Report to WIPO SCIT Plenary
Trilateral Secure Virtual Private Network Primer

February 3, 1999

Standard	Technology and Description	Product	Comments
Frame Relay	Frame Relay is an international standard for high-speed access to public wide area data networks (WAN). It is currently priced to offer low cost per unit of capacity compared to other competing technologies. Capacity is packaged in terms of a committed information rate (CIR) that the vendor promises to provide all the time and an excess information rate (EIR) typically 2x the CIR that the vendor will support when capacity is available.	Frame Relay circuits from international telecommunications carriers	
IDEA	International Data Encryption Algorithm IDEA is a single key encryption algorithm. IDEA is not export restricted from North America. IDEA has a 128-bit key length.	IDEA is implemented in the BorderGuard router and it will be used for the TSVPN encryption.	IDEA was developed in Switzerland at the Swiss Federal Institute of Technology, at Züriche. It is believed to be a strong algorithm and no practical attacks on it have been published.
IP	Internet Protocol An Internet Standard for the network layer defining an addressing mechanism and rules for routing data packets between addressed systems on interconnected networks.	IP router devices that interconnect networks and IP interface cards in computers attached to a network. Many products.	IP routers will be used to interconnect the Frame Relay Network and patent office networks.

Standard	Technology and Description	Product	Comments
IPSEC	Internet Protocol Security A set of protocols being developed by the Internet Engineering Task Force (IETF) to support secure exchange of packets at the IP layer. IPSEC uses public/private key technology. IPSEC is intended to be a standard that will be acceptable and attractive to equipment vendors whom will incorporate it in their products in order to provide interoperability with equipment from other vendors.	CISCO Systems	The final form of the IPSEC standards is being developed. Consequently, many vendors are taking a wait and see approach before going forward with plans to implement IPSEC in their products.
	Intrusion Detection System A system used with the secure network packet encryptor devices to detect attempts to penetrate or intrude into the network.	NetRanger Probes and NetRanger Director software licensed by CISCO systems.	Intrusion detection depends on recognizing packets that fail to match with what the encryptor expects to see, traffic patterns that differ from normal, or known intrusion patterns. The vendor periodically updates this software to detect new threats.
PKCS#7	Public Key Cryptographic Standard 7 A RSA Laboratories standard for encapsulating data that may have cryptography applied to it such as digital signatures and digital envelopes.	A number of products from RSA Data Security, Inc. use PKCS#7.	The Trilateral Partners have agreed to use PCKS#7 as the standard for applying digital signatures to priority documents and for creating digital envelopes that contain secure priority documents.

Standard	Technology and Description	Product	Comments
	Digital Signature A technique for certifying the data integrity of a digital document and associating the signer with a digital certificate from a trusted third party. To create a digital signature, the object to be signed is processed by a Secure Hash Algorithm to create a small message digest file that is uniquely associated with the signed object. This means that if the digest is recalculated after any change occurs to the signed object, the digest will be different. The digest is encrypted with the public key of the signer to create a digital signature block which is then packaged with the signed object using PKCS#7 rules.	Digital Signature is provided in products from RSA, Trusted Information Systems, Netscape, Microsoft, Entrust and others.	Export restrictions on the use of strong encryption do not apply to digital signatures provided it can be shown that the digital signature software is not readily adaptable to encrypting data content.
	Digital Envelope A technique for packaging encrypted data that combines secret and public key cryptography. Data is encrypted using a unique secret key. The unique secret key (session key) is encrypted using the private key of a public/private key pair. Next, the encrypted data and the encrypted secret key are packaged using PKCS#7 rules for enveloped data. The result of the preceding steps is referred to as data in a digital envelope.	Digital Envelope is provided in products from RSA, Trusted Information Systems, Netscape, Microsoft, Entrust and others.	The recipient of the digital envelope uses the public key of public/private key pair to recover the unique secret (session) key. The session key is used to decrypt the data and then it is discarded. The digital envelope technique uses fast secret key cryptography for bulk data and slower public key cryptography to encrypt the secret key.

Standard	Technology and Description	Product	Comments
PKI	Public Key Infrastructure The standards, procedures and authorities required to issue, publish, manage and revoke digital certificates. Digital certificates are used to identify individuals and organizations that intend to use public key cryptography based services between them.	Netscape Communications Entrust Systems	A PKI consists of: • A Certificate Authority issuing and verifying digital certificates • A Registration Authority to verify certificate applicant identity • Public ITU X.500 standard directories to hold certificates • Procedures and software for managing the certificates
TCP/IP	Transmission Control Protocol and Intenet Protocol An Internet Standard protocol for ensuring reliable end-to-end transfer of data between TCP ports on computers attached to interconnected networks. TCP assembles a message from the IP packets used to send the message. If any message packets are missing or defective, TCP requests retransmission.	TCP/IP is implemented in software that is normally supplied by the computer system vendor or networking software vendor.	TCP/IP will be used for communications between software applications on computers that are connected via the TSVPN. Combined together TCP and IP implement the Network and Transport layers of the ISO 7-layer Network Protocol Model.
	Virtual Private Network (VPN) A technology for providing private communications within a public network by using data encryption. The data payload of packets sent through the network is encrypted and only the header information used to route data across the network is sent as clear text. Data that might be intercepted or monitored by parties other than the intended recipient is protected by the cryptographic system.	BorderGuard packet encryptor device from StorageTek, Inc.	The BorderGuard is installed between the patent office's firewall and the wide area network port in the patent office. The BorderGuards are managed by a network management system that will be located at USPTO. An export license has been obtained to allow using 128 bit cryptographic key lengths.

Standard	Technology and Description	Product	Comments
X.509 Ver. 3	X.509 Digital Certificate Standard An international standard for the format and content of digital certificates. A digital certificate enables a trusted third party to certify (vouch for) the relationship between a public key and information identifying the key's owner.	X.509 is implemented in software that runs on the BorderGuard encryption device. X.509 certificates are authenticated by authentication servers on the patent office networks.	Digital Certificates, Digital Signatures, Public Key Cryptography and procedures for verifying certificates form the basis for a Public Key Infrastructure (PKI). Although the X.509 standard is used, certificate systems from different vendors don't inter-operate readily.