E-Signature and Digital Signature

1. A Signature is a mark that proves a person's identity. It may be in the form of a name seal, thumbprint, or QR code. It must be unique to and encrypted for only one person. Forgery of signature is common - the convenience of use should never outweigh the risk.

2. An E-Signature is a virtual signature used to sign a digitized document - usually created with the use of a mouse or a digital stylus (pen).

3. An electronic message such as an email, SMS message, and WhatsApp message may also be an acceptable E-Signature form. A contract can be formed with an electronic message as long as the person's identity can be reasonably authenticated and the electronic message originates from a reliable source. For the source to be deemed reliable, it must be linked to and solely under the control of the signer, and no change to the document post-signing can be detected.

> CAUTION: Passwords to computers and email accounts may be the only security features in-place to generate a valid E-Signature originating from an electronic message.

4. A Digital Signature is used to facilitate the secure electronic transfer of information. A Digital Signature is a legally legitimate contract signing method when it is accompanied by a valid certificate issued by a licensed certification authority (like Adobe Sign).

   A Digital Signature has an embedded Personal Key Infrastructure (PKI). With PKI, the sender signs a document using a private key and the recipient decodes the signature using a public key provided by the sender.