



INTERLINK ELECTRONICS, INC.

ENCRYPTION OF ELECTRONIC SIGNATURES, A WHITE PAPER

WHAT IS ENCRYPTION?

Encryption is the translation of data into a secret code and is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it at a later time. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

There are two basic types of encryption, Public-key encryption and Symmetric-key encryption.

PUBLIC-KEY ENCRYPTION

Public-key encryption uses a combination of a private key and a public key. The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key—provided by the originating computer—and its own private key. This is the PKI method, and while very valuable in other parts of the Interlink eSignature architecture, it is not used in the ePad hardware for secure communication.

SYMMETRIC-KEY ENCRYPTION

In Symmetric-key encryption, each computer has a secret key (code) it can use to encrypt a packet of information before it sends it to another computer. Symmetric-key encryption requires that you know which computers will be talking to each other so you can install the same key on each one. Symmetric-key encryption is essentially the same as a secret code that each of the two computers must know in order to decode the information. The code provides the key to decoding the message. Think of it like this: You create a coded message to send to a friend in which each letter is substituted with the letter that is two down from it in the alphabet. So “A” becomes “C,” and “B” becomes “D”. You have already told a trusted friend that the code is “Shift by 2”. Your friend gets the message and decodes it. Anyone else who sees the message will see only nonsense. Interlink uses Symmetric-key encryption in the new ePads for secure transfer of signature data between the device and the host computer (ref. <http://computer.howstuffworks.com/encryption2.htm>).

WHY USE ENCRYPTION IN AN EPAD?

Data sent from a signature pad to a host computer without encryption could be compromised by the use of a USB “sniffer.” A person could intercept the transmission of the data using a sniffer and use the data to sign fraudulent documentation. Interlink Electronics uses Symmetric-key encryption in the ePad for signature data—as well as other data transferred to the



device (such as bitmap images)—in order to secure the data before and during transmission. This method makes a sniffer useless, because the data is encrypted and meaningless to the culprit.

WHAT TYPE OF ENCRYPTION DOES INTERLINK USE?

AES (Advanced Encryption Standard) is the encryption standard that we use as the default, but we also support other symmetric key algorithms such as DES and triple-DES. AES – or The Rijndael algorithm was chosen to replace DES (the previous standard). In June 2003 the U.S. Government (NSA) announced that AES is secure enough to protect classified information up to the TOP SECRET level.

One of the features we employ is a new key for each session using Diffie-Hellman key exchange. What this means is that we choose a new, random key for each session. DH key exchange allows the host and device to share common data that is used in computing the private-key without transmitting the key itself.

The details of a DH key exchange are described at <http://www.netip.com/articles/keith/diffie-helman.htm> and <http://web.usna.navy.mil/~wdj/book/node47.html>

HOW CAN I TELL IF A SIGNATURE HAS BEEN ENCRYPTED AND DECRYPTED?

The encryption is turned on in the Control Panel for the ePad. We have designed the transport in such a way as to make this transparent to the user. So, from the user's point of view, they cannot tell if encryption is enabled or not.

WHY CAN'T OTHER PAD VENDORS USE ENCRYPTION?

NCR owns two very broad patents (5,195,133 and 5,297,202) on the application of encrypting a signature within a signature pad and sending it securely to a host. Topaz, Steptover and other vendors are in violation of these patents and have been claiming the use of encryption to data, but have not obtained a license from NCR to do so legally.

Interlink entered into a licensing arrangement with NCR late last year that that gives Interlink the right to encrypt signatures in their devices, while making it virtually impossible for any other (non-POS) vendor to offer encryption.

HOW ARE INTERLINK'S ENCRYPTION PRODUCTS SOLD?

ePad-ink Pro, ePad-ID Pro, and ePad LS all have SKU's available with and without encryption.