IdenTrust
part of HID Global

Accepting Digital Signatures Created with IdenTrust® IGC Certificates

The use of digital signatures is becoming more commonplace both in the workplace and for personal use. Digital signing allows organizations to streamline signature and approval processes, eliminate paper and establish an audit trail.

This document was prepared by IdenTrust to help engineering firms and agencies understand how to prepare and accept documents, such as plans and CADD drawings, which include digital signatures.

Information provided in this document includes:

- Background about the ESIGN Act
- Digital signing vs. electronic signing
- Overview of identity-based digital certificates
- Using digital seals
- How digital signatures are created using a digital certificate
- How digital signatures are validated

The ESIGN Act Authorizes the Use of Digital Signatures

The Electronic Signatures in Global and National Commerce Act (ESIGN, Pub.L. 106–229, 114 Stat. 464, enacted June 30, 2000, 15 U.S.C. ch. 96) is a United States federal law passed by the U.S. Congress to facilitate the use of electronic records and electronic signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically.

Although every state has at least one law pertaining to electronic signatures, it is the federal law that lays out the guidelines for interstate commerce. The general intent of the ESIGN Act is spelled out in the very first section (101.a), that a contract or signature "may not be denied legal effect, validity, or enforceability solely because it is in electronic form". This simple statement provides that electronic signatures and records are just as good as their paper equivalents, and therefore subject to the same legal scrutiny of authenticity that applies to paper documents.

Digital Signing vs. Electronic Signing

It must be noted that there are important distinctions between a digital signature and an electronic signature. This is shown in the chart below.

DIGITAL SIGNING

A legal term
Tied to a specific individual via a PKI-based digital certificate
Created using a digital algorithm to bind the document using a certificate, resulting in a unique "fingerprint"
Non-repudiable and auditable
A "hash" of the content being signed - any tampering will be evident
Digital signing is required when using a digital seal

ELECTRONIC SIGNING

A functional term
Not technically bound to a specific individual or validation process
Created options such as typed names, scanned images or a "click wrap" agreement on a web site
Legal, but not easily audited and can be repudiated
Cannot be validated through electronic means

IdenTrust
part of HID Global

Visit IdenTrust.com for more information about IGC digital certificates or contact the IdenTrust IGC sales team at 801-384-3514 or ECASales@IdenTrust.com

Sample Digital Seal

Overview of Identity-Based Digital Certificates

Digital signing requires that the signer use a credential (such as a digital certificate) that is bound to his or her identity. Binding the identity of a signer to the credential that is used for signing creates assurance that the individual who is signing a document really is who they say they are. When an identity-based credential is used, the signature is considered non-repudiable and is legally binding.

IdenTrust issues certificates under the IdenTrust Global Common (IGC) program, a policy owned and managed by IdenTrust and cross-certified with the Federal Bridge PKI program to use for digitally signing and sealing plans and other documentation. IGC certificates are considered identity-based, because the identity of the individual who applies for the certificate is "vetted" by validating that the information provided during the application process is accurate. Only then can a digital certificate be issued.

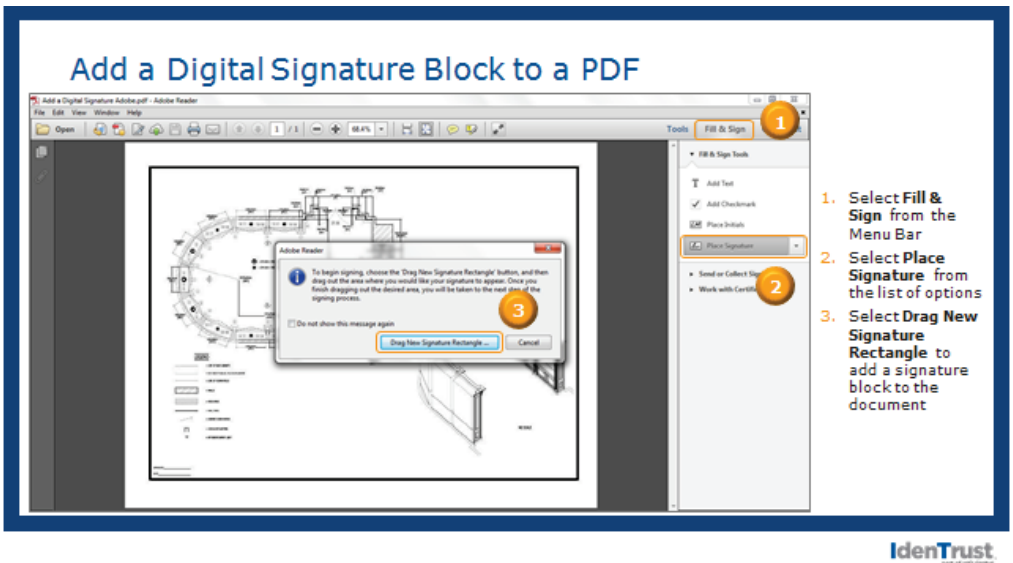
Using Digital Seals

Many federal, state and local agencies now accept digital professional seals (such as engineer, architect, surveyor and notary seals) in conjunction with a digital signature. In fact, some State Department of Transportation (DoT) agencies and cities now require the use of digital signing and sealing on plan submissions. Digital seals can be purchased from various vendors who provide traditional rubber stamps and embossing seals. A digital seal is easily incorporated into a digital signature that is produced when signing with an identity-based digital certificate.

How Digital Signatures are Created Using a Digital Certificate

Typically, documents that are submitted with a digital signature and a professional seal are created using the digital signature function that is incorporated into Adobe®. A digital signature is created by using an identity-based certificate. The digital signature can be configured to incorporate an official digital seal to replace the traditional stamped or embossed seal paired with a wet ink signature.

The following graphics illustrate how digital signing is accomplished in Adobe®.



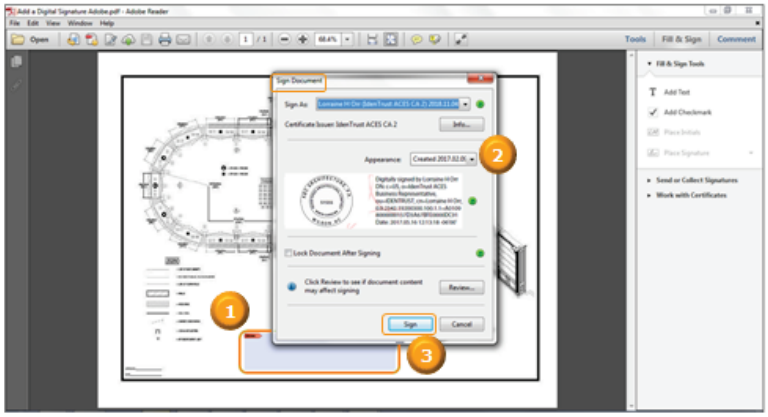
IdenTrust
part of HID Global

How Digital Signatures are Validated

Adobe® also has the ability to validate digital signatures, including validation of the certificate used to create the signature, as depicted here.

Each time a signed Adobe® PDF is opened, the application automatically validates the signature. If more than one digital signature has been applied to the document, then all signatures are validated when opened.

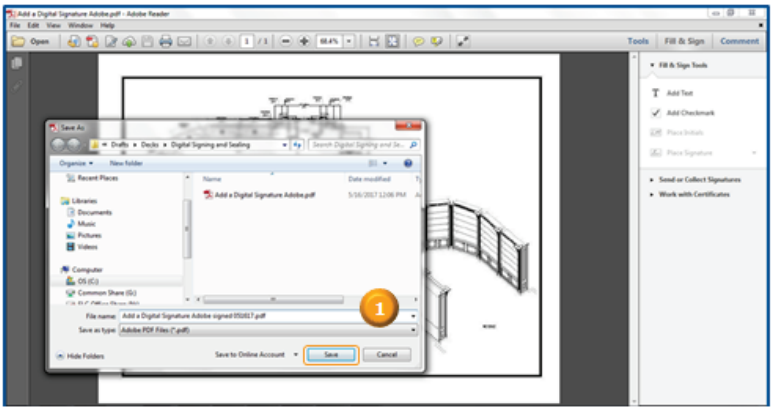
Create the Digital Signature in the PDF



1. After you have drawn the signature block the **Sign Document** window will automatically open
2. You can add your professional or agency seal to the digital signature if desired
3. Select **Sign** to initiate digital signing

IdenTrust

Save the Signed Document



1. Adobe® will require you to **Save** the document before proceeding

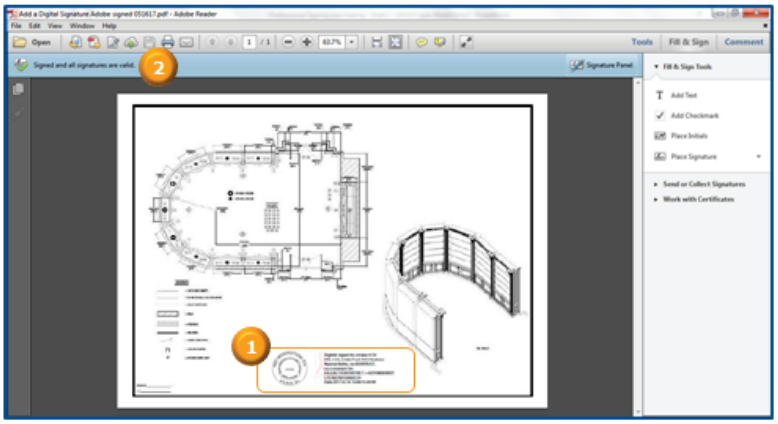
NOTE: A browser certificate can be set up with a password to protect it from use by others.

Certificates that are stored on a token or smart card are automatically protected by a password.

If a password is required the user must provide it before the document can be saved.

IdenTrust

Digital Signature Validated and Placed in Document



1. Once the document has been saved, the digital signature is automatically placed in the document.

NOTE: At this point the document is locked and cannot be altered.

2. The signature is automatically validated and the result of the validation is displayed to the viewer.

IdenTrust

ASSA ABLOY