The Internet is Inherently Insecure…

By design, the Internet is an open network which facilitates the flow of information between computers. Technologies are available so the Internet may be used for secure electronic commerce transactions, but failure to review and address the inherent risk factors increases the likelihood of system or data compromise.

Data Privacy and Confidentiality

Unless otherwise protected, all data transfers, including electronic mail and FTP, travel openly over the Internet and can be monitored or read by others. Given the volume of transmissions and the numerous paths available for data travel, it is unlikely that a particular transmission would be monitored at random. However, programs, such as "sniffer" programs, can be set up at opportune locations on a network to simply look for and collect certain types of data. Data collected from such programs can include sensitive data (e.g., credit cards numbers, social security numbers, customer details, orders, payment information) and passwords.

Data Integrity

Potentially, the open architecture of the Internet can allow those with specific knowledge and tools to alter or modify data during a transmission. Data integrity could also be compromised within the data storage system itself, both intentionally and unintentionally, if proper access controls are not maintained. Steps must be taken to ensure that all data is maintained in its original or intended form.

Authentication

Essential in electronic commerce is the need to verify that a particular communication or transaction is legitimate. To illustrate, computer systems on the Internet are identified by an Internet protocol (IP) address, much like a telephone is identified by a phone number. Through a variety of techniques, generally known as "IP spoofing" (i.e., impersonating), one computer can actually claim to be another. Likewise, user identity can be misrepresented as well. In fact, it is relatively simple to send e-mail which appears to have come from someone else, or even send it anonymously. Therefore, authentication controls are necessary to establish the identities of all parties to a communication.

Non-repudiation

Non-repudiation involves creating proof of the origin or delivery of data to protect the sender against false denial by the recipient that the data has been received or to protect the recipient against false denial by the sender that the data has been sent. To ensure that a transaction is enforceable, steps must be taken to prohibit parties from disputing the validity of, or refusing to acknowledge, legitimate communications or transactions.

Encryption Technology and Digital Signatures

Encryption directly addresses the security issues surrounding data privacy, confidentiality, and data integrity. Encryption technology is also employed in digital signature processes, which address the issues of authentication and non-repudiation.

Encryption

Encryption, or cryptography, is a method of converting information to an unintelligible code. The process can then be reversed, returning the information to an understandable form. The information is encrypted (encoded) and decrypted (decoded) by what are commonly referred to as "cryptographic keys." These "keys" are actually values, used by a mathematical algorithm to transform the data. The effectiveness of encryption technology is determined by the strength of the algorithm, the length of the key, and the appropriateness of the encryption system selected.

Because encryption renders information unreadable to any party without the ability to decrypt it, the information remains private and confidential, whether being transmitted or stored on a system. Unauthorized parties will see nothing but an unorganized assembly of characters. Furthermore, encryption technology can provide assurance of data integrity as some algorithms offer protection against forgery and tampering. The ability of the technology to protect the information requires that the encryption and decryption keys be properly managed by authorized parties.

Symmetric and Asymmetric Key Systems

There are two types of cryptographic key systems, symmetric and asymmetric. With a symmetric key system (also known as secret key or private key systems), all parties have the same key. The keys can be used to encrypt and decrypt messages, and must be kept secret or the security is compromised. For the parties to get the same key, there has to be a way to securely distribute the key to each party. While this can be done, the security controls necessary make this system impractical for widespread and commercial use on an open network like the Internet. Asymmetric key systems can solve this problem.

In an asymmetric key system (also known as a public key system), two keys are used. One key is kept secret, and therefore is referred to as the "private key." The other key is made widely available to anyone who wants it, and is referred to as the "public key." The private and public keys are mathematically related so that information encrypted with the public key can only be decrypted by the corresponding private key.

The private key, regardless of the key system utilized, is typically specific to a party or computer system. Therefore, the sender of a message can be authenticated as the private key holder by anyone decrypting the message with a public key. Importantly, it is mathematically impossible for the holder of any public key to use it to figure out what the private key is.

Regardless of the key system utilized, physical controls must exist to protect the confidentiality and access to the key(s). In addition, the key itself must be strong enough for the intended application. The appropriate encryption key may vary depending on how sensitive the transmitted or stored data is, with stronger keys utilized for highly confidential or sensitive data. Stronger encryption may also be necessary to protect data that is in an open environment, such as on a Web server, for long time periods. Because the strength of the key is determined by its length, the longer the key, the harder it is for high-speed computers to break the code.

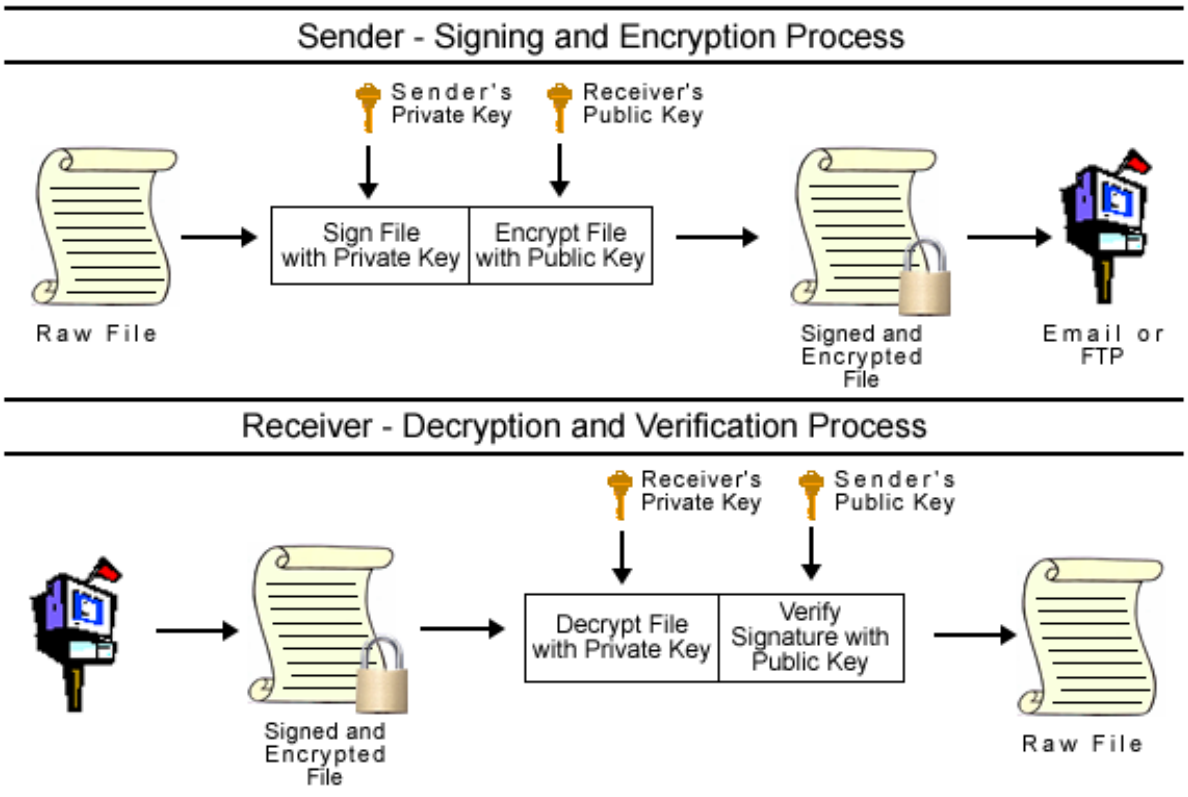
Digital Signatures

Digital signatures authenticate the identity of a sender, through the private, cryptographic key. In addition, every digital signature is different because it is derived from the content of the message itself. The combination of identity authentication and singularly unique signatures results in a transmission that cannot be repudiated.

Digital signatures can be applied to any message (i.e. file or document). To generate a digital signature, the original unencrypted message is run through a mathematical algorithm that generates what is known as a message digest (a unique, character representation of the data). This process is known as the "hash." The message digest is then encrypted with a private key, and sent along with the message.

The recipient receives both the message and the encrypted message digest. The recipient decrypts the message digest, and then runs the message through the hash function again. If the resulting message digest matches the one sent with the message, the message has not been altered and data integrity is verified. Because the message digest was encrypted with a private key, the sender can be identified and bound to the specific message. The digital signature cannot be reused, because it is unique to the message.

The strength and security of a digital signature system is determined by its implementation, and the management of the cryptographic keys.



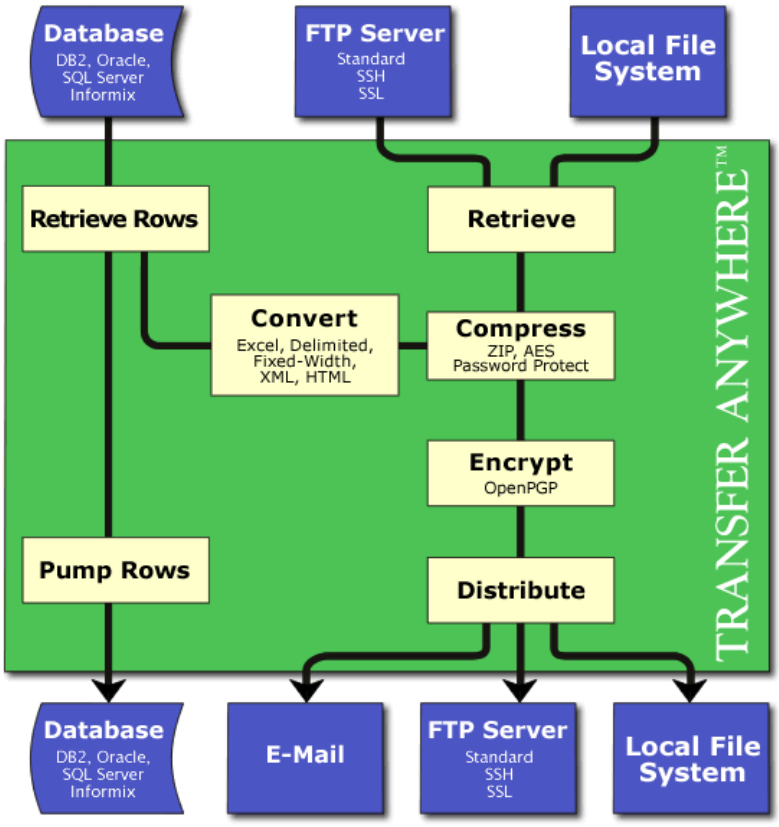
Transfer Anywhere and Open PGP Encryption

Linoma Software's *Transfer Anywhere* product incorporates Open PGP compliant encryption technology to address the privacy and integrity of data. Open PGP encryption implements the preferred asymmetric (public key) cryptography standard for providing a high level of data protection, making Open PGP one of the most popular encryption methods used today. Transfer Anywhere also addresses the issues of data authentication and non-repudiation with the ability to "sign" files via embedded digital signatures.

Transfer Anywhere includes a Key Management facility that can be used by an organization to create keys, change keys, export keys and import keys. These keys can be utilized within Transfer Anywhere for automating Open PGP data encryption and decryption within your organization. Public keys can be exported for sharing with trading partners.

Transfer Anywhere is an enterprise solution for automating encryption and decryption processes. These cryptology functions can run natively on IBM System i, iSeries or Windows platforms.

After signing and/or encrypting files, Transfer Anywhere can automatically place those files on the local file system, or distribute the files to one or more FTP servers or E-mail recipients. For instance, a transfer can be defined to automatically retrieve records from a database, create an Excel document from those records, then encrypt the document and e-mail it to one or more recipients.



Transfers can be executed from within the Transfer Anywhere graphical client or through native iSeries/Windows commands which can be incorporated into your scheduler or batch processes. Additional commands are included with Transfer Anywhere for performing command-line driven Encryption, Decryption, Signing and Verification of files on the local file system.

Linoma Software has also developed a PC-based product named *Crypto Studio* which is a graphical workbench for creating and organizing encryption keys. Crypto Studio can additionally be used to perform desktop encryption and decryption of PC documents. It can be installed onto Windows, Macintosh, Linux and many other graphical desktop operating systems.

Listed below is a chart summary of the Open PGP cryptology features offered by Linoma products.

Feature	**Crypto Studio**	**Transfer Anywhere**
Create, import, export and manage cryptographic keys	**X**	**X**
Encrypt files from the workstation	**X**	
Sign files from the workstation	**X**	
Decrypt files from the workstation	**X**	
Verify signatures from the workstation	**X**	
Associate cryptographic keys with e-mail addresses		**X**
Associate cryptographic keys with FTP Servers		**X**
Encrypt files in batch (System i, iSeries or Windows)		**X**
Sign files in batch (System i, iSeries or Windows)		**X**
Decrypt files in batch (System i, iSeries or Windows)		**X**
Verify signatures in batch (System i, iSeries or Windows)		**X**

Visit www.linomasoftware.com for more information on Transfer Anywhere or www.cryptostudio.com for more information on Crypto Studio. Both products are available for a free trial basis. Linoma Software can be contacted toll-free at 1-800-949-4696 or 402-944-4242 or via e-mail at sales@linomasoftware.com .