

IdenTrust® Digital Signing Solution



DIGITAL SIGNING OFFERS MULTIPLE BENEFITS

- **Non-Repudiation** - Digital certificates that are bound to a trusted identity are used to digitally sign electronic documents, creating a binding and non-repudiable signature.
- **Inherent Applicability** - Digital certificate protocol is embedded in Adobe® and Microsoft® products 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.
- **Multiple Uses** - Electronic documents can be incorporated into online applications, standalone processes and attached to email.

Identity-Based Certificates:

- 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
- Are used to sign documents and email communications
- Create a legally-binding digital signature
- Fulfill requirements to transact business with state and federal government agencies

Digital Signing Using Identity-Based Certificates

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.

How to Obtain an Identity-Based Certificate

Obtaining an identity-based credential is similar to the process of applying for a driver's license or passport.

Digital Signing is Easy to Deploy and Use

Digital signing, through the use of a Trusted Identity, can be used to transact business in a virtual world. This introduces added convenience and the elimination of paper, while creating an auditable and verifiable electronic workflow.

IdenTrust identity-based certificates are compatible with standard applications that support digital signing such as Adobe® and Microsoft® Word, Excel and Outlook.

Multiple Options to Meet Your Business Needs

Depending on the identity-based certificate you select, it can be stored in your internet browser or in a hardware token or smart card, providing added convenience and portability.

Some identity-based certificates can also be used for data and email encryption, helping you to secure your confidential documents and communications.



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



Other Certificate Features

Other available features are defined based on the type of certificate and the program under which it is issued.

- Use when interoperability with U.S. Government applications is required
- Secure emailed communications using digital signing and encryption
- Combine a digital certificate and an electronic professional seal to replace traditional signing and sealing processes

SPECIFICATIONS

Software-Based Certificates	<ul style="list-style-type: none"> ▪ Personal/Individual or Affiliated/Business Certificates ▪ Install in a browser <ul style="list-style-type: none"> • Microsoft® Internet Explorer v9+ • Mozilla® Firefox ▪ 1, 2 and 3 year validity periods are available • Renewable online prior to certificate expiration (new certificate fee applies)
Hardware-Based Certificates	<p>All of the features of a software-based certificate and installed in a device providing portability and added security:</p> <ul style="list-style-type: none"> • Token • Smart card • Smart card and OMNIKEY® reader • Reuse purchased hardware device at renewal (no fee applied)
Integrated Signing Applications	<ul style="list-style-type: none"> ▪ Adobe® Reader ▪ Microsoft® Office products
Supported Platforms	<ul style="list-style-type: none"> ▪ Microsoft® Windows v7, 8x and 10 ▪ Apple® iOS ▪ Google® Android ▪ Additional platforms may be supported based on specific certificate type
Technical Specifications	<ul style="list-style-type: none"> ▪ 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 5081 1650

For IdenTrust Sales inquiries: +1 866-IDENTRUST | +1 866- 433-6878 | sales@identrust.com

© 2017 HID Global Corporation. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design, OMNIKEY and IdenTrust are trademarks of HID Global and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

2017-04-19-iam-identrust-doc-sign-sol-ds-en

PLT-03301