HID IdenTrust® Digital Signing and Sealing for Engineers and Architects

USE HID IDENTRUST IGC-GOV CERTIFICATES FOR SIGNING AND SEALING

- **U.S. Federal and State Government Approved –** IGC-GOV certificates are recommended for digitally signing and sealing plans and other documentation.
- **Non-Repudiation -** Digital certificates that are bound to a trusted identity are used to digitally sign electronic documents and can be combined with a digital professional seal to create a binding and non-repudiable signature.
- **Inherent Applicability -** Digital certificate protocol is embedded in products like Adobe®, Microsoft® and Bluebeam® facilitating a turn-key implementation for digital signing.
- **Improved Processes -** Digital signing allows an organization to streamline signature and approval processes, eliminate paper and establish an audit trail.

Identity-Based Certificates:

- Fulfill requirements to transact business with municipal, state and federal government agencies
- Are used to sign documents and email communications
- Create a legally-binding digital signature
- Contain information about the certificate holder that has been independently verified before certificate issuance
- Facilitate Digital Signing (vs. Electronic Signing)
- Can be issued to an individual person or to an individual who represents a specific organization

Identity-Based Certificates for Digital Signing

The use of digital signatures is becoming more commonplace both in the workplace and for personal use. However, the difference between digital signing and electronic signing is not widely understood.

True 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.

The use of digital signing introduces added convenience, the elimination of paper and creates an auditable and verifiable electronic workflow.

Adding a Digital Professional Seal

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 plans 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.

HID IdenTrust Provides Identity-Based Certificates

Obtaining an identity-based credential is similar to the process of applying for a driver's license or passport. Registration information is provided via a secure website hosted by HID IdenTrust. Paperwork to prove your business affiliation may also be required. Once your identity has been validated by HID IdenTrust, you are provided with activation information to download your certificate via a secure online website, also hosted by HID IdenTrust.

HID IdenTrust IGC-GOV certificates are compatible with standard applications that support digital signing such as Adobe®, the Bluebeam® document management system and Microsoft® Word, Excel and Outlook and are stored in your internet browser. Optionally, for added convenience and portability, you can purchase a hardware token or smart card to store your certificate.

It is important to understand the differences between Electronic Signing and Digital Signing:

ELECTRONIC SIGNING

- A functional term
- Not technically bound to a specific individual or validation process
- Created through multiple 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 verified through electronic means

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 digital certificate, resulting in a unique "fingerprint"
- Non-repudiable and auditable
- A "hash" of the content being signed – any tampering will be evident

SAMPLE DIGITAL SEAL

Use HID IdenTrust identity-based certificates for digitally signing and sealing plans and other documents for submission to federal, state or local government agencies.

SPECIFICATIONS

Multiple Certificate Types	**Software-Based Certificates**
	• IGC-GOV Unaffiliated Individual Certificate
	• IGC-GOV Business Representative Certificates
	• Install in a browser
	  • Microsoft® Internet Explorer v9+
	  • Mozilla® Firefox
	• 2 year validity period
	  • Renewable online prior to certificate expiration (new certificate fee applies)
	Hardware-Based Certificates
	• All of the features of a software-based certificate and installed in a device providing portability and added security:
	  • HID USB token
	  • HID Smart card
	  • HID Smart card and OMNIKEY® reader
	  • Reuse purchased hardware device at renewal (no fee applied)

Integrated Signing Applications	• Adobe® Reader • Microsoft® Office products • Bluebeam® Document Management application
Supported Platforms	• Microsoft® Windows v7, 8x and 10 • Apple® iOS • Google® Android
Technical Specifications	• X509 v3 digital certificates • 2048+ bit key length • SHA-256 hashing algorithm • Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) validation • Annual WebTrust for Certification Authority audit

IdenTrust part of HID Global

hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 55 9171 1108

HID IdenTrust sales inquiries: +1 866- 763-3346 IGCsales@identrust.com

2020-12-09-iam-ihid-dentrust-digi-sign-seal-eng-arc-ds-en PLT-05630

Part of ASSA ABLOY