Digital Signature

Providing a High Level of Assurance

ImageSite Digital Signature™ is an optional module, now included with the core ImageSite, that lets authorized users "sign" documents or markups to indicate authorization and ensure documents stored in the ImageSite repository have not changed since they were signed. Like a written signature, a digital signature functions as a unique identifier. However, a digital signature offers a key benefit — it's quite difficult to forge a digital signature. That's because a digital signature is a code that is attached to a computer generated drawing or document that uniquely confirms the signer.

Benefits of ImageSite Digital Signatures

A digital signature on a document or markup guarantees other ImageSite users that the document has not changed since it was signed, and that the signer is really who they claim to be within the ImageSite user system.

ImageSite makes the act of signing a document irrevocable from the database and further places a date and time stamp, including any comments, along with the digital signature. This provides nonrepudiation, the assurance that the document signer cannot deny the authenticity of their signature or the act of signing itself.

The Technology Behind ImageSite Digital Signature

Using ImageSite Digital Signature is fast and simple, yet the underlying technology is extremely sophisticated. ImageSite creates public and private encryption key pairs for each authorized signer. Public keys and private keys are related in such a way that only one key can be used to encrypt (translate data into a secret code) and only the other key can be used to decrypt them. It is nearly impossible to guess the private key, even if you know the public key.

ImageSite manages these public and private keys using Microsoft's cryptographic infrastructure. The signer's private encryption key is used to sign a document and the signer's corresponding public encryption key verifies the signer's digital signature when the document is accessed by other ImageSite users.

To sign a document or a markup, the authorized signer checks the box next to the desired document component and then clicks the "Sign" button. Next the Microsoft cryptographic technology goes to work.

The cryptographic technology hashes a document, that is, compresses the data into a few lines called a message digest, along with the signer's private encryption key. The resulting digital signature is associated with the signed document or markup layer and stored in the ImageSite repository. When another ImageSite user wishes to verify a signed document or markup layer, they click the "Review, add, or remove digital signature(s)" button. ImageSite then decrypts the digital signature using the signer's public encryption key and compares its message digest with the message digest of the signed document. This process assures the viewer the document remains unchanged since it was signed and confirms the person who signed the document.

Key Features

- ImageSite Administrators grant signing privileges to selected users, by project
- Manages the signing password for users; these signing passwords provide an additional layer of security
- Authorized signers can sign a document, as well as one or more of its markups, at one time
- Allows multiple signers on a single document or markup layer
- Displays special icon for documents with digital signatures
- Displays all digital signatures for a document and each of the document's markups
- Includes date and time information, plus any comments with the digital signature
- Automatically verifies the status of a digital signature when selected by a user; displays a caution symbol if the signature is invalid because the document has been changed.