Article

Signature Capture Guidelines

Table of Contents

Overview

The following are general requirements for electronic signature capture. These requirements are based upon the concepts used to determine the authenticity of any electronic signature-to-document relationship and are based on e-Sign and digital handwritten signature regulations.

All of the data being agreed to (the document or transaction data) should be contained in the original document or transaction data.

The document should be reviewed. A time-and-date stamp can be used to record information about the document, its presentation and acceptance, and any changes that may occur to the document prior to the completion of its review by the signer. The signature should be bound to the entire single document, transaction or message that was reviewed, and to no additional information. Displaying or storing any additional statement or data that may relate to the signature or the intent of the signer should be avoided. These statements or data could potentially conflict with other facts or with the wording in the actual document being signed. The goal is to mimic traditional pen-on-paper transactions - just the document or transaction data and the signature with nothing extra added or subtracted.

The signature should be linked in some way to the document or contract.

The best way to do this is with the Topaz SigPlus binding, which forms a direct cryptographic relationship between the signature and a single document or aggregated data message, and security data.

Changing any document data after capturing the signature results in a binding violation. Without the original document, you cannot examine, print, or display the signature. This is evidence of a powerful link between data and signature. Topaz SigPlus ActiveX software is compliant with state and federal regulations, which require that the signature be cryptographically bound to only a single document message.

The Autokey function provides a cryptographic hash based on a file or a set of data.

Hundreds of data-base cells can be combined to form a single document to be signed. Autokey is commonly used to aggregate all of the database or form cells into a common hash, creating therefore a single message entity for binding to the signature(s).

Patented SigPlus software generates document and signature receipts.

Receipts are unique 8-character strings representing the data content of the signature or the document. They can be provided to the signer as a virtual receipt of the contents of the paperless document being signed. The patented Topaz receipt system allows all parties to detect attempts to tamper with documents or signatures.

The signature should be prevented from being copied by ordinary means.

Binding is the best way to achieve this. The SigPlus ActiveX control signature-capture software binds the signature using the Autokey function or to a hash of your own choice.

The captured signature should be stored in a Topaz .sig file if the application permits.

Storing a signature in a Topaz ".sig" file preserves the original signature in electronic form. No data is lost in a driver layer, and the combination of patented hardware and software facilitates forensic authentication and verification of the signature at a later date.