Secure Virtual Private Networks
The future of data communications

Eli Herscovitz
President and CEO, RADGUARD Ltd.

The proliferation of the Internet has broken down traditional boundaries to international communication. It has linked peoples and worlds otherwise separated by physical and emotional barriers, and it has provided an inexpensive yet quite reliable means for inter-organizational information sharing and data transfer.

With the development and increased use of the Internet have come new communications opportunities, as well as challenging security problems. The Internet is an almost ideal means for information retrieval and exchange. It is cost-effective, easy to use and accessible in nearly every major city of the world. Similarly, the Internet is a shared media, to which millions of users are connected, and there are very few regulations (thankfully so) on how it is to be used. And just as these traits make the Internet an attractive method for honest activity, so too do they make it a very efficient medium for devious tasks such as data tampering, eavesdropping and theft.

These contradictory aspects of the Internet revolution seemingly place a tremendous hurdle in the way of the business community's embracing of the Internet. "Why use something I can't trust?" is a refrain that could be, and is heard from many network administrators or technology officers. Results from a Forrester Research survey aptly convey the scope of these fears. Polling Fortune 1000 companies for why they were not using the Internet for business transactions, Forrester found that 48% (the highest score) indicated that security was the primary reason.

The fears surrounding network security, made all the more acute with the recent wave of high profile successful hacks, and the search for cheaper means of connectivity have generated the demand for turn-key solutions capable of creating secure Virtual Private Networks (VPNs): cost effective multi-site networks built on public backbones. The IT community has responded, and the results are emerging VPN technologies that incorporate network encryption, access control, certification and network management.

Not surprisingly, secure VPNs represent one of the hottest areas of the international networking market. Infonetics Research estimates that today's $200+ Million VPN market will grow to over $11.9 Billion by 2001, with VPN product sales alone representing $1.19 Billion. CIBC Oppenheimer is similarly bullish on the potential of VPNs. In their opinion, VPN "market acceptance will be immediate and revenues should ramp up quickly." From the buyer's perspective, a recent International Computer Security Association (ICSA) survey notes that "VPNs are another big-ticket item." The ICSA found that VPN systems were third on the list of "Top 10 products and services organizations plan to buy in near future."

VPN systems enable distributed private networks to communicate securely with each other over untrusted, public networks. They encrypt transmitted information with complicated algorithms so as to hide sensitive data from prying eyes. The general process is as follows:

1. A protected host sends clear traffic to a VPN kit (the source device) located at the point of connection to the public network.
2. The source device examines the data according to rules specified by the network manager, securing the information or allowing it to pass unaffected.
3. When data protection is required, the source device encrypts (encodes) and authenticates (attaches a digital signature to) the whole packet, including the transmitted data as well as the source and destination host IP addresses.
4. The source device then attaches a new header to the data, including the information that the destination device requires for security functions and process initialization.
5. The source VPN kit then encapsulates the encrypted and authenticated packet with the source and destination IP addresses of the destination device, or devices. This results in a virtual tunnel through the public network.
6. When the data reaches the destination device, it is decapsulated, its digital signature is checked and the packet is decrypted.

Diagram I illustrates the over-all structure of a secure VPN. In this example the network includes four private networks that are interconnected via an untrusted public network. The private areas sit behind secure VPN devices (represented in Diagram I by the oblong shapes that connect the virtual tunnels), which are themselves connected to the public network via routers (represented in the diagram by squares containing arched arrows).

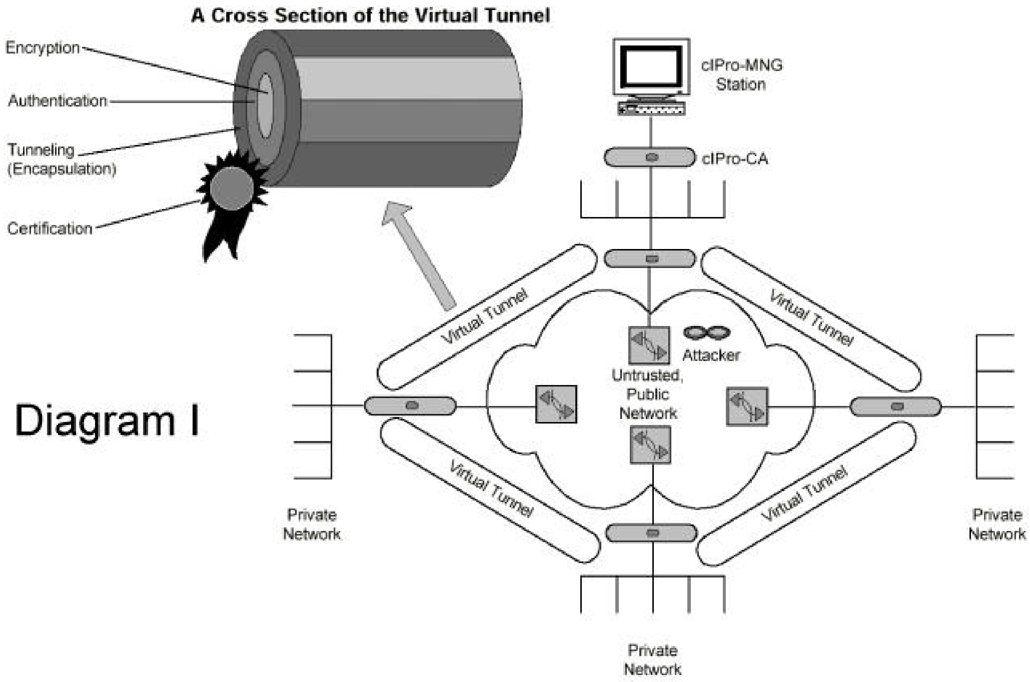


Diagram I

Within this secure VPN, data passed from one device to another flows through the public network through a multi-layer "virtual tunnel" of security algorithms (in the diagram the virtual tunnels are separated from the public network to demonstrate their isolation from the rest of the public network). The tunnels begin at the VPN devices, continue through the routers and traverse the public network on their way to the other VPN devices.

Marking the entire tunnel is a digital certificate which identifies the tunnel as belonging to the secure VPN. The outer most section of the tunnel represents the encapsulation of the data, the alteration of the data to appear as the destination device. The second most outward level, authentication, involves the use of a different set of algorithms that verify the authenticity of the information’s source. Travelling further inward, we reach the encryption level, where the transmitted data itself is encoded to ensure its confidentiality.

The end result of the tunneling process is the scrambling of transmitted information to make it legible only to its intended recipient. Diagram II demonstrates this process in its most simplified form. User A, residing in Ottawa, sends a message to his colleague Bob, who works in Orlando. His message, “Hi Bob,” passes through the Ottawa VPN device, where it is scrambled to read “^g4#bh.” The encoded message travels across the public network to the Orlando VPN kit, which then decrypts the message, letting Bob receive his colleague’s friendly words, “Hi Bob.”

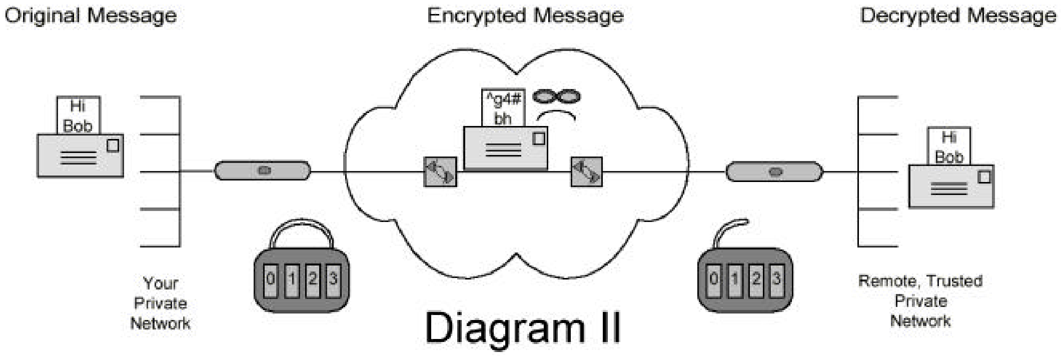
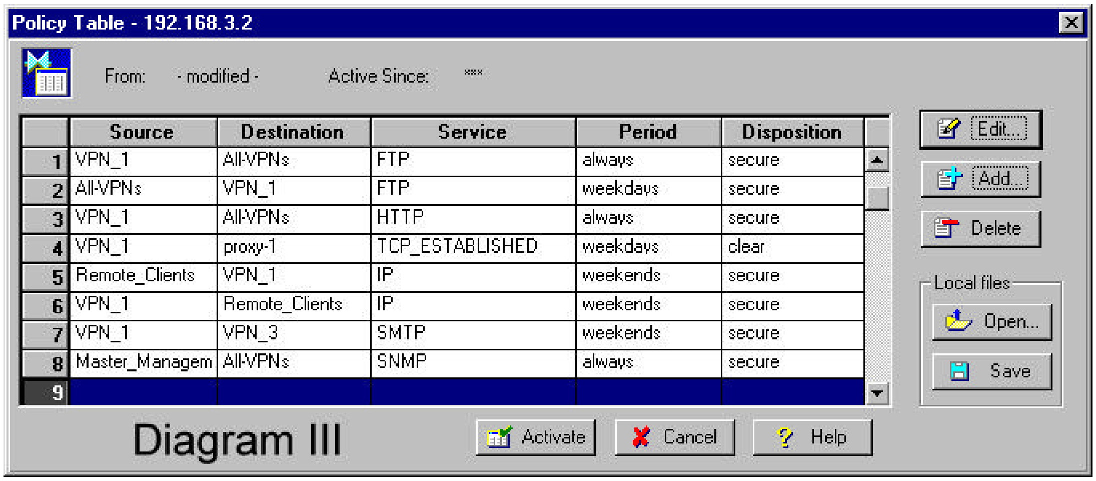


Diagram II

In this simplified example, the secure VPN that connects User A and Bob scrambles the message as it travels through the public network. Not only was the information not altered on its way (it was authentic), but no one else was able to see the transmitted message (it was confidential) nor pretend that they were User A.

Creating a secure VPN requires devices capable of performing the different scrambling tasks as well as guidelines that determine what communications traffic is encrypted and what is not: i.e., they must be able to answer questions like: Do I protect all email but not file transfers? What about web browsing, can my secure VPN users access the World Wide Web, or are they limited to my company’s intranet?

In order to address these issues, secure VPNs work according to predefined rules. Diagram III below illustrates how such rules are defined and how they impact the flow of information in and out of the VPN.



Policy Table - 192.168.3.2

From: - modified - Active Since: ***

	Source	Destination	Service	Period	Disposition
1	VPN_1	All-VPNs	FTP	always	secure
2	All-VPNs	VPN_1	FTP	weekdays	secure
3	VPN_1	All-VPNs	HTTP	always	secure
4	VPN_1	proxy-1	TCP_ESTABLISHED	weekdays	clear
5	Remote_Clients	VPN_1	IP	weekends	secure
6	VPN_1	Remote_Clients	IP	weekends	secure
7	VPN_1	VPN_3	SMTP	weekends	secure
8	Master_Managem	All-VPNs	SNMP	always	secure
9					

Diagram III

The policy table is divided into five columns: (1) “Source,” the originating point for the communications traffic; (2) “Destination,” where the traffic is heading; (3) “Service,” the type of traffic; (4) “Period,” time frame; and (5) “Disposition,” the state of the traffic: i.e. encrypted or clear. The secure VPN represented in Diagram III includes a number of different networks as well as remote access for teleworkers, and it allows different kinds of information transfer, at different times and under different conditions.

Rule 1 specifies that network users residing behind VPN-1 can upload and download files securely with the other members of the VPN, at any time of day. Rule 2 illustrates, however, that for reasons determined by the VPN’s manager the other members of the VPN may only complete file transfers with VPN-1 on weekdays. Rule 3 creates an intranet between VPN-1 and the other private networks; it establishes that all HTTP traffic between the members of the VPN is secure.

Rule 4 provides an non-encrypted outlet for IP communications with sites beyond the VPN, allowing users to access the Web and send email to outside parties (on weekdays only) without opening sensitive company information to hackers. Rules 5 and 6 create secure tunnels for employees working from home on the weekends. These two rules extend the scope of the VPN to beyond the workplace; similar capabilities can be included for travelling salespeople as well.

Rule 7 creates a secure tunnel within the VPN. It links one private network (VPN_1) to another (VPN_3) with a secure email channel. The use of tunnels within VPNs allows network managers to add security precautions within the network, thus preventing the very real possibility of internal security breaches. Rule 8 corresponds to SNMP (management and control) traffic. It is interesting to note that in the above diagram, all the management traffic is secure, an important point considering the sensitivity of network control.

The end result of the policy table is a secure VPN that operates automatically and transparently to the user. Employees residing in the VPN work normally. They go on line, send email to customers and suppliers or download presentations, and the VPN determines which of their tasks are to be conducted secured and which should continue in the clear. Full privacy is maintained, communications costs are reduced, but efficiency and employee output remain unchanged.

Undoubtedly, today’s single most important VPN is that of the Automotive Network eXchange (ANX – information on the ANX can be found at the AIAG’s web site: www.aiag.org). Developed jointly by the Automotive Industry Action Group (AIAG—the trade organization of the US automotive industry) and Bell Communications Research, the ANX will link automotive trading partners into a single, secure network for electronic commerce and data transfer. It will bring the thousands of companies involved in one of the world’s single largest business sectors, with annual earnings numbered in the hundreds of billions of dollars, into a single communications environment, and in so doing, it will radically change the way business is conducted.

The importance of the ANX project has only begun to be felt, and yet it has already made the VPN the new communications paradigm for multi-national corporations and complex industries. Aviation, defense, and other major enterprises are keeping a watchful eye on the developments surrounding the ANX project, as it will determine the rules of communications between and within corporations involved in multiple-component products and services.

From a savings standpoint, the use of the Internet as a backbone for networking is far less expensive than private leased lines, frame relay, or ISDN networks. In fact, the driving force behind the concept of the ANX, for the US automotive industry, was reduced costs. A previous Byte Magazine article noted that use of the ANX is expected to reduce the costs of automobile production by as much as $70 per car. In addition, the added security a VPN provides prevents the sizable losses brought on by security breaches. In a recent study conducted by the FBI and the Computer Security Institute (CSI), the average costs of a network security breach, for the companies which participated in the survey, was found to be around $1 Million.

VPNs also present a viable networking option for small or midsize companies. The Israeli home soft drink company, Soda Club, is a good example. Through their VPN, Soda Club employees can share files, send email messages, browse the Web, manage inventory, order products and plan corporate strategy, all in real time and from any of their international offices. The entire network is managed from one central office (with the option for hierarchical or regional management), and new offices can be added to the network without any network alteration. In addition, travelling Soda Club representatives can access the network from anywhere in the world, and they can do so securely and efficiently.

Companies interested in setting up VPN have a number of options at their disposal. They can choose between software add-ons to routers, software firewalls with encryption patches, software VPN systems, or dedicated hardware VPNs. Other options include the types of algorithms used for encryption—DES/3XDES, RSA, RC4, RC5, IDEA, etc.—and key exchange (IKE, SKIP)—as well as the means of identifying and certifying the different members of a VPN—dedicated certificate authorities (CAs), third-party CAs and others.

Encryption

Encryption is the starting point of any VPN solution, and one of the key differentiators between effective and ineffective VPNs is the use of well established encryption algorithms and strong encryption keys. Several techniques are suitable, although the symmetric DES/3XDES algorithms are mostly used for payload encryption, while the asymmetric (also known as Public Key) RSA and Diffie-Hellman algorithms are popular for key exchange. The above mentioned encryption keys are well known and tested, and libraries of information have been devoted to their reliability and efficacy.

Encryption is a difficult process, and when dealing with the quantities of information transferred across modern networks, CPUs can be confronted with staggering workloads. Infonetics Research, as noted in a recent PC Week article, puts the CPU strain for DES (Data Encryption Standard) encryption at 25 times that of regular computing work. It is not surprising, therefore, that the secure VPN market is heading towards dedicated hardware solutions over their software equivalents. Hardware focussed on security-only functions is better able to cope with the strains involved in encryption and authentication and, as a result, can provide powerful security features without significantly delaying network performance.

Key generation and management

Since encryption algorithms are well known, the strength of the encryption process comes down to the *key* used in encrypting and deciphering transmitted data—the well-kept secret shared by the component machines of the VPN— and the protocol used in the key management process.

The security of the VPN’s encryption methodology is a combination of the following factors:

- *Key length*: In general, the longer the key - the tougher to break. Today, a key length of less than 56 bits (when using the DES algorithm) is considered insecure.

- *Key exchange mechanism*: As mentioned above, keys are the common secret upon which the whole encryption process strength is based. Key exchange, therefore, should be based on well established algorithms (e.g., Diffie-Hellman for encryption and RSA for signature) as specified in strong key management standards. Today, the IKE protocol (rather than Simple Key Management for Internet Protocol, or SKIP), is the preferred method. The primary advantages of IKE over SKIP is the former’s ability to negotiate with a number of different encryption keys. This prevents unrecognized messages from being sent outside protocol guidelines, thus providing greater robustness and enhanced security.

- *Rate of key exchange:* As a rule, the more frequently a key is *automatically* exchanged, the more secure the encrypted data. VPN solutions which use manual key exchange are extremely insecure, as users may not always remember to change keys or may choose not to bother with the often cumbersome manual key exchange process. Similarly, a key exchange only at the end of a session is unreliable, as large amounts of data can be accessed if the key is compromised.

- *Key generation*: In principle, the use of true random keys ensure the highest levels of security. With real random numbers as the bases for encryption keys, it is impossible to know or predict the structure of past or future keys. The best method of key generation is hardware (usually, a noise diode). Software-based key generation, in contrast, use known algorithms, which, given enough time and money, can be cracked.

Certification

Certification is the registration and identification of VPN components. It requires establishing well defined secrets between a centrally controlled Certification Authority and any VPN device. A poorly designed and implemented certification process, such as a password, may result in an "easy to join" VPN to which unwanted entities may connect as members.

The first step in adding new gateways to the VPN involves the transfer of secret information in a simple yet secure way. This process must be carried out with extreme caution as no encryption system has been established. The use of secured hardware tokens is recommended for this preliminary certification phase, as they provide a secure means of loading the security information, off line, into the new gateway.

Once the transfer of the initial secret is complete, the rest of the certification process, as well as the distribution of the new certificate to all existing VPN gateways, should be done secretly and quickly in order to allow for the fastest possible set-up and operation. It is necessary, therefore, to employ a fully automatic and secure (encrypted and signed) certification process. VPN solutions which send the initial secret unprotected over untrusted networks are ineffective and are not secure, and those which involve the manual input of new units into an existing data base involve significant costs when expanding the VPN.

Tunneling

Tunneling is the encapsulation and encryption of entire transmitted packets. An effective tunneling mechanism hides the networking data in addition to the application and payload layers, i.e. from layer 3 and above (referring to the OSI model). A VPN solutions which only encrypts the payload is not sufficiently secure, as a multitude of information is obtained by analyzing networking parameters. Layer three tunneling is also advantageous from a scalability stand point. As IP's dominance continues to strengthen, greater will the need become to protect all varieties of IP applications over IP backbones. Layer three encryption is application and network independent. It can be applied to any form of routable communications (voice, video, data), thus providing an effective scalability pathway.

Interoperability

The emerging Internet Protocol Security (IPSec) standard, as created by the Internet Engineering Task Force (IETF), is becoming the international standard for virtual private networking. With IKE key management at its base, IPSec has created a secure means for interoperable security. It guarantees that encrypted information is protected on its way from one network to another, while also allowing partner companies to link their respective VPNs together, even if their encryption systems were manufactured by different vendors. VPN solutions that are not IPSec compliant, i.e. not interoperable with the industry standard, will prove more expensive in the long run and will limit a VPN's growth potential.

Access Control

Encryption without effective and efficient access control (i.e., "firewalling") is but half the VPN story, for Internet-based VPNs require defense mechanisms from those who would seek to hack their way into the networks from the Internet. Two issues of primary importance in evaluating the strength of firewall features are the operating system on which the system runs and the methodology used:

- *Operating system*: Software-based solutions are built on well known operating systems, such as UNIX and NT. Hacking methods for targeting bugs and security holes in these operating systems are readily available on the Internet. Hardware-based solutions, in contrast, employ real time, hardened operating systems that do not fall victim to popular hacking methods. The strength of the hardware VPN’s OS translates into better security throughout the network.

- *Methodology*: The effectiveness of a firewall is linked directly to scope of its inspection technique. Access control systems must be able to analyze all levels of incoming and outgoing data, including the content payload itself. Content analysis gives the ability to look inside data flowing through the VPN system. It can weed out commands from sessions, such as FTP “get” or “put” instructions, thereby providing limited access to areas of a VPN but preventing attempts to alter stored information.

Performance

Networking environments have developed at an amazing pace, with the speed of communications representing one of the most significant areas of development. As a result, effective VPN solutions must be able to operate at true wire speeds. Those that do not will form a bottle neck in the communications environment and will prevent the transfer of information. The performance issue becomes even more crucial when more complex encryption algorithms are used (e.g., Triple DES). Hardware based solutions, which are fully dedicated to the task of generating and processing encryption algorithms, are better suited to coping with longer encryption algorithms, and therefore provide a communications infrastructure better able to adapt to the needs of the future.

Network Reliability and Management

A VPN is a networking solution. As such the basic requirements of other networking media must be met by a VPN.

- *No single point of failure*: this important characteristic is achieved through the incorporation of automatic backup gateways (redundancy) into a VPN. Mission critical networking applications require redundancy options for worse case scenario planning. The recent failure of a US communications satellite and its impact on US beeper networks clearly demonstrated that the unthinkable can and will take place. In order to protect a VPN from the potentially disastrous effects of an office fire, for example, it is important to include “hot backup” topologies within the network architecture. In addition, VPN devices must be configurable to distribute security functions throughout the network. Centralized session or key distribution authorities are incompatible with mission critical communications.

- *Network management*: the over-riding concept behind VPN communications is the use of security technologies to increase connectivity. Capable security features in themselves, however, do not an effective VPN make. Indeed, powerful control capabilities are of primary importance in VPN communications, as wide area networking is at best a complicated endeavor. A VPN must include management methods that allow for centralized and regional control over the security devices (and the other networking components) within the network.

- *Management Security*: a VPN's management traffic is the most sensitive data flowing in the network. It includes policy table updates, security auditing and logging data, key exchange definitions (elapsed time or bytes sent), and encryption and authentication methodologies. In order to maintain the confidentiality of such information it is important to secure it with no less than the same technologies used for the other forms of VPN traffic. Better still, however, would be to provide a dedicated encryption plus firewall device for the central management station. Such a precaution not only secures management traffic as it traverses the public network, but it also builds a wall between the VPN master manager and personnel residing in his own local network whom might seek to undermine the security of the VPN.

The above user needs were the design inspiration for RADGUARD's advanced VPN products. Built on dedicated hardware platforms, they deliver advanced security features in tamper proof and easily managed solutions. RADGUARD's products offer IPSec network encryption, integrated firewall functions, redundant back-up tunneling, advanced dynamic key management, network address translation (NAT), automatic network topology learning and IPSec encrypted VPN management traffic. Designed for both large and small-scale environments, RADGUARD VPNs come with user-friendly management systems that provide simple and secure pathways (with IPSec encryption and dedicated firewall support) for centralized and regional network management.

The technology incorporated into RADGUARD′s products is at the forefront of the VPN market. Encryption, authentication and communication procedures are performed simultaneously, in separate dedicated chips, so as to maximize throughput, minimize latency, and cope with network straining capacities. Key generation is based on a unique, real random (not algorithm-based) number generator–dedicated hardware components–so that it is impossible to guess the previous or future encryption keys used by the system. Session key exchange is performed by an in-house designed procedure that allows key generation to be triggered by user specified criteria, elapsed time or number of packets sent, so that new keys can be exchanged in the middle of communications sessions. And, the systems' private encryption keys are physically protected so that the VPNs′ most fundamental security information are tamper proof and inaccessible.

As the VPN market begins to mature, we are confident that our attentiveness to customer demand will provide us with the ability to maintain our leadership position. Our second generation product family, the comprehensive IP protection suite (cIPro), has been widely accepted as the top VPN solution available today. In addition to its "Finalist" award at CeBIT 98 and "Blue Ribbon" from *Network World* magazine, cIPro recently has also received "Tester's Choice" and "Editor's Choice" commendations from *Data Communications* and *SC Magazine*, respectively.

RADGUARD's leadership position is further proven by virtue of the significant VPN projects in which the company and its products are involved. In the spirit of compliance with international standards and supporting interoperability and compatibility, RADGUARD was one of six vendors to receive IPSec interoperability certification by the ICSA for use in the ANX program, described earlier in this article.

RADGUARD can be reached at (201) 828 9611, via email at info@radguard.com, or on the Web at http://www.radguard.com.

Notes:

- ANX® and Automotive Network eXchange® are registered in the U.S. Patent and Trademark Office as service marks by the Automotive Industry Action Group (AIAG), Southfield, Michigan.
- For more information on the ICSA and testing criteria, visit www.icsa.net; for more information on the ANX or AIAG, visit www.aiag.org.