

## INTERLINK ELECTRONICS, INC.

### ESIGNATURE ARCHITECTURE – WHERE TO BEGIN?

#### WHAT IS ELECTRONIC SIGNATURE ARCHITECTURE?

An Electronic Signature Architecture refers to the framework for ensuring your workflow automation or security implementation has the appropriate technical foundation to incorporate the benefits of electronic signatures into all channels of your business. Initially, many customers want to address the business channel that generates the most revenue or the one that generates the largest amounts of paper and expense. Though an excellent place to start, catering to just one business channel can present a limited view of what could be a unified solution. A successful implementation will consider all of the relevant business channels and evaluate the approaches used in each.

If you think about all of the business channels—branch office, Web, phone, and mobile agents for example—each option probably involves filling out a form and submitting the completed work to the same back-office service personnel. This back-office group starts by accessing and evaluating the data that is contained within the form or application. They probably don't care where it came from, because it all arrived looking the same—with paper and wet-ink signatures.

#### YOUR BUSINESS NEEDS ALL CHANNELS WORKING IN UNISON

By implementing an Electronic Signature Architecture, your IT organization will have the tools and appropriate framework to enable all of your channels to conduct business and capture customers' consent through whatever means is the most appropriate.

Some examples might be:

1. In-branch: electronic handwritten signature captured on an ePad
2. Web: electronic signature with digital signature tamper-evident seal
3. Phone: personal telephone pin or voice with digital signature tamper-evident seal
4. Mobile Agent: electronic handwritten signature captured on a tablet PC

In the examples above, the technology and their implementations might differ. But how they capture and generate a compliant, legal, and enforceable signature should be the same.

#### WHAT KIND OF SIGNATURE DO YOU WANT?

Consider the reasons for capturing a signature. The technology, its implementation, and the processes must come together to provide a secure signature that can stand up against legal scrutiny. Therefore, it's important to ensure that the desired electronic signature result must be clearly understood and accepted by the business, legal, compliance, and security personnel within your team.

During your planning stages and in meetings with the different organizational stakeholders, you will discuss the type of information, affirmation, security approaches, and required evidence. As a team, you must agree to the elements that will be included within the signature you will seek from your implementation.

#### GENERAL IMPLEMENTATION GUIDELINES

In the next few sections of this document, we will outline some of the key methods used in building a trustworthy electronic signature process. Your organization may use all or a subset or even a hybrid approach to these methods.

## WHO SIGNED?

Of course one of the most important elements of any signature—wet-ink or electronic—is the identity of the signer. The signature, according to law, must be unique, under the sole control of the signer, and verifiable. In most implementations, the handwritten electronic signature is the method organizations start with.

The captured signature provides unique visual and biometric aspects, the pen is under the signer's sole control, and the identity is associated to a reference signature, such as a driver's license or some other ID.

Authentication and authority are paramount in establishing a legally enforceable signature. This authentication process links the signer's identity to a particular document, place, and time of the resulting transaction. When considering authentication and authority within your process, think about the following;

- Identification or authentication itself is only one component of a particular eSignature implementation.
- An eSignature process of authentication can vary widely depending on the implementation. Some signature methods that employ Public Key Infrastructure rely on the network to establish a reliable and traceable authentication path directly to a credential-issuing authority. Other methods may depend on the network of the relying enterprise. The options for establishing signer authentication are rich and varied, regardless of method. It's assumed the process will employ identification or authentication mechanisms that are industry recognized and highly secure.
- Authentication must persist through the signing process and become part of the resulting signature. As in the case of an in-person scenario, the proof of authentication becomes part of the resulting signature to satisfy the legal requirements of proving the signature was created from within a trusted environment.

During an in-person process, an authorized agent is required to authenticate to the platform's network. The signer, however, depending on the implementation, might be authenticated by the agent, by a separate authentication or certifying system, or through the application system itself.

- Once authenticated, the signer could sign by applying their handwritten electronic signature on an electronic signature capture device or by using an issued credential. As in the paper process, someone is required to manage the process on behalf of the enterprise to ensure the signer is, in fact, the right person

## CONSENT TO USE ELECTRONIC RECORDS AND SIGNATURES

Once authentication has occurred, but prior to capturing the signer's actual signature, the process must capture the signer's consent to receive and create an electronic record with legal enforceability. The chosen method should be demonstrable and satisfy the eSignature requirements as mentioned earlier. Federal agencies have provided specific guidance on the requirements in delivering eDisclosures in advance of capturing an electronic signature on a contract or agreement. Your system must:

- Obtain the signer's affirmative consent to use electronic records and signatures
- Provide the E-SIGN Consumer Consent Process disclosures
- Communicate where the consumer may go to find these disclosures after the completion of the process (providing a URL is typical as is printing the actual disclosures). At a minimum, copies of the disclosures must be made available for 90 days after the conclusion of the transaction.
- Provide strategies for meeting the E-SIGN reasonable demonstration requirement
  - o Reasonable demonstration refers to the consumer's ability to access and read the final electronic disclosure or agreement in its executed format. For most implementations, this is satisfied by printing the disclosures during an in-person process.
  - o Another practical way of satisfying this requirement is to print the disclosure and provide an electronic acceptance process where the system will capture the signer's acceptance in receiving the disclosures and opt-in provision showing they have chosen to continue with the process electronically.

## PROVIDING INFORMATION ABOUT THE SIGNING PROCESS

When gaining eSignature consent prior to executing an electronic contract, the signer must understand the eSignature process. Therefore, the disclosure for capturing consent should include a description that informs the signer what steps they will be asked to perform to demonstrate their consent to be bound to the terms about to be outlined in the agreement.

The execution of an eSignature should be preceded by an opportunity for the signer to review a description of the procedure used to create the eSignature and a description of the events that will result in the signature becoming final and effective.

### ESTABLISHING INTENT TO SIGN

The process used to create an eSignature should be designed so that it's clear that the signer intended to create a signature. When not reasonably apparent, the signer is advised that the signature fulfills one or more purposes:

- Affirming the accuracy of information in the record
- Affirming assent or agreement with the information in the record
- Affirming the signer's opportunity to become familiar with information in the record
- Affirming the source of the information in the record
- Other specified purposes

### WHAT GETS SIGNED

Once the signer has been informed of his or her rights and has consented to the process of eSigning, the actual process must be created so the association of the signer, their intent, the data or agreement, and the place and time are inseparable and sufficiently secured should the record itself come under scrutiny.

For this reason, the legal establishment, in its drafting and ultimately the passing of E-SIGN, used the term 'process' signature. In order to be considered a reliable signature-of-record, the burden of proof will fall on the enterprise application architects to show that the process will result in an agreement that is tamper-evident and trustworthy.

A process for signing records should be designed so that the record is presented for signature before the signature is applied; the signature is attached to, embedded, or logically associated with, the record presented; and the process used to attach, embed, or associate the signature shall make for a verifiable, tamper-evident signature.

### ATTRIBUTING A SIGNATURE

The process for signing records should be designed so that either the signature itself provides evidence of the signer's identity (i.e., a handwritten eSignature, digitized signature, or digital certificate) or the process surrounding creation or affirmation of the signature provides evidence of the signer's identity and is in some manner preserved, evidenced, or capable of recall or re-creation during the life of the transaction.

### DEFINING YOUR ESIGNATURE ARCHITECTURE

The process to establishing your Electronic Signature Architecture begins by accessing your existing architecture and infrastructure within your business channels. That means you need to first catalog your existing applications and evaluate the process and technical architecture that is in place today. Once you understand your existing infrastructure and applications within your business channels, you can determine your ideal needs for each.

### WHERE DO I SIGN?

One of the keys to your architecture choices will be where the signing will take place. Will the signer be in-person or online? In either case the document will need to be presented just prior to capturing the signer's electronic signature. Will you present the document in its true format (PDF, Word, TIF, PCL, HTML, etc)? Will you keep it in that format after it has been signed? Will you archive it as-is or convert it to an archive format? Do you keep it a smart document or flatten it? Some of these choices are a function of cost and consideration for existing standards or existing systems.

The choice of document format will also force other architecture decisions, such as what platform to use (i.e., Web, client-server, ActiveX, C#, C++, VB, Java etc). The container or application and its existing architecture will determine the approach to binding the signature to the final document of record.

## ONLINE VS. OFFLINE

Document formats, presentation choices, and respective platforms may also force you to consider the needs for offline vs. online connections. The architecture and their associated platforms will dictate what could be done online vs. offline. Traditionally, thick client and client-server models are used in mobile applications that, by their very nature, make them mostly offline. Regardless of online or offline, Web or client-server, your eSignature Architecture should be adaptable to the platform and connections available.

The implementation choice of signing on a desktop with a client-server, a thick C+ application, or online via server API should not generate a different level of trust in your electronic signature. The eSignature Architecture should ensure that your resulting signature is as trustworthy in one channel as another.

## ARE SIGNED DOCUMENTS FROM DIFFERENT CHANNELS TRUSTWORTHY?

One of the elements of your eSignature architecture is the implementation of a back-end validation application. This application rests within your firewall between the application server and your document management or archive system. It is based on the same technology you've chosen to use to bind signatures to documents.

One of the key benefits of electronically signed documents is the use of encryption to bind and protect the signed documents from tampering. The validation application does two things: 1) it validates that documents received to be processed are legitimate and unaltered, and 2) once validated, it can convert the file to your archive format while retrieving audit information to store with the archived document.

## PULLING IT ALL TOGETHER

Your particular application and process will dictate how your organization will assemble the ingredients for your eSignature implementation. Interlink Electronics has helped many Fortune 500 companies in their eSignature Architecture decisions and is perfectly suited to help your organization plan, design, and implement a solution. We understand that an effective eSignature Architecture requires flexible signing options, varied implementation schemes, key legal components, and ideally a common validation platform tying it all together – providing consistency throughout your organization, and most importantly, a legally binding and enforceable transaction. Interlink Electronics stands ready to provide professional services to assist your organization in needs assessment through implementation.

Please contact us at (805) 484 8855 or [www@interlinkelectronics.com](http://www.interlinkelectronics.com) to find out more.