

The Automotive Network Exchange

by

Ronald G. Wolak
wolakron@scis.nova.edu

A paper submitted in fulfillment of the requirements
for DISS 790 - Assignment Seven

School of Computer and Information Sciences
Nova Southeastern University

July 1999

An Abstract of a Paper Submitted to Nova Southeastern University
in Fulfillment of the Requirements for DISS 790 - Assignment Seven

The Automotive Network Exchange

by
Ronald G. Wolak

July 1999

Electronic commerce is projected to grow at a staggering rate in the future, and a significant portion of that growth will occur in business-to-business transactions. In recognition of this, the automotive industry, led by the Automotive Industry Action Group, created the Automotive Network Exchange (ANX) in 1995. As envisioned, the ANX will be the world's largest virtual private network or extranet. It will ultimately connect more than 50,000 businesses. In the following pages, this paper focused on the automotive industry's deployment of the ANX. It began with a brief discussion of the Internet-based electronic commerce initiatives of DaimlerChrysler and Ford Motor Company along with a discussion of the use of extranets as a method of conducting secure electronic commerce. This was followed by a comparison of the VPN protocols currently available for extranet security. Following this discussion of automotive electronic commerce and extranet security, the paper proceeded with an in depth investigation of the ANX. Topics covered included the network's organizational structure and trading partners. The paper concluded with a discussion of the network's plans for growth in the future.

The Automotive Network Exchange

Electronic commerce is projected to grow at a staggering rate in the future, and a significant portion of that growth will occur in business-to-business transactions. In recognition of this, the automotive industry, led by the Automotive Industry Action Group (AIAG), created the Automotive Network Exchange (ANX) in 1995. As envisioned, the ANX will be the world's largest virtual private network (VPN) or extranet. It will ultimately connect more than 50,000 businesses (Steding, 1999). The ANX reached production status in January 1999, and today there are more than one hundred trading partners on the network.

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 automotive supply-chain. In short, the ANX will eliminate the intertwined web of connections that currently connect the automotive industry with a single IP-based network. Procedures, guidelines, models, and technologies developed during its implementation will not only benefit the automotive industry but will also provide a basis for future growth in business-to-business electronic commerce.

In the following pages, this paper focuses on the automotive industry's deployment of the ANX. It begins with a brief discussion of the Internet-based electronic commerce initiatives of DaimlerChrysler and Ford Motor Company along with a discussion of the use of extranets as a method of conducting secure electronic commerce. This is followed by a comparison of the VPN protocols currently available for extranet security. Following this discussion of automotive electronic commerce and extranet security, the paper proceeds with an in depth investigation of the ANX. Topics covered include the network's organizational structure and trading partners. The paper concludes with a discussion of the network's plans for growth in the future.

Automotive E-Commerce

A growing number of U.S. companies, including DaimlerChrysler, Ford Motor, and General Motors are expanding their Internet business links with both domestic and overseas suppliers, customers, and trading partners. DaimlerChrysler, for example, 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. DaimlerChrysler plans to buy from more than 3,000 suppliers via TradeWeb by the end of 1999.

Ford Motor Company is also moving quickly into business-to-business electronic 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 will require its vendors to follow a proprietary implementation of the Open Buying on the Internet (OBI) standard.

Ford chose Intelisys Electronic Commerce (a software company specializing in procurement solutions) to create its OBI-compliant Internet-based purchasing environment.

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 automotive trading partners are employing standard Internet technology to conduct electronic commerce in the situations described above, they are also looking to extranets for the secure transport of sensitive and mission-critical information (Horowitz, 1998). The public Internet has not met automotive industry requirements for network availability, rapid problem resolution, and predictable performance for time-critical business applications. In contrast, the ANX extranet will provide a common global TCP/IP network infrastructure that meets specific automotive industry requirements for performance, reliability, security, and management.

The trend to deploy extranets is not limited to the automotive industry. In fact, as many 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.

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. In addition, 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.

Security

Although the security products available for extranets such as the ANX are still quite young, a handful of protocols have emerged as the leading choices for building this type of secure network. 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) extends 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 the security protocol used by the ANX. Developed by the IETF, it provides authentication and encryption over the Internet. IPSec evolved during the development of Internet Protocol version six (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 that makes it well suited for LAN-to-LAN VPNs. This is also the primary reason IPSec was chosen to be the security protocol for the ANX. 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.

Organizational Structure

The Automotive Industry Action Group is responsible for the ongoing operation of the ANX network (AIAG, 1999). The AIAG is a nonprofit trade association of North American automobile manufacturers and suppliers. The association's members include the Big Three along with over 1200 automotive supplier companies. In 1994, the AIAG

recommended that TCP/IP with IPSec security become the standard for transport of automotive trading partner electronic commerce. The ANX project was launched shortly thereafter in December 1995.

Within the AIAG, the Implementation Task Force (ITF) and the Telecommunications Project Team (TPT) are responsible for the day-to-day operation of the 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 to the appropriate AIAG manager for AIAG-related administrative functions.

The ANX Overseer (ANXO) company is the single administrative entity that 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 service level agreements with ANX subscribers. Their compliance with these objectives is closely monitored by the ANXO. The following sections describe the roles of the ANX Overseer, Certified Service Providers, Certified Exchange Point Operators, Certified Security Companies, and Certification Authority Service Providers.

Overseer

Telcordia Technologies was selected as the ANX Overseer (ANXO) in May 1998 (ANX Press Release, 1998). Telcordia Technologies is a leading provider of communications software, engineering, consulting, and training services. As ANXO, Telcordia Technologies provides administrative services such as security certificate handling, trouble handling, dispute resolution, and ANXO help desk services (AIAG, 1999). In addition, Telcordia Technologies administers certification services for service providers and registration services for automotive trading partners.

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 four certified service providers (Pappalardo, 1998). Ameritech, Bell Canada, Electronic Data Systems (EDS), and AT&T 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 and Concentric Network. 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 the ANX VPN available to other vertical industries, such as health care, insurance, and finance according to Karl Schohl, ANX Business Manager (AIAG, 1999). 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 created 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 the 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.

Certified Exchange Point Operators

ANX Certified Exchange Point Operators (ANX CEPO) provide ATM-based network services to interconnect ANX CSPs (AIAG, 1999). Certified exchange point operators must demonstrate one hundred 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 Telcordia Technologies 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 (AIAG, 1999).

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.

Certified Security Companies

In addition to signing up with a certified service provider and the AIAG, trading partners must also choose one of eight approved 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 VPNet as interoperable IPsec gateways. The testing also certified that the gateways complied with the pending IETF IPsec standard.

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 Krysnakowski, 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.

VPNet Technologies was one of the eight VPN companies chosen to support the ANX (Clark, 1998). VPNet 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 (Clark, 1998). "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. VPNet 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.

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 (AIAG, 1999). 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 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 Telcordia Technologies, 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 in 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.

Trading Partners

Since November 1, 1998 (the ANX's full production launch date), 3715 automotive trading partners were ANX sponsored (ANXO, 1999). ANX sponsorship is the first step in connecting to the ANX network. Trading partners next become contracted, registered, and finally subscribed. Currently, 125 companies are ANX subscribed. Among the list of subscribed partners are Ford Motor, DaimlerChrysler, General Motors, Taylor Steel, and American Axle and Manufacturing. The following is a brief look at the ANX implementation efforts at these five companies.

Ford Motor

Ford Motor Company's ANX implementation plans are quite aggressive (Kirchoff, 1999). The company intends to use the ANX as its strategic telecommunications transport and network service for supply chain communications. In fact, all of Ford's U.S. and Canadian suppliers connected to the company's private IP VANs are requested to migrate to the ANX by September 30, 1999.

Ford's current supplier networks are divided into two types: TCP/IP and SNA (Theisen, 1999). The company's communication goal is to be 100 percent TCP/IP by January 2000. In the future, Ford's vision includes TCP/IP communications over two networks - the ANX and the public Internet. The ANX will be used for applications that fall into one of five categories: business-critical, high-availability, time-critical, confidential, and real-time. The public Internet will be used for applications that are non-critical and have a low requirement for end-to-end accountability.

Currently, Ford has 11 ANX-enabled applications: C3P-IMI file transfer, C3P-FRPPAH file transfer, PDGS file transfer, EDM CADD5 file transfer, global prototype inventory requisitioning, analytical warranty, mainframe IP printing, common manufacturing management, engineering release, procurement and receiving, and material supply. The company's future deployment plans include applications that are high volume, business critical, or confidential (e.g. EDI and direct data links mainframes).

DaimlerChrysler

DaimlerChrysler is another automotive trading partner committed to the success of the ANX (Jackson, 1999). According to Thomas Stallkamp, DaimlerChrysler President, the company is committed to the use of the ANX. DaimlerChrysler'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 DaimlerChrysler to electronically route product shipment schedules, order information, CAD files for product designs, purchase orders, and other financial information.

DaimlerChrysler has an extensive ANX support organization (Jackson, 1999). The goals of this internal information systems staff are to:

- Support internal application development and coordinate the strategic use and integration of the ANX
- Design, develop, evolve, and support DaimlerChrysler's technical infrastructure
- Provide trading partner interface and connectivity support

Thus far, DaimlerChrysler's internal ANX staff has successfully connected 15 applications to the ANX (DaimlerChrysler, 1999). These mainframe applications include capacity planning, change notice, numerical control system manual, national customs automation program, premium transportation, purchase order inquire, smart manual, supplier claims, supplier claims (SEECS), supplier feedback, supplier material tracking, supplier profile update system, total maintenance system, warranty maintenance system, and warranty information system. In 1999 and 2000, the company plans to migrate additional business applications from seven of its major departments: procurement and supply, human resources, sales and marketing, manufacturing, public relations and communications, engineering and design, and information systems.

The use of the ANX will result in new business practices between DaimlerChrysler and its vendors (Merkow, 1997). "They'll be holding information rather than inventory," stated Laura Migliore, a DaimlerChrysler process control specialist. DaimlerChrysler also hopes the ANX will help it alleviate chronic design cycle problems by allowing it to collaborate in real time with its suppliers.

DaimlerChrysler's ANX connection will also enable simultaneous engineering using multiple workstations or graphics terminals to run finite element analysis software, solid modeling CAD packages, and high-speed prototyping (Jackson, 1999). 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 DaimlerChrysler's cost of doing business and aid in reducing the current five-year product design cycle down to less than three years.

General Motors

While General Motors is committed in its support of the ANX (ANX, 1999), the company (unlike Ford and DaimlerChrysler) has chosen not to publish its current ANX deployment plans. However, interested trading partners are encouraged to contact the appropriate General Motors application owners and arrange for the migration of specific applications to the ANX (GM Supplier, 1999).

Taylor Steel

Taylor Steel 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. Before the ANX, the company communicated with customers via a dial-up EDI connection. This dial-up connection was slow and in cases where customers were located a few minutes away, the truck usually arrived before the electronic order did.

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 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. In addition, use of the ANX reduced Taylor's phone charges by 75 percent.

American Axle and Manufacturing

American Axle and Manufacturing (AAM) is another ANX subscribed trading partner. AAM (headquartered in Detroit, Michigan) is a growing, multi-billion-dollar supplier of automotive driveline systems (AAM, 1999). Unlike the trading partners described above, AAM decided just 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 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

AAM has completed phase one, two, and half of phase three of its ANX implementation plans (AAM, 1999). Phases one and two were completed in 90 days. Phase three has a planned completion date of the last quarter of 1999. AAM is currently investigating the use of the ANX for EDI data communications to GM and to connect to its outside suppliers. AAM's ability to rapidly implement the ANX is evidence of the AIAG's success in putting together an effective organizational structure and in producing a viable production network.

Future Plans

Developers of the ANX envision that the network will continue to grow until all 1,000 tier-one suppliers, 9,000 tier-two and tier-three suppliers, and 40,000 others will all be connected (Steding, 1999). Currently, ANX users are predominantly suppliers to the automobile manufacturers, including the steel industry. However, once the infrastructure of the widespread network is in place, this will change.

Vertical Expansion

In the future, the AIAG plans to make ANX available to other vertical industries (Wallace, July 1998). One example is a group of health care organizations that are holding talks with the AIAG about becoming ANX participants. These 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 others in the health industries, health care organizations would be able to link with the automakers and other partners on the ANX. "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 (Wallace, July 1998). "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.

Unlike the health care industry, the ability of the ANX to integrate with the banking industry in the future is still uncertain (Bartels, 1998). 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. In fact, auto companies have sufficient 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.

Global Expansion

The ANX is also planning to become a global service (Wallace, September 1998). 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. The AIAG is pursuing a cooperative agreement with the European auto association and the Japanese Auto Manufacturers Association to extend the ANX globally.

The ANX is currently limited to the U.S. and Canada. "We're trying to make the ANX a global network that the entire industry can take advantage of," said Don Hedeem, ANX director (Steding, 1999). Hedeem's next step is to extend the ANX into Mexico and the many automotive manufacturing installations there. The first release of ANX in Mexico is planned to be operational sometime in the fourth quarter of 1999.

In 1997, the AIAG developed a formal ANX Memorandum of Understanding (MOU) (Hedeem, 1999). Its purpose was to share information and to 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 (Hedeem, 1999):

- France - The national organization Groupement pour l'Amelioration des Liaisons dans l'Industrie Automobile (Galila) 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.
- 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.
- 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.
- 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.
- South America - AIAG and ODETTE are in the process of identifying interested national organizations. MOUs with country-specific automotive groups will be established.
- 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.
- Japan and the Pacific Rim - Informal ANX information transfer has been established between the AIAG and the Japan Automobile Manufacturers Association (JAMA) (Frook, 1998). 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.

Expanding the ANX overseas will be very beneficial to U.S.-based automakers (Wallace, September 1998). 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.

Conclusion

In summary, the goal of the ANX 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. In addition, the ANX provides the opportunity to solve data communications problems once instead of one trading partner and application at a time. New applications will be deployed faster, redundant connections will be eliminated, and communications costs will be reduced. The ANX's mission is to create an environment that maximizes the ability of each trading partner to compete efficiently.

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 more secure and better protected than most private networks.

Reference List

- AAM. (1999). AAM: Forging new world driveline standards [Online]. Available: <http://www.aam.com/> [1999, July 10].
- Anonymous. (1998, November). New Internet tool starts paying dividends. *Ward's Auto World*, 34(11), 18.
- AIAG. (1999). The automotive industry action group [Online]. Available: <http://www.aiag.org/> [1999, July 8].
- ANX. (1999). Automotive Network Exchange [Online]. Available: <http://www.anxo.com/> [1999, July 3].
- ANXO. (1999). ANXO directory [Online]. Available: <http://www.anxo.com/directory/tplist.html> [1999, July 8].
- ANX Press Release. (1998, May 20). ANX overseer opens for business. *ANX* [Online]. Available: <http://www.anxo.com/press/1998/980520.html> [1999, July 7].
- Bartels, A. (1998, December 7). Bank roles in ANX are limited. *GigaWeb* [Online]. Available: <http://www.gigaweb.com/> [1999, June 21].
- 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* [Online]. Available: http://www.eds.com/about_eds/homepage/homepage_headlines_2.shtml [1999, July 7].
- Clark, T. (1998, March 20). VPN firms win OK for auto project. *CNET News* [Online]. Available: <http://www.news.com/News/Item/0,4,22327,00.html?st.ne.ni.rel> [1999, July 8].
- Covill, R. (1998). *Implementing Extranets: The Internet as a virtual private network*. Boston: Digital Press.
- DaimlerChrysler. (1999). The DaimlerChrysler ANX page [Online]. Available: <http://supplier.chrysler.com/general/anx/index.html/> [1999, July 10].
- 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* [Online]. Available: <http://home.aam.com/americanaxle/Corporate/mis/misproj3.htm>

[1999, July 10].

FAQs: DST and the ANX Network. (1998, January). *Digital Signature Trust* [Online]. Available: <http://www.digsigtrust.com/faqanx.html> [1999, July 8].

Frook, J. (1998, April 20). Automotive extranet lights fire globally. *Internetweek* [Online]. Available: <http://www.techweb.com/se/directlink.cgi?INW19980420S0001> [1999, July 6].

GM Supplier (1999). ANX contact list [Online]. Available: <http://www.gmsupplier.com/apps/gsnhome/anx/supplier/contact.htm> [1999, July 10].

Hedeen, D. (1999, March 11). ANX public forum - Grand Rapids, Michigan [Online]. Available: <http://www.anxo.com/> [1999, July 5].

Horowitz, A. (1998, January 5). Year of the extranet at last? *Informationweek* [Online]. Available: <http://www.techweb.com/se/directlink.cgi?IWK19980105S0025> [1999, July 7].

Jackson, M. (1998, September 1). Big 3 value proposition viewpoints: A Chrysler perspective [Online]. Available: <http://supplier.chrysler.com/general/anx/> [1999, July 7].

Kirchoff, D. (1999, March 11). Ford Motor Company plans for the ANX network [Online]. Available: <https://web.suppcomm.ford.com/anxpage.htm> [1999, July 9].

Kosiur, D. (1998). *Building and managing virtual private networks*. New York: Wiley.

Merkow, M. (1997, August 27). The Big 3's network. *Internet.com* [Online]. Available: [Webreference.com](http://www.webreference.com) [1999, July 10].

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.

Simmons, D. (1998, December). Ameritech Advanced Data Services is first ANX CEPO. *Actionline*, p. 6.

Steding, P. (1999, May). Getting the message. *AIAG Action Line*, 19(4), 18-21.

Temkin, B. (1998, October 30). Ford casts net around suppliers. *Forrester Business Trade & Technology Strategies*, 2(6) [Online]. Available: <http://www.forrester.com/> [1999, June 21].

- Theisen, D. (1999, May). Ford ANX-enabled applications [Online]. Available: https://websupcomm.ford.com/anxenabled_applications.htm [1999, July 9].
- 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* [Online]. Available: <http://www.techweb.com/se/directlink.cgi?IWK19980323S0023> [1999, July 6].