Attachment #17 – PKI Document Change Detection Process

1. User creates a hash of the document.

Document

2. User encrypts the hash using a private key. The encrypted hash, certificate and public key are embedded onto the document.

Encrypted Hash
Public Key
Certificate
Document

User's Private Key

Computed Hash

3. The digitally signed document is transferred across a secured connection to the TVE System.

4. The TVE System receives the signed document and computes a hash of it and also decrypts the embedded encrypted hash with the public key for comparison.

Computed Hash

Encrypted Hash
Public Key
Certificate
Document

User's Public Key

Decrypted Hash

Did the hash match?

No

Invalid Document
(Change Detected)

5. The computed hash is matched to the decrypted hash from the user. If they match, the document has not been changed since it was signed and the signature can be legally binding.

Yes

Valid Document
(No Change Detected)