

ImageSite® Digital Signature™

Providing A High Level Of Assurance

ImageSite® is a Web-based solution for the management, collaboration, and distribution of engineering and technical documents.

ImageSite empowers communication with a single, secure point of access for all project or product information.

- Project Collaboration
- Supply Chain Collaboration
- Engineering Drawing Management
- Design Review Cycle
- Wide-area Facilities Management
- Corporate Document Distribution

ImageSite Digital Signature™ is an optional, separately priced module that lets authorized users “sign” documents or mark-ups to ensure that documents stored in the ImageSite repository are not changed once they are 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 Signature

A digital signature on a document or markup is a guarantee to 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 and further places a

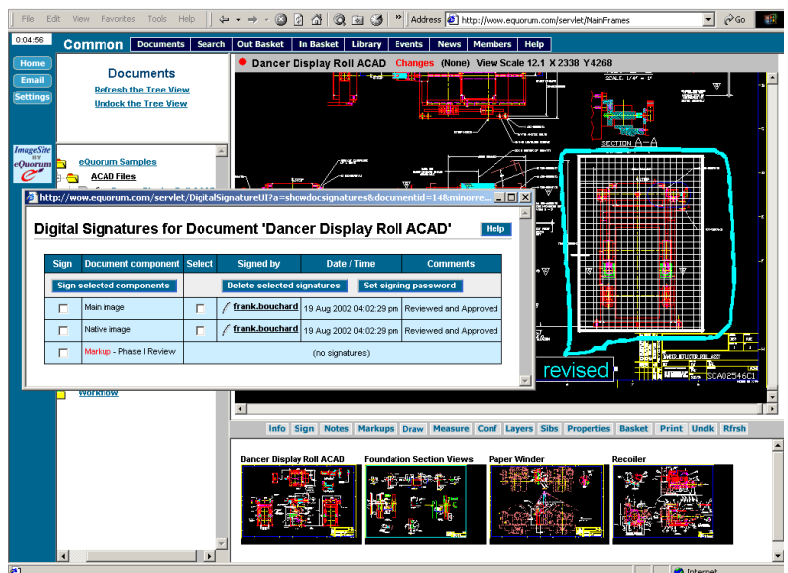
date and time stamp, including any comments, along with the digital signature. This provides *nonrepudiation*, the assurance that the document signer can not deny the authenticity of their signature or the act of signing itself.

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 CryptoAPI infrastructure. The signer’s private encryption



To sign one or more document components, an authorized signer checks the box next to the desired component then clicks the “Sign selected components” button to enter their signing password.


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 markup, the authorized signer checks the box next to the desired document component and then clicks the "*Sign selected components*" button. Next the Microsoft CryptoAPI technology goes to work.

The CryptoAPI 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 stored in the ImageSite repository.

When another ImageSite user wishes to verify a signed document, they click the "*Sign*" 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 that the document remains unchanged since it was signed and confirms the person who signed the document.

General Features

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



**eQuorum • 6285 Barfield Road, 1st Floor • Atlanta, GA 30328
404. 497. 8100 tel • 800. 800. 7568 toll-free • 404. 497. 8101 fax • www.equorum.com**