joe Boyd, a telecommunications analyst at Ford, commented that the company needed the flexibility to support suppliers on other continents with applications located on servers in North America. A global ANX would meet these requirements.

## **ANX Banking**

Through the ANX, auto companies will distribute their product specifications, price, quantity, and delivery date requirements for auto parts and components to suppliers. The ANX will also be used to negotiate terms and exchange purchase orders. However, payment for purchases will be handled outside of the network through checks and wire transfers from one bank to another (Bartels, 1998). In fact, auto companies have sufficient market leverage over suppliers that they often delay payment to suppliers for 30 to 60 days. For this reason, there is little interest in using an Internet-based payment method over the ANX.

One possibility, however, would be for a bank to buy accounts receivables at a discount from suppliers that desired faster cash flow or to provide suppliers with loans secured by receivables. A bank interested in providing such a service would need to negotiate with the ANX for a site that suppliers would use to access this type of financing. However, in trading networks more open-ended than the ANX, opportunities for banks and other financial services companies will be much greater. In these cases, purchase prices, much lower than those transacted over the ANX, would justify the use of payment products like purchasing cards or even credit cards.

## **Conclusion**

The Automotive Network Exchange will allow thousands of companies in the automotive supply-chain swap CAD files, e-mail, and other information. The auto industry expects the ANX to cut its costs by about \$1 billion a year. The ANX could ultimately involve as many as 40,000 companies that have a stake in manufacturing, financing, and insuring cars and trucks (Scott, 1998). The ANX network will provide automotive trading partners with a single, secure network for electronic commerce and data transfer - replacing complex, costly, and redundant connections that currently exist throughout the automotive supply-chain.

Finally, extranet VPNs, such as the ANX, are slowly extending themselves to other industries. In the future, they will grow to provide ubiquitous data networking. Networking that is secure and better protected than most private networks from outside attack. VPNs will provide this high-quality and inexpensive networking over the Internet.

## **Reference List**

Anonymous. (1998, November). New Internet tool starts paying dividends. *Ward's Auto World*, 34(11), 18.

AIAG Web Site: <http://www.aiag.org>

ANX Press Release. (1998, May 20). ANX overseer opens for business. *ANX*.  
<http://www.anxo.com/press/1998/980520.html>

ANX Web Site: <http://www.anxo.com/whatis.htm>

Apfel, A. (1997, August 27). The Internet, intranets and extranets: IT paradigm, paradise or pariah? *Gartner Group: Strategic Analysis Report*.

Bartels, A. (1998, December 7). Bank roles in ANX are limited. *GigaWeb*.

<http://www.gigaweb.com/scripts/forwarder.dll/Get.s/gncqa1/365774-AB98.htm?bHiligh=true>

Bradner, S. (1998, August 17). When is the Internet not the Internet? *Network World*, 15(33), 27.

Capps, K. (1998, September 1). It's pedal to the metal for EDS/ANX. *EDS Press Release*. [http://www.eds.com/about\\_eds/homepage/homepage\\_headlines\\_2.shtml](http://www.eds.com/about_eds/homepage/homepage_headlines_2.shtml)

Chabrows, E. (1998, October 5). Instruments of growth. *Informationweek*.  
<http://www.techweb.com/se/directlink.cgi?IWK19981005S0001>

Clark, T. (1998, March 20). VPN firms win OK for auto project. *CNET News*.  
<http://www.news.com/News/Item/0,4,22327,00.html?st.ne.ni.rel>

Covill, R. (1998). *Implementing Extranets: The Internet as a virtual private network*. Boston: Digital Press.

Dalton, G., & Davis, B. (1998, August 31). ANX gets certified network providers. *Informationweek*, 698, 134.

Daum, K. (1998, October). AAM ANX implementation plan. *AAM MIS Report*.  
<http://home.aam.com/americanaxle/Corporate/mis/misproj3.htm>

Diaz, K. (1998, March 30). VPNet products selected by automotive industry's ANX project to participate in world's largest VPN. *VPNet Press*.  
<http://www.vpnet.com/about/press17.htm>

FAQs: DST and the ANX Network. (1998, January). *Digital Signature Trust*.  
<http://www.digsigtrust.com/faqanx.html>

Frook, J. (1998, April 20). Automotive extranet lights fire globally. *Internetweek*.  
<http://www.techweb.com/se/directlink.cgi?INW19980420S0001>

Gasparro, D. (1997, May 6). Charting the data VPN movement. *Tele.com*.  
<http://www.teledotcom.com/0597pl/tdc0597plvpn.corp.html>

Horowitz, A. (1998, January 5). Year of the extranet at last? *Informationweek*.  
<http://www.techweb.com/se/directlink.cgi?IWK19980105S0025>

- Kosiur, D. (1998). *Building and managing virtual private networks*. New York: Wiley.
- Merkow, M. (1997, August 27). The Big 3's network. *Webreference.com*.  
<http://search.internet.com/dual-webref/http://webreference.internet.com/content/extranet/examples.html?WebReference+2176+The&Big&3's&Network>
- Pappalardo, D. (1998, September 7). Three years in the making, the ANX is official. *Network World*, 15(36), 56.
- Saunders, J. (1998, July). Automotive network acts as vehicle for VPNs. *Computing Canada*, 1(7), 18.
- Scott, A. (1998, July/August). Beyond 2000: Technology for your tomorrow. *TMA Journal*, 18(4), 24-27.
- Simmons, D. (1998, December). Ameritech Advanced Data Services is first ANX CEPO. *Actionline*, p. 6.
- Temkin, B. (1998, October 30). Ford casts net around suppliers. *Forrester Business Trade & Technology Strategies*, 2(6).  
<http://www.forrester.com/cgi-bin/cgi.pl?displayOP&URL=/business/1998/briefs/bt103098.htm>
- Wallace, B. (1998, September 7). Automakers eye global VPN. *Computerworld*, 32(36), 4.
- Wallace, B. (1998, July 20). Health orgs eye sharing private 'net. *Computerworld*, 32(29), 1.
- Wilder, C., Dalton, G., & Davis, B. (1998, March 23). Companies are turning to the Internet for tighter integration with suppliers overseas. *Informationweek*.  
<http://www.techweb.com/se/directlink.cgi?IWK19980323S0023>
- VPNet Web Site: <http://www.vpnet.com/about/about.htm>