Article

Robust Signature Capture Using SigPlus® Software

Table of Contents

Robust Signature Capture Using SigPlus® Software

The goal of a good electronic digital signature-capture system is to reproduce the techniques, ceremony, familiarity and convenience of using handwritten signatures on paper to acknowledge a contract. The following example is a suggestion of how to implement a robust signature capture system:

1. *The document or transaction is reviewed by the signer(s).*

2. *The signature is captured using the SigPlus control (TabletState property). This completes the signing process and the completion of signature capture.*

3. *The signature is bound to a document via cryptographic hashing via the AutoKey generation and EncryptionMode functions of the control.*

4. *The Signature and Key receipts are obtained from the control (GetSignatureReceipt, GetKeyReceipt, and corresponding ASCII methods). These are then concatenated together to form a Transaction receipt.*

5. *The Transaction receipt is then printed for or emailed to the customer. The customer can then verify that the Document and Signature portions of the Transaction receipt match those displayed by the application. The Transaction receipt, the signature, and the document data are stored as evidence of the completed transaction.*

If a dispute arises, the stored contract and signature are used to re-generate the receipts. The receipts are then compared to the stored receipts and can be compared to the printed receipt that was provided to the signer at the time of signing. The comparison of the stored receipts to the regenerated receipts from the e-contract is used to provide non-repudiation and to prove that the document and signature are the same as that originally signed. At this point we have proven that the contract is the one signed, and that it was signed with the stored signature. If the dispute continues with the signer claiming that the signature is a forgery, the bound signature and document data are provided to a forensic document examiner utilizing the Topaz SigAnalyze tool and handwriting analysis expertise to authenticate the identity of the signer.

The Signature and Document receipts are unique to the original document and signature. The public distribution and storage of receipts allows for conclusive comparisons at a later date. The validation of the transaction through multiple receipts prevents forgery from going undetected. With reliable receipt storage, it is impossible to modify the document and fool this kind of system, protecting the company and the client. Because each signature is identifiable by its receipt it cannot be used for another document, thus protecting the client.

Since the effectiveness of the Topaz receipt system improves as the reliability of the receipt storage improves, third party PKI can also be employed in the Topaz system. A signing authority can be used to sign the transaction receipt and store it in escrow. This adds proof of when the document was signed, and provides also an independent location for storage of the receipts. This is easily implemented using commercial digital signature services, such as VeriSign.

In addition to the methods used above, the SigPlus software tools are fully compliant with State and federal digital signature regulations. A handwritten digital signature meets the regulations and is captured in accordance with good practice if the signature meets the following conditions:

1. *It is unique to the person using it;*

    The Topaz .sig data format records the original metrics of the signature including all pen events. Image files and bitmaps of the signature can be used for reports, export or printing as long as the original signature .sig format data is used by the SigPlus control to regenerate the image files as needed.

2. *It is capable of verification;*

    Topaz signature analysis software tools are provided to the expert handwriting and document examiner to assess the authenticity of a .sig-format signature.

3. *It is under the sole control of the person using it;*

    The Topaz software tools bind signatures to the message, document, or contract and to no other message.

4. *It is linked to data in such a manner that if the data are changed, the digital signature is invalidated;*

    Autokey is designed so that the totality of the contract data and additional security data is passed through the Autokey function to create binding. There is a direct cryptographic relationship between a single message and the signature.

    The example code below illustrates the basic techniques of capturing and securely binding signatures to document data.

    Capture
    ```
    Private Sub SigPlus1_GotFocus()
    SigPlus1.ClearTablet
    SigPlus1.TabletState = 1
    End Sub
    ```

Bind Signature to Document

```
Private Sub SigPlus1_LostFocus()
SigPlus1.TabletState = 0
Dim text3 As String
text3 = ActiveDocument.Content
SigPlus1.AutoKeyStart
SigPlus1.AutoKeyData = text3
SigPlus1.AutoKeyFinish
SigPlus1.EncryptionMode = 2
SigPlus1.ExportSigFile ("") or .GetSigData or SigString (preferred)
End Sub
```

Electronic Signatures in Global and National Commerce Act

Download the "Electronic Signatures in Global and National Commerce Act" from the Topaz website at: **www.topazsystems.com/links/s761.pdf**.

You can access the act at: **www.senate.gov**. Then, search under "bill s.761". Some important issues are noted below:

Section 101(c)(1) – Consent to Electronic Records

This section applies in situations where there is an existing statute requiring that a copy or the transaction be made available to the consumer in writing. The applicability of this section, therefore, depends on your regulatory environment

Consent to an electronic record is needed if you decide not to give the consumer a written copy (a piece of paper), when normally required. Therefore, if you don't intend to give the consumer a paper copy at any time, then you need to go through the consent requirements and procedure that will assure the consumer that he will be able to see the transaction that has been signed.

However, if you are giving the consumer a paper copy at the time of the transaction, or mailing a paper copy later, even though you are keeping only an electronic version of the contract, then the consent requirements do not apply, because you are not using the electronic record to satisfy the requirement that the information be made available in writing - you are using a paper record to do so. Topaz tablets and inking pens make it very easy to provide a paper version at the same time that the electronic version is created, and a paper copy can always be printed and mailed after the fact, thus eliminating the burden of the consent process. Topaz is also compatible the consent requirements by providing software tools to make the transaction available via e-mail or by the consumer accessing the data using a standard web browser.

Section 106 - Definitions

Electronic Signature - The term 'electronic signature' means 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.

This definition is best suited for electronic handwritten signatures using a pen and tablet, because the person actually does "sign" the record; the intent of the signer is inherent, automatic, and proven by the existence of the signature itself. There is no need to state or prove intent to sign as there would be for other forms of electronic signatures, such as a fingerprint, password, or PKI digital signature.

Important Notice

This software or any or all additional documentation, guidelines, or examples do not constitute a warranty about the performance, security, or legal acceptability of SigPlus software control in any specific use or implementation. To the extent that SigPlus is used to achieve regulatory or other specific objectives within an industry, you must consult competent experts or regulatory officials together with your own plan to achieve your desired business objectives using the Topaz tools.