Frequently asked Questions

1. What is a court order?

A court order is an order or decision given by a court. A judge reviews a situation and passes a decision that must be followed. If someone decides to go against the order, they can be held accountable by the court and be in serious trouble.

2. Digital Signatures:

In 1995, the U.S. State of Utah became the first jurisdiction in the world to enact an

ESL (Electronic Signature Legislation). The Utah statute gave digital signatures legal recognition, but did not do the same for other types of e-signatures. The authors of the Utah statute believed, with some justification, that digital signatures provide the greatest degree of security for electronic transactions. Utah was not alone in this attitude; other jurisdictions that grant exclusive recognition to the digital signature include India, Germany, Italy, Malaysia and Russia.

3. Are All Electronic Signatures Valid Signatures:

The disadvantage of the permissive perspective is that it does not take into account that, in fact, some types of e-signatures are better than others. A PIN number and a person's name typed at the end of an e-mail message are both forms of e-signatures, but neither even approaches the degree of security that the digital signature provides.

4. Attributes of a Digital Signature System:

Some of the characteristics of a digital signature system. If the parties to an e-commerce transaction decide to use a digital signature, there is a need for two underlying technologies and a third party: (1) asymmetric cryptology; (2) public key infrastructure ("PKI"); and (3) a Certification Authority ("CA").

5. Asymmetric Cryptology:

Under the Utah Model, digital signatures receive legal protection "only if asymmetric key cryptology produced the digital signature." Such a system employs double keys—the sender uses one key to encrypt the message, and the recipient uses a different, albeit mathematically related, key to decrypt the message. Senders have a private key, known only to them used to generate the digital signature, and the recipient uses the public key, often available online, to verify that the proper party created the message and that it has not been altered during transmission. This is a very good system for e-commerce, since two stranger-parties, perhaps living far apart, can confirm each other's identity and thereby reduce the likelihood of fraud in the transaction.

6. Public Key Infrastructure:

Before a party can digitally "sign" anything, he or she must first be in possession of a pair of keys-the private key and a related public key. The party must apply to a CA to confirm his or her identity. After the CA confirms the applicant's identity, the CA will issue the pair of keys, and a certificate as verification of the subscriber's identity. The CA places the certificate in a public repository, most often the CA's website. Whenever the subscriber digitally signs a message, the CA confirms the signature of the sender; the CA then informs the recipient of the encrypted message which public key is necessary to decode the message. At that point, the recipient is able to access the public key, the decryption code which the recipient uses to read the sender's encrypted message.