Mi-Co

Mobile Data Capture Solutions

Electronic Signatures and Mi-Forms

Mi-Forms

As data processes in all industries continue to be automated, there has been a rapidly expanding use of electronic and digital signatures on documents of all types. Businesses are able to accrue large improvements in efficiency by not having to hand-sign every important document on paper hardcopy. To help encourage this transformation, in recent years national law and policy combined with advanced technology have made electronic, digital and wet ink signature capture acceptable for use in place of physical signatures on paper documents.

Electronic vs. Digital Signatures and Wet Ink

The terms ‘electronic signature’ and ‘digital signature’ are often used synonymously, and some confusion can exist about the differences between them. Wet ink signatures are also an option for organizations seeking to automate their paper processes.

- Electronic Signature – is defined by the Uniform Electronic Transactions Act as “an electronic sound, symbol, or process, attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.” The fundamental issue with electronic signatures is security, as they do not necessarily provide integrity or authentication since they are frequently used to simply record images or data.
- Digital Signature – is a certain segment of electronic signature. Also called a digital signature scheme, digital signature is a type of cryptography used to simulate the security properties of a handwritten signature on paper. They are often used to implement electronic signatures, but not all electronic signatures use digital signatures. Digital signature is seen as more secure than electronic signature, but still has issues with trusted time stamping and non-repudiation.
- Wet Ink – is slightly different from electronic and digital signatures since it is essentially capturing a handwritten signature electronically (e.g. signing for a UPS package). Although wet ink is generally associated with weaker security than the previous two options, it has been in use much longer and can now include a record of the image, time, pressure and other key elements to satisfy requirements for security and integrity.

As can be inferred from the descriptions above, legal questions can arise when organizations attempt to completely automate their paper processes by using electronic signature capabilities. However numerous laws have been passed, including US and international law, to ensure the validity and legality of contracts and other documents executed electronically. In the end, the signature requirements of each organization must be determined by their own legal counsel and compliance officers, since their needs will vary depending on the security requirements of their industry.

Mi-Forms and Electronic Signatures

The Mi-Forms technology is flexible when working with signature compliance. Mi-Forms provides built-in wet ink signature capture capabilities due to its inherent handwriting capture and recognition technology, but can also provide electronic and digital signatures when needed. Mi-Forms solutions with electronic signature capture have been deployed by large corporations, federal government agencies and healthcare organizations such as hospitals and pharmaceutical companies. Mi-Forms capabilities which support the needs of electronic signatures include:

Audit Trails

Each time a data record is opened in Mi-Forms, information about the environment on which it was opened is recorded. This environment information includes username, device name, record open time, Mi-Forms versioning, operating system versioning, memory availability, battery level, record end time and potentially record transmittal time. A given record may have an unlimited number of environment information recorded depending on the number of times the data record has been opened and processed. Each environmental information item is accessible via the Mi-Forms object model and is retained for the life of the data record.

When ink data is captured in Mi-Forms, information additional to coordinate data is recorded. For each ink stroke, the user is recorded, the current time-stamp is recorded, and each point's pressure data is recorded if available. This audit data is available via the Mi-Form component's object model and is retained for the life of the record.

When a field's value (text data) is updated, the data that used to be in the field is not replaced. Instead it is moved down a list of available data elements, and its most current data is considered its new value. Every time a data element is recorded with a new value, its time-stamp, updating user and method of input is recorded as well. Data elements are kept for all textual value recording field types.

Workflow and Credentials

Mi-Forms includes workflow capabilities where it is possible to specify which users are allowed to make certain approvals to a record in the system. For example, a workflow may be configured such that a form requires approval before moving to the next step. The approval mechanism for such a workflow is directly connected to the approval function and includes the identity of the approver, when the record was approved, and approval status. These details are recorded within the Mi-Forms record. At each stage of completion, a user may be prompted to enter their credentials to act as an electronic signature. Using a combination of built-in functionality and scripting, the time-stamp of the signature may be displayed in conjunction with user action.

Controlled System Access

The Mi-Forms Client allows for username and password combinations, typically verified via a Mi-Forms Server. Once a user has successfully authenticated once on the Client, the user may continue to use those credentials until they are known to be different (e.g. from a server). Additionally, if a form has been designed to require authentication on start or finish, the Mi-Forms Client prompts the user to re-enter their password at the appropriate time. A time-stamp is recorded indicating when authentication took place. Failure to authenticate correctly at start will result in the form not being displayed. Failure to authenticate correctly on finish will result in the form's data not being exported.

Typically, a Mi-Forms Server is used in cases where authentication is required. The Server has the ability to be the master arbiter of unique usernames and passwords that can be used by a form filling application such as the client.

The Server allows an administrator to specify password policies for all users including providing three levels of password strength and expiration. Additionally, it allows account lockout settings based on failed authentication attempts. Failed authentication attempts are logged by the Server.

It is possible to configure the Mi-Forms Server to use an Active Directory domain controller as its authentication source. If this is done, the domain controller specifies all security policies and they are not modifiable via the Mi-Forms Server itself.

The Mi-Forms Server provides three levels of privileges to known users. These privileges are assigned on the group level and users inherit privileges from all groups of which they are a member. The privileges are as follows:

- User – Allows a user to download form templates assigned to their group(s) as well as upload data records created from these templates. Also allows the user to see data records created by anyone in any group of which they are a member.
- Publisher – Allows a user to publish new form templates
- Administrator – Encompasses all privileges in User and Publisher levels and provides additional functionality. Users with this privilege have the ability to configure security settings, client updates, and licenses updates. They may also manage user permissions and group memberships. They may see all data records uploaded as well as perform actions such as assigning them to different queues (bypassing the workflow of a data record), deactivating/reactivating them or forcing an unlock.

Encryption

Mi-Forms form templates are encrypted to prevent tampering, and all data is secured on the Client using 128-bit encryption. Client-server communications can be encrypted via HTTPS. In addition, all ink and data is recorded, time-stamped and marked with the originating user, and full history for all form sessions is available on the Mi-Forms Server. Security hashing with warnings about tampering and automatic background saving are also available.