

Secure & Enforceable: The DocuSign Electronic Signature

Introduction

This white paper describes the DocuSign electronic signature in the context of state, federal and international standards for legal and enforceable electronic signatures.

The simplicity of the DocuSign Online Signing Service causes some business customers to mistakenly assume that the DocuSign electronic signature must be unsophisticated. Nothing could be further from the truth. The DocuSign electronic signature is comprised of visible elements as well as invisible, encrypted elements that make it totally secure, legal and enforceable.

Elements of the DocuSign Electronic Signature

The components of DocuSign's electronic signature are managed by the DocuSign service to ensure compliance with all legal requirements for electronic signatures. Those components include both visible and invisible (encrypted) elements.

Visible Elements:

1. Script Signature Name

DocuSign's visual signature contains a script-written name that is generated in the DocuSign system by the document signer. Creating this script signature has legal significance, as the user is required to agree that the script signature will have the same legal effect as his or her handwritten signature.

2. "DocuSigned By:" Box

Every signature is bordered by a signature block that contains a portion of the signer's Globally Unique Identifier (GUID). A GUID is a 128-bit number in hexadecimal form, such as {3F2504E0-4F89-11D3-9A0C-0305E82C3301}, which is created for the signer by DocuSign. The GUID is only partially visible so that the full ID remains concealed.

Invisible Elements:

1. Globally Unique Identifier or (GUID)

Every person in the DocuSign system has a unique GUID. A GUID is a pseudo-random number used in software applications. Each GUID is “mathematically guaranteed” to be unique, based on the principle that the total number of unique keys is so large that the possibility of the same number being generated twice is virtually zero. The full GUID is associated with a user upon authentication and signature creation. The association between signer and signature is managed internally and is both encrypted and hashed to ensure that it cannot be modified. Hashing means that an algorithm has been applied to the GUID to create a digital representation of the GUID in the form of a “hash value.” Any change in the underlying document would produce a different hash value, which would be evidence of tampering.

2. Hash of Signature

The entire signature element is stored in the DocuSign system in secure (hashed) format.

3. Signer Certificate

The data structure of the DocuSign system links a signer’s attributes, GUID and signature stamp to ensure that only that particular person ever has access to use that particular signature.

These visible and invisible elements work together to link the person, the document and the signature in an auditable system. Copying or duplicating only the visible elements of the electronic signature does not compromise the signer’s identity because the invisible elements are solely under the control of the person owning the signature, and are known only to that person. This is analogous to handwritten signatures, in that it is easy to photocopy a handwritten signature but very difficult to copy the minute hand movements, pressure and stroke speed used to write the signature.

Electronic Signature Legislation

State, national, and international laws and agreements set out clear legal requirements for electronic signatures:

» Legislatures in at least 46 U.S. states have enacted the Uniform Electronic Transactions Act (UETA) since its adoption in 1996 by the National Conference of Commissioners on Uniform State Laws. These state laws mirror federal electronic-signature legislation almost word for word.

» The 2000 Federal Electronic Signatures in Global and National Commerce Act <http://www.ftc.gov/os/2001/06/esign7.htm> - N_1_#N_1_ (E-SIGN Act) defines an electronic signature as “an electronic sound, symbol or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.”

» Virtually the same definition is used at the international level. The United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce of 1996 defines an electronic signature as “data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory’s approval of the information contained in the data message”.

Each of these laws require that an electronic signature include certain subtle but important elements that differentiate electronic signatures from less binding forms of agreement such as the 'I agree' buttons on e-commerce web sites. Unlike electronic signatures, the 'I Agree' button does not provide attribution, intent, or secure control of the association among the signer, the signature and the document.

Minimum Legal Requirements of an Electronic Signature

To qualify as an electronic signature under these legal frameworks, the signature must have the following attributes:

1. The signature is an electronic symbol, sound or mark unique to a person. The system must ensure that the symbol is unique and is owned by and under the sole control of a single person.
2. The signature is logically associated with, or affixed to a record. This means the system managing the signing must be capable of attaching the signature to the document in a manner that ensures the document remains attached to the signature and cannot be modified or removed.
3. The signature must be attributable to a person. An electronic record or signature is attributable to a person if it was the act of the person. The act of a person may be shown in any manner, including a showing of the efficacy of a security procedure applied to determine the identity of the person to which the electronic record or signature was attributed.
4. The signature must show the person had intent to sign the record. Intent includes the recording of actions taken by signers that demonstrate that they knew and agreed that they were signing, and that they intended to be bound by their signature. This can be determined from the context and surrounding circumstances at the time of its creation, execution or adoption, including the party's agreement, if any, and otherwise as provided by law.

It is clear from these attributes of legal electronic signatures that simple name stamps, 'I agree' boxes, and names typed into a box do not create valid, non-reputable electronic signatures.

The DocuSign Electronic Signature Meets or Exceeds All Legal Requirements

The DocuSign electronic signature meets or exceeds all legal requirements for valid, non-reputable electronic signatures. Here's how:

1. **Must be a sound, symbol or mark**
DocuSign enables the signer to create a 'signature' element that qualifies as a mark or symbol. The system also ensures that the signature is unique, and only usable by the owner.
2. **Must be affixed or logically associated with a record**
During the DocuSign signing process, a signer affixes his or her signature or initials by clicking "Sign Here" or "Initial" tabs, or by dragging his or her signature onto the page. When signing is completed,

the DocuSign system uses a proprietary method to affix the signatures to the document in specific locations without creating the possibility of tampering. Once affixed, the signature cannot be modified or moved without triggering a fault in the document that would make it invalid.

3. Must be attributable to a person

DocuSign provides several means for attributing the signature to a person. The system gathers authentication information, including email address and IP address. It also provides for enhanced levels of attribution, including requiring the signer to enter the last four digits of his or her Social Security number, answering specific questions from the signer's past, or knowing a secure PIN for a specific signing.

4. Must convey a person's intent to sign

DocuSign has several tools to ensure the person's intent is conveyed. First, a signer must agree to an E-SIGN-required consumer disclosure. Second, a signer must place his or her signature and/or initials onto documents in the locations specified by the sender. This act of reading through the document to find the locations to be signed and initialed is a common practice with paper documents. Finally, after a signer has signed and initialed all the locations in the document, the signer must confirm that he or she in fact wants to complete the signing. It would be impossible for a signer to later claim as a defense that they signed by mistake.

Summary

When the law requires a signature on a contract or other binding document, such as for sales of more than \$500, a simple click-wrap agreement or typed e-signature may not meet the stringent legal requirements for a valid signature. The DocuSign electronic signature, on the other hand, meets and in many cases exceeds the requirements set by E-SIGN, UETA and UNCITRAL for a fully compliant, enforceable electronic signature. Also, encrypting and hashing of DocuSign GUIDs and e-signatures add a very high level of data security to the DocuSign Online Signing Service.

About DocuSign

DocuSign offers an electronic signature service that provides the simplicity, speed and security required to deliver, sign and store documents. Designed from the ground up for business-class usage, this service integrates the technical infrastructure and legal compliance needed to operate an end-to-end signing service. DocuSign customers span a variety of industries and range from the largest corporations to the smallest branch offices. DocuSign, Inc. is a privately held company based in Seattle, Washington.