



Electronic Signature Assurance & the Digital Chain-of-Evidence

Executing Legally Admissible Digitally Signed Records

by Jacques R. Francoeur, B.A.Sc., M.A.Sc., MBA



Table of Contents

1. Executive Summary	3
2. Electronic Signatures shall be Equivalent to Handwritten Signatures — Easier Said than Done	4
3. What needs to be Equivalent — an Electronic Signature?	5
4. The Challenges and Risks of the Electronic Medium	9
5. The Formation of a Digitally Signed Record	11
6. Electronic Signature Assurance	13
6.1 Signing Module	14
6.2 Act-of-Signing	17
6.3 Signed Record	20
6.4 The Digital Chain of Evidence	24
7. The Digital Chain of Admissibility: Meeting Legal Standards & Regulatory Requirements	26
8. Conclusion	29
About the Author	31



1. Executive Summary

The vast majority of information today is generated and processed in electronic form. Consequently the majority of business conducted today is in part or entirely electronic. However, the need to obtain signatures causes business processes to be driven to the physical world, resulting, not only, in delays and costs, but also, in the loss of competitiveness and the ability to adapt. The objective is simple — maintain an end-to-end electronic state throughout the business process. But are electronic signatures legal? Are they regulatory compliant? Can I hold my management accountable for approvals and decisions? Are my contracts enforceable? Can I have the same degree of control and security over my business? The answer is yes, if done correctly.

The U.S. e-Sign Act provides for the non-discrimination of electronic signatures and records when compared to their physical counterparts. In legal terms, the legislation provides the same “legal effect and validity” to an electronic signature as that granted to a handwritten signature on a paper. Note, the legal recognition granted a handwritten signature, which is that of admissibility in a court-of-law, is far greater than the legal recognition granted an electronic signature, which is not to be deemed invalid solely because it is electronic. The key challenge is how to have an electronic signature have the same legal recognition as a handwritten signature — that of admissibility.

In converting from ink-based signatures to electronic signatures, governing laws and regulations describe the overall goal that electronic signatures be generally “equivalent” to handwritten signatures. In order to achieve this requirement, one must understand first what makes an ink signature reliable. Secondly, one must understand what new challenges and risks are created by adopting the electronic medium. There are many abstract and intangible factors involved in the formation of a multi-party electronically signed record. If not performed and maintained reliably, internal approvals may not be accountable; electronic evidence in legal disputes may not be admissible; and regulated processes may not be compliant.

This white paper defines the life cycle of an electronically signed record and describes the equivalence requirements throughout its retention period. A risk management framework called Electronic Signature Assurance will be presented that defines a generic Digital Chain of Evidence that guides the architectural choices available in deploying an electronic signature solution. However, the requirement for equivalence establishes a minimum legal admissibility standard that restricts the architectural choices to high reliability options. The result is a high assurance Digital Chain of Admissibility that holds individuals accountable for approvals and decisions and is deemed admissible and regulatory compliant.

This white paper will lay out an innovative risk management model (Electronic Signature Assurance) and reference architecture (Digital Chain of Evidence) that can be used to deliver confidence that an electronic signature solution can execute signed records that will meet the requirements for legal admissibility.



2. Electronic Signatures shall be Equivalent to Handwritten Signatures — Easier Said than Done

Currently, for a legally significant transaction, such as contract execution, or a regulatory significant transaction, such as e-Clinical Trial approval, electronic documents are printed and ink-based signatures are captured on paper. These signed documents are then stored and archived for a predetermined retention period driven by legal and or regulatory requirements. Anytime during this period, these documents can be called upon in a discovery request and offered as evidence in legal or regulatory proceedings.

Ink signed paper documents are deemed sufficiently reliable to be admitted as evidence due to their intrinsic physical attributes or reliability. That is, they are inherently stable, indelible, durable, self-contained and transportable.

In addition, decades of laws, regulations, precedence and established practices have created a human condition that generally presumes that when individuals sign paper documents, the:

- person signing is who they say they are, their identity can be established from their signature and they have the authorization to sign;
- person signing has applied their signature in a state of informed consent, in full awareness of the meaning of content being signed and the implications of signing;
- intent of their act-of-signing is an agreement to be bound by the content;
- document being signed will not change after the signature, and the signature only relates to the associated document;
- signed document is admissible in a court-of-law and enforceable.

The challenge before electronic signature applications is to impart mechanisms and design architectures that will ensure these physical attributes or reliability are persistently and verifiably “recreated” by design.

In summary, the standard for electronic signed records can be simply articulated by — generating electronically signed records that are legally “equivalent” to their physical counterparts. The FDA 21 CFR Part 11 articulates this electronic-to-physical “equivalence” as follows:

“The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, ... to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.”¹

In addition,

“Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, ... , are intended to be the legally binding equivalent of traditional handwritten signatures.”²

1 General Provisions: 11.1 Scope (a)

2 SP C: Electronic Signatures: 11:100 (c) General Requirements



The requirement for electronic-to-physical “equivalence” is also clearly articulated in the European Union Electronic Signature Directive³ where a special class of electronic signature (i.e., digital signature) is defined with a guaranteed level of legal recognition/admissibility as evidence in a European Union court-of-law, as follows:

*“Member States shall ensure that **advanced [qualified] electronic signatures** that are based on a qualified certificate and that are created by a secure Signing Device:*

- a) satisfy the legal requirements of a signature in relation to data in electronic form **in the same manner** as a **handwritten signature** satisfies that requirement in relation to paper-based data; and*
- b) are **admissible as evidence** in legal proceedings.”*

Requiring that an electronically signed record be “equivalent” to ink-based signed paper is an easy goal to set, but it is easier said than done. Demonstrating how this can be accomplished with confidence is less obvious. However, it can be achieved if one understands the legal and regulatory issues and how technology and process can be integrated into a verifiable digital “chain-of-trust” that is sufficiently reliable to meet legal standards and regulatory requirements.

3. What needs to be Equivalent — an Electronic Signature?

Before one can understand how an electronically signed record can be equivalent to its physical counterpart, one must first understand what it is that needs to be equivalent — an electronic signature.

The definition of an electronic signature as provided by the UN Model Law⁴ is:

An electronic signature is “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 indicate the signatory’s approval of the information contained in the data message.”

The definition as provided by the EU Electronic Signature Directive⁵ is:

“electronic signature means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication...”

Finally, the definition as provided by the US e-Sign Act⁶ is:

“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.”

It is interesting to compare how each of the three bodies of knowledge defines an electronic signature. These three definitions are compared side-by-side in Table 1.

³ European Union Electronic Signature Directive Article 5.1

⁴ UNCITRAL Model Law on Electronic Signatures Article 2a

⁵ European Union Electronic Signature Directive Article 2.1

⁶ United States Electronic Signatures in Global and National Commerce Act: Section 106 Definitions (5) Electronic Signature



Table 1: Electronic Signature Definition Comparison

Electronic Signature Components	United Nations Model Electronic Signature Law	European Union Electronic Signature Directive	U.S. Global and National e-Commerce Act
Electronic Nature of Signature	“data in electronic form	“data in electronic form	“an electronic sound, symbol, or process
Link of Electronic Signature	in, affixed to, or logically associated with	which are attached to or logically associated with	attached to or logically associated with
What is Being Signed	a data message,	other electronic data	a contract or other record
Identification of the Signatory	which may be used to identify the signatory in relation to the data message	and which serve as a method of authentication...”	and executed or adopted by a person
Purpose of Signing	and indicate the signatory’s approval of the information contained in the data message.”		with the intent to sign the record.”

Electronic Nature of Signature: All three definitions are consistent in that an electronic signature is “data in electronic form” with the U.S. e-Sign Act further defining the nature of the data as “an electronic sound, symbol, or process.”

Link of Electronic Signature: All three definitions require the signature to be affixed to or associated with what is being signed. Therefore an electronic signature cannot exist without a context and the specifics of what is being signed.

What is being Signed: All three definitions are consistent in that what is being signed is data in electronic form with the U.S. e-Sign Act further defining the nature of the data as “a contract or other record.”

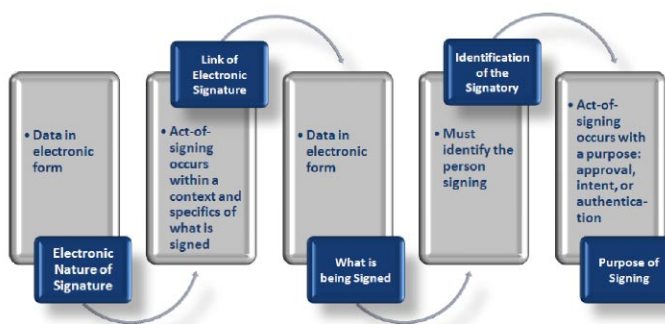
Identification of the Signatory: All three definitions are consistent in that a signature must identify the person signing.

Purpose of Signing: The UN Model Law and the U.S. e-Sign Act definitions stipulate that the act-of-signing must be an act-of-approval or an act-of-intent, respectively and the EU Directive defines the intent as a method of authentication. Therefore, an electronic signature cannot further exist without the existence of intent.



Consequently, in the most general sense these definitions describe the formation of an electronic agreement — a signature in electronic form linked to a record in electronic form with an identified individual performing and act-of-signing for the purpose of approval, authentication or intent. This is illustrated in the figure below.

An Electronic Signature



It is also interesting to compare Table 1 to the definition of an electronic signature as articulated by FDA 21 CFR Part 11, as follows:

“Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual’s handwritten signature.”

The impact of electronic signature legislation such as the U.S. e-Sign Act is to provide for the non-discrimination of electronic signatures and records as compared to their physical counterparts. That is, no signature or record will be deemed inadmissible merely because it is in electronic form. In legal terms this means that the legislation provides the same “legal effect and validity” to an electronic signature and record as to the legal effect granted a handwritten signature on a paper. Note that the legal recognition granted a handwritten signature, which is that of admissibility in a court-of-law, is far greater than the legal recognition granted an electronic signature, which is not to be deemed invalid solely due to being electronic.

For example, the U.S. e-Sign Act⁷ ensures the non-discrimination of electronic signatures and records by ensuring their legal effect and validity, as follows:

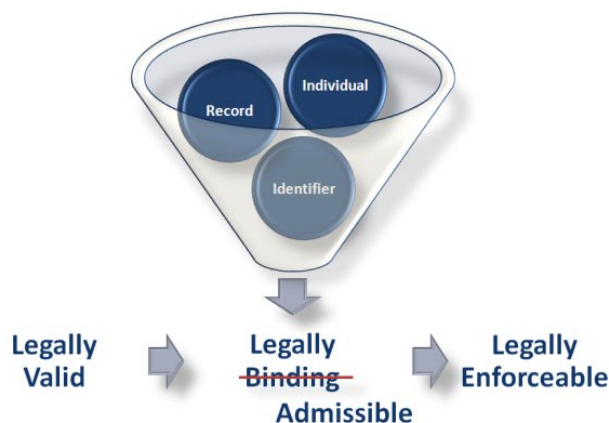
- “1) A signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
2) A contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.”*



The objective is to build from legal effect and validity, as provided by electronic signature legislation, and reach legal admissibility, a prerequisite of enforceable signed records, by designing a signature process that is sufficiently reliable to meet the legal standards.

However, legally binding implies that the implications or meaning of what was signed is enforceable. The enforceability of the “meaning” of the document is subjective and the sole purview of the adjudication authority, such as the arbiter or judge. The legal limit of a reliable signature is that it is deemed sufficiently reliable to be admitted into evidence, a prerequisite of legal enforceability as illustrated in the figure below.

Legally Valid, Admissible & Enforceable



This white paper addresses a specific form of electronic signature, a digital signature that has mechanisms of reliability intrinsic to its form. Such a signature is defined by “21 CFR Part 11” as follows:

“Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.”

However, in order to achieve this, one must understand the challenges that electronic mediums creates in enabling verifiable reliability.



4. The Challenges and Risks of the Electronic Medium

Ironically, the electronic form of data was invented in large part to increase the ease to which it could be created, modified, deleted, substituted and copied. Electronic data is ultimately represented by a series of zeros and ones, inherently volatile and unstable. The inability to differentiate between “good” (original) and “bad” (manipulated) data is a challenge. The mobility of data, its ability to move between systems and applications and people is frictionless. In addition, evidentiary techniques to determine the “provenance” of data such as time-of-creation and unchanged state are immature to non-existent. Therefore, unless mechanisms are put in place, electronic data itself and time can be modified and manipulated, often without detection, creating core challenges to establishing the reliability of electronically signed records. These challenges are illustrated in the figure below.

Challenges of Being Electronic



The transition from ink-based signed documents to electronic equivalents does not impact the need to adhere to existing legal standards, meet current legislative requirements and comply with governing regulations. However, executing legally equivalent and regulatory compliant electronic signatures creates new legal and technical challenges that radically change the methods of meeting the standards and requirements and demonstrating their adherence and compliance.



In order for a signature to be reliable, various bases of denial must be controlled as illustrated in the figure below. FDA 21 CFR Part 11 articulates the requirement for mitigating the possible bases of denial as follows:

*“Persons who use closed systems to create, modify, maintain, or transmit electronic records shall **employ procedures and controls** designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine.”⁸*

Signature Bases of Denial



The ability to refute these bases of denial will depend on the reliability designed into the signed record formation and verification processes. It is not only a matter of signature creation, but also the ability to preserve, verify the integrity, and render the signature and record in human readable form when required. At the core of the ability to maintain the reliability of a signed record over time is the ability to detect any modification after the signature is applied. The UN Model Law articulates this electronic signature integrity requirement as follows:

*“An electronic signature [signed record] is considered to be reliable for the purpose of satisfying the requirement [of law] if any **alteration** of the electronic signature, made after the time of signing, is **detectable**;”⁹*

Similarly, an electronic signature as an act of agreement and intent to be bound or an act of approval and intent to be responsible is predicated on the ability to preserve and verify the integrity of the content signed. That is, the ability to detect any modification to the content after the record has been signed. The UN Model Law articulates this content integrity requirement as follows:

*“An electronic signature is considered to be reliable for the purpose of satisfying the requirement [of law] if, ... any **alteration** made to that **information [record]** after the time of signing is **detectable**;”¹⁰*



Failure to mitigate the bases of denial; or the ability to falsify or manipulate signed record may result in the signed record being deemed inadmissible as evidence in a court-of-law or the inability to assign accountability for internal approvals and decisions.

FDA 21 CFR Part 11 articulates the requirement for ensuring “**accountability**” as follows:

“The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.”¹¹

5. The Formation of a Digitally Signed Record

In order to understand what is required to ensure that a signed record is sufficiently reliable to be deemed admissible and compliant, one needs to understand the stages involved in its formation, retention and final disposition. This white paper focuses on digital signatures, an electronic signature based on asymmetric cryptography (i.e., Public Key Infrastructure). The use of a digital signature does not necessarily mean that the resulting signatures will be reliable.

The stages of a two party signed record transformation process are illustrated in the figure below according to the legend.



11 SP B: Electronic Records: 11:10 (j) Control for Closed Systems



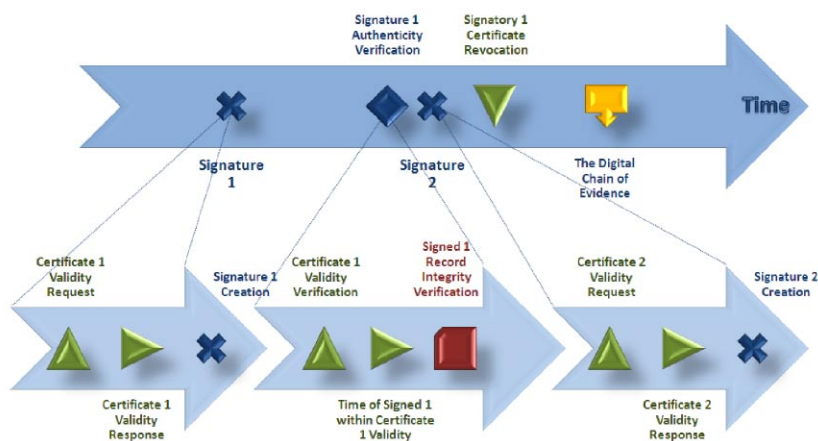
The stages start with the creation of the content to be signed (Unsigned Record). The record is then signed by the first individual (Signatory 1) to create Signed 1 Record. This is then transmitted to the second individual (Signatory 2) who in turn signs the Signed 1 Record to create an official corporate record (Executed Signed Record) for which a legal retention period applies. At the end of this period, the Executed Signed Record can be legally destroyed (Signed Record Disposition). However, anytime during this period, the Executed Signed Record can be required in a legal discovery request (Signed Record Discovery) where its reliability will have to be established. This is the business critical event — demonstrating the reliability of the digitally signed record.

FDA 21 CFR Part 11 articulates the requirement to preserve, verify and render a record throughout its retention period as follows:

“Protection of records to enable their accurate and ready retrieval throughout the records retention period.”¹²

As the record is being signed, there are a number of transparent but critical signature related events occurring in the background that are essential to reliability as illustrated in the figure below.

Signature Events Within Life Cycle



The first key assumption prior to the start of the signing process is that the digital certificates of Signatory 1 (Certificate 1) and Signatory 2 (Certificate 2) are valid, that is, they have not been revoked, suspended or expired. The first record transformation stage is the application of the first signature by Signatory 1 where the Unsigned Record becomes Signed 1 Record. At the time Signatory 1 initiates the act-of-signing, the certificate status of Signatory 1 is verified (Certificate 1 Validity Request). If the status is valid, the Certificate Authority returns a response to that effect (Certificate 1 Validity Response) and the signature is generated (Signature 1 Creation). If the status is invalid, the signing process is terminated.



The second record transformation stage is the application of the second and final signature by Signatory 2 where the Signed 1 Record becomes Executed Signed Record. A precondition of applying Signature 2 is that Signature 1 be authentic (Signature 1 Authenticity Verification), that is, the signature is “what it purports to be.” If the signature of Signatory 1 was applied after the validity of its Certificate 1, then Signature 1 is not reliable. If the content has been modified after the application of the first signature (Signature 1), the Signed 1 Record is no longer what was signed by Signatory 1 and is no longer reliable. Signature 2 should not be applied.

The authenticity of Signature 1 is determined as follows: The identity of the first Signatory 1 is verified to ensure it is the signature of the correct person. The validity Signature 1 is verified by ensuring the time of the Certificate 1 Validity Response was at a time when Signatory 1’s certificate was valid. If not, the signature is unreliable. The integrity of the Signed 1 Record is verified to ensure the content has not been modified since Signature 1 was applied. If the Signature 1 Authenticity Verification is positive, the second signature (Signature 2) is applied in the same way the first signature was applied and the record becomes an official corporate record (Executed Signed Record).

A key question in the life cycle of a digitally signed record is, once the certificate of a Signatory is no longer valid after it was involved in the application of a signature, such as Signatory 1 Certificate Revocation, does this invalidate the legal recognition provided to the of the signature? The answer is no. As long as the certificate of the Signatory was valid at the time-of-signing (Identifier private, secure and under the sole control of the Signatory), the signature has legal effect and validity.

6. Electronic Signature Assurance

Section 2 discussed the attributes and expectations of physical signatures that must be recreated in the electronic counterpart, Section 4 discussed the challenges and risks of adopting electronic signatures and Section 5 discussed the key stages of the record formation process. The pieces are now in place to discuss a framework that will address these challenges, map to the record formation process and translate the ambiguous requirements of electronic-to-physical “equivalence” into a signed record digital chain of evidence.

Electronic Signature Assurance (ESA) is a digital signature risk management framework that defines a generic signed record architecture called the Digital Chain-of-Evidence. This chain-of-evidence contains discrete “links” that can be evaluated for or designed to a level-of-reliability.



The Electronic Signature Assurance framework consists of three segments, illustrated in the figure below.

Electronic Signature Assurance



- 1) **Signing Module:** this segment relates to the reliability of the module used to initiate the act-of-signing;
- 2) **Act-of-Signing:** this segment relates to the individual's state-of-mind at the time-of-signing; and
- 3) **Signed Record:** this segment relates to the methods used to create and store the signed record.

Each segment of Electronic Signature Assurance will be discussed individually.



6.1 Signing Module

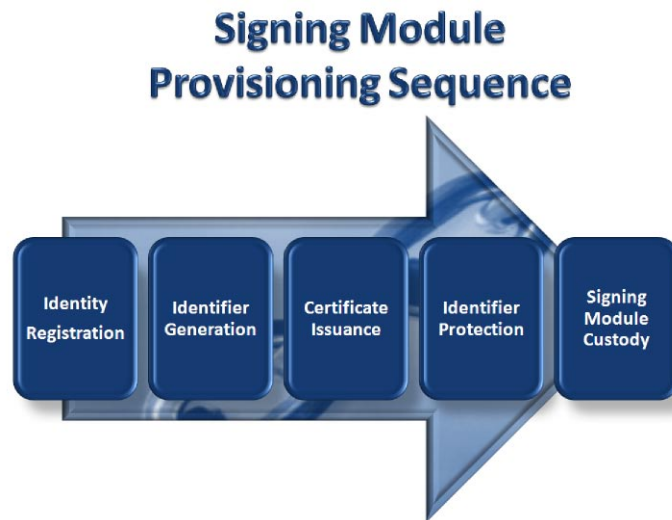
The Signing Module segment of the Electronic Signature Assurance framework relates to the processes involved in provisioning the signing module, whether hardware or software based, used to initiate the act-of-signing. The nature of these processes will determine the reliability of signatures generated by the module. The main function of the Signing Module segment is to establish the true identity of the Signatory by capturing and preserving a reliable and valid digital chain-of-identity. The chain-of-identity establishes the link between an electronic signature, a unique identifier, a registered identity and a physical individual acting as a Signatory. This chain-of-identity should only lead to one individual.

The UN Model Law requirement is articulated as follows:

*"An electronic signature is **considered to be reliable** for the purpose of satisfying the requirement [of law] if the signature creation data [unique identifier] are, ..., **linked to the signatory and no other person;**"*¹³



The reliability level of the digital chain-of-identity is derived from the procedures performed in each of the stages that make up the signing module provisioning process, as illustrated in the figure below.



The primary objective of the process is to transfer sole control of a secure signing module to the Signatory and no other individual.

The UN Model Law articulates this requirement as follows:

*“An electronic signature is **considered to be reliable** for the purpose of satisfying the requirement [of law] if the signature creation data [unique identifier] were, at the time of signing, under the **control of the signatory and no other person;**”¹⁴*

A loss of sole control invalidates the reliability of any subsequent electronic signature created by the signing module. The concept of “sole control” embodies four critical aspects — the uniqueness, privacy, security and exclusive access to the identifier contained in the signing module, hereinafter referred to as “Identifier.” The Identifier is effectively the electronic version of an individual’s “hand with pen.”

The Signing Module segment of ESA is made up of the following provisioning stages:

- 1) **Identity Registration:** the process of establishing the true identity of the individual forming the basis of the Signatory’s registered public identity (stage 3 below).
- 2) **Identifier Generation:** the process of generating a unique Identifier (e.g., Private Key) that can only be associated with one individual — the Signatory.
- 3) **Certificate Issuance:** the process of issuing a public identity (i.e., digital certificate) containing the Public Key that is bound to the registered identity (stage 1 above).
- 4) **Identifier Protection:** The Identifier generated in stage 2 above must only be known by or under the control of the individual — private. This is accomplished through a secure process that places the Identifier in the signing module, while preventing its duplication, and protects the Identifier from unauthorized access or unintended disclosure.

- 5) **Signing Module Custody:** The process of transferring physical custody or logical control of the signing module to the Signatory and no other individual and establishing a second factor of authentication necessary to ensure sole control over the signing module. The second factor of authentication (e.g., PIN or password) is used to ensure that only the Signatory can initiate the act-of-signing.



The Signing Module segment of Electronic Signature Assurance framework contributes two metrics-of-reliability to the Digital Chain-of-Evidence: Signatory Identity and Signing Module. The Signatory Identity metric determines the confidence in the ability to establish the true identity of the Signatory. The Signing Module metric establishes the confidence that no other individual could have initiated the act-of-signing other than the Signatory. In order to establish the reliability of each element of the Signing Module segment, reliability metrics are defined for each as follows and illustrated in the figure below.

Signing Module Metrics of Reliability



This Signatory Identity metric of reliability is composed of the following parameters:

- 1) **Identity Vetting:** the level-of-confidence in the identity of the Signatory is determined by the number and type of independent identity credential used to vet the individual's identity. For example, government issued photo ID credentials such as passports are considered reliable.
- 2) **Identifier Uniqueness:** the level-of-confidence that the Identifier (i.e., Private Key) is unique and can only associated with the Signatory and no other person.
- 3) **Certificate Trustworthiness:** the level-of-confidence in the Certificate Authorities who issued the digital certificates (i.e., Private Keys) in the certificate path, from the Trust Anchor (root) to Signatory's digital certificate, and the ability to determine the current status of the certificates.

This Signing Module metric of reliability is composed of the following parameters:

- 1) **Identifier Security:** the level-of-confidence that only a single instance of the Identifier is in existence and that it is located on the signing module.
- 2) **Signatory Sole Control:** the level-of-confidence that only the Signatory can initiate the act-of-signing.



6.2 Act-of-Signing

The Act-of-Signing segment of the Electronic Signature Assurance framework has less to do with technology than with creating a “state-of-mind” at the time-of-signing. The purpose of this segment is to control a class of denials related to the Signatory’s state-of-mind previously discussed in Section 4: it is my signature but, I did not intend to sign; it is not what I meant when I signed; or I did not understand what I was signing.

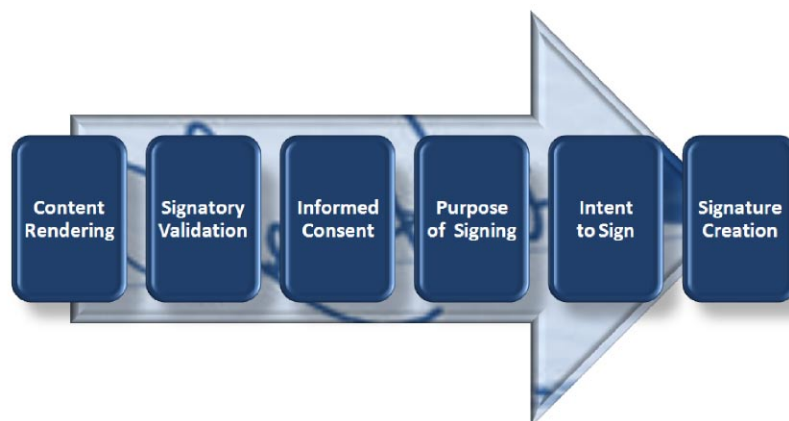
To control this class of denials, the design of the act-of-signing process must demonstrate that a state of informed consent existed in the mind of the Signatory at the time-of-signing. That is, the signing process must demonstrate by design, notice, or response that the Signatory was fully aware that a signature execution process was taking place; clearly understood the purpose of signing; and was sufficiently aware of the implications of signing and the resulting obligations or responsibilities.

The requirement of informed consent originates from an established physical-world legal standard called Legal Sufficiency¹⁵. This legal standard involves two basic elements referred to as “Writing” and “Signature.” These concepts combine measurable parameters, including content with less measurable notions of context, consent and intent. Legal Sufficiency requires that certain transactions, such as contracts, be reduced to writing on paper to be legally enforceable. The requirement is important as it builds awareness that an agreement formation process is taking place and the implications of signing. The functional purpose of “writing” was also to create verifiable records of the obligations that are not subject to manipulation, imperfect memory or competing claims. This needs to be recreated in the execution of an electronically signed record. The second element of Legal Sufficiency is called “Signature.” Legal Sufficiency requires that certain transactions, such as contracts, must not only be reduced to writing but also must contain a signature in order to be legally enforceable. The act-of-signing must clearly establish the identity of the Signatory, and a clear expression of the intent of signing. This also needs to be recreated in the execution of an electronically signed record.

The Act-of-Signing segment can be subdivided into four technology centric processes and two awareness centric processes, as illustrated in the figure on the next page. Content Rendering, Signatory Validation, Intent to Sign and Signature Creation are technology centric and therefore, can be measurable and demonstrable. However, Informed Consent and Purpose of Signing are awareness centric and are difficult to measure and demonstrate.



Act-of-Signing Sequence



The Act-of-Signing segment of ESA is made up of the following stages:

- 1) **Content Rendering:** The process of ensuring what was signed was the content that was rendering to the Signatory — What you See is What you Sign “WYSIWYS.”
- 2) **Signatory Validation:** Verifying that the signing module was reliable at the time-of-signing. This is critical to the legal admissibility of the corresponding signature. A signing module is no longer reliable if its corresponding certificate is revoked or expired or if the security of the Identifier and sole control over the signing module is compromised.
- 3) **Informed Consent:** The process of creating a clear understanding of the meaning of the content and the implications of signing.
- 4) **Purpose of Signing:** The process of creating a clear understanding of the purpose of signing, for example to approve, or agree to be bound.
- 5) **Intent to Sign:** The process to ensure that the Signatory’s intent to sign (initiate the act-of-signing) is an explicit and unambiguous act that cannot occur inadvertently.
- 6) **Signature Creation:** The process of creating the digital signature.



The Act-of-Signing segment of the Electronic Signature Assurance framework contributes two metrics-of-reliability to the Digital Chain of Evidence: State-of-Mind and Signature Reliability. The State-of-Mind metric establishes the level of understanding and awareness the Signatory had at the time-of-signing. The Signature Reliability metric determines the robustness of the digital signature.

In order to determine the level-of-reliability of the Act-of-Signing segment, reliability metrics are defined as follows and illustrated in the figure on the next page.

Act-of-Signing Metrics of Reliability



State-of-Mind: The state-of-mind of the Signatory at the time-of-signing is difficult to establish. However, a few simple measures can be designed into the signing process to drive awareness, clarify intent, and prevent inadvertent actions. The State-of-Mind reliability metric is composed of the following parameters:

- 1) **What You See Is What You Sign:** The content of what is to be signed must be fully rendered to the Signatory in human readable form at the time-of-signing and what is signed must be exactly what was rendered.
- 2) **Informed Consent:** The level-of-confidence that the Signatory had a reasonable understanding of the content and the implications of signing. The Signatory should be required to indicate they have read and understood the content; however it does not guarantee they have.
- 3) **Purpose of Signing:** The level-of-confidence that the Signatory had a clear understanding of the purpose of applying their signature. The Signatory should be required to indicate the reason for signing or the Signatory should receive a notice indicating the purpose of signing such as to be legally bound.

Signature Reliability: The reliability of a digital signature is based on whether at the time-of-signing the Signatory was in good standing, the act-of-signing was not accidental and the robustness of the signature. The Signature Reliability metric is composed of the following parameters:

- 1) **Signatory Validation:** the level-of-confidence that the Signatory was in good standing at the time-of-signing (certificate was valid and signing module was under sole control). The confidence level is also associated with reliability of the validation information (e.g., time stamped, signed) contained in the response (Certificate Verification Report).
- 2) **Intent to Sign:** The level-of-confidence that the Signatory explicitly intended to initiate the act-of-signing. Clear intent to sign is ensured when a second factor of authentication is required to exercise control over the signing module that is, initiate the act-of-signing.
- 3) **Signature Creation:** the robustness of the signature creation process including the hashing function, encryption algorithm and key length.



6.3 Signed Record

The signed record formation process discussed in Section 5 yields a record with one or more signatures that is then stored, subsequently transmitted and processed for business purposes and ultimately archived for legal retention purposes. The signed record at anytime may be called upon in a discovery request and offered as evidence. The questions then become: Does the signed record contain the necessary information and mechanisms of verification to establish its reliability? Will the reliability level be sufficient for the signed record to be admitted into evidence? What information has been captured about the Signatory(s), the content signed, and the time of critical events during the signed record formation process? In addition, what is the “evidentiary quality” of the signed record?

The Signed Record segment of ESA is not a process as in the previous two segments but a series of signed record attributes, illustrated in the figure below, that contribute directly to reliability as follows:

Signed Record Attributes



Signatory Profile: This attribute refers to capturing the Digital Chain-of-Identity. That is, the data objects associated to the Signatory(s) including its certificate, all the Certificate Authority certificates in the certificate path and the corresponding certificate status validation responses received at the time-of-signing. The process of establishing the validity status of the Signatory’s certificate involves requesting and receiving a certified (signed) response from the Certificate Authorities in the certificate path at the time-of-signing. Evidence of this verification and its results as an event uniquely associated with the signed content is essential.

Signature Profile: This attribute refers to capturing the data objects associated with the signing event(s) including the time-of-signing(s), the purpose of signing(s) and the content signed. Note, the Signatory Profile above should be considered an integral part of the Signature Profile.



Self-Evident: This attribute refers to how the signed record is constructed in terms of its ability to independently verify and convey its authenticity at any given time. If the signed record is self-evident, all the information necessary to verify and convey its authenticity is present (self-contained) and the signed record can be verified in real time without external dependence. If the signed record is a distributed object composed of associated data elements, then the signed record must be reconstructed before its authenticity can be established. A self-evident signed record offers the highest level of assurance for preserving the reliability of the signed record over an extended period of time. It also reduces the storage and archival complexity compared to distributed schemes.

Audit Trail: This attribute refers to capturing the series of time-based events occurring in the life cycle of the signed record discussed in Section 5. A signed record involves events before and after its signatures that relate to the overall business or transaction context. For example, the time of final content creation and its prior draft versions provides evidence of content awareness and informed consent in the act-of-signing. This Legal Sufficiency requirement of “writing” was discussed in Section 6.2. In addition, a signed record involved in a business process or transaction involves contextual information related to the intent of the parties, historic information related to the negotiation or case history of the record, prerequisite information such as credit checks and other material information. This information may need to be captured and preserved.



The Signed Record segment of the Electronic Signature Assurance framework contributes three metrics of reliability to the Digital Chain of Evidence: Rendering, Evidentiary Quality, and Trusted Time.

In order to estimate the level-of-reliability of each element, reliability metrics are defined for each as follows and illustrated in figure below.

Signed Record Metrics of Reliability





Rendering: The ability to accurately and completely render the signed record in human readable form and to convey its authenticity at the time of rendering is very important from a business and legal perspectives.

The U.S. e-Sign Act articulates this requirement as follows:

*“Notwithstanding [General Rule of ES Validity], if a statute, ... requires that a contract or other record... be in writing, [its] legal effect, validity, or enforceability... **may be denied if such electronic record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled....**”¹⁶*

This requirement is articulated by FDA 21 CFR Part 11 as follows:

*“The ability to generate **accurate and complete** copies of records in both human readable and electronic form **suitable for inspection**, review, and copying by the agency.”¹⁷*

The requirement to accurately and completely render the signed record applies to anytime during its retention period. The retention period of a signed record is the same as the electronic record.

The U.S. e-Sign Act articulates this requirement as follows:

*“If a... rule of law requires that a... record relating to a transaction... **be retained**, that requirement is met by... an electronic record... that: accurately reflects the information set forth in the contract or other record [transaction]; **remains accessible to all persons entitled to access... for the period required... in a form that is capable of being accurately reproduced...**”¹⁸*

The authenticity of the signed record relates to establishing that it is what it purports to be. This is achieved by performing integrity checks related to the integrity of the content compared to when it was signed and the validity of the signature(s).

Evidentiary Quality: The nature of how the signed record was constructed will affect the ability to verify its authenticity and preserve its reliability over time. The Evidentiary Quality metric or reliability is composed of the following parameters:

- 1) **Self-Verifiable:** To what degree is the signed record a self-contained object? It may, in whole or in part, be composed of distributed data elements. That is, does it contain all the information necessary to verify its authenticity without external dependencies?
- 2) **Tamper Evident:** What is the ability of the signed record, its components or its audit trail to detect any unauthorized modifications (i.e., tampering) over its retention period? For example, the certificate validity status response is a digitally signed data object that is verifiable.
- 3) **Association:** What is the nature of the binding between data elements of a signed record? For example, the definitions of an electronic signature discussed in Section 3, define an electronic signature as electronic data ... affixed to, logically

¹⁶ United States Electronic Signatures in Global and National Commerce Act: Section 101 (e)

¹⁷ SP B: Electronic Records: 11:10 Control for Closed Systems (b)

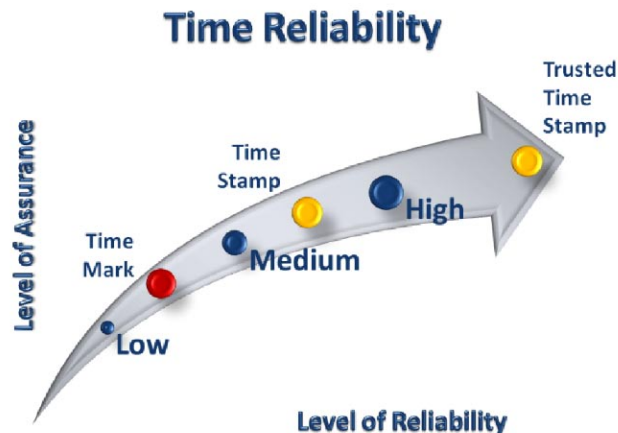
¹⁸ United States Electronic Signatures in Global and National Commerce Act: Section 101 (d)



associated or embedded in ... electronic data (content signed). The robustness of the association will affect reliability. Cryptographically bound objects provide an intrinsic association that is more reliable than non-cryptographically bound objects such as inferred associations of data pointers. For example, a digital signature is the cryptographic binding between the digest and the Identifier (Private Key). This is why a digital signature can be more reliable (if done correctly) than an electronic signature. Also, a Certificate status response cryptographically binds the Certificate Authority's identity to the certificate validity request.

Trusted Time: Time is the only invariant reference that is beyond the control of humans, yet time in a computer system is ephemeral, a parameter set by an administrator or a value contained in a data field or record. Time is one of the most important reliability attributes of a signed record.

The nature of the association between time and data can determine reliability. There are two fundamental ways time is linked to data. The first is inferred by association. For example, when a time value is extracted from a source of time and placed as a value in a data field, such as a record header or file metadata. This is referred to as a Time Mark, as illustrated below, which is an unprotected machine or human readable value representing time. A Time Mark is unreliable as it is susceptible to manipulation without detection.



The second way time can be linked to data is intrinsically bound cryptographically which provides a much higher level-of-reliability. This can be achieved by two means, as illustrated above. The first is called a Time Stamp which is a Time Mark (value of time) added to content to be signed and cryptographically bound, such as what occurs in a digital signature. However, where and how the time is sourced is also important to reliability. Time Stamps are protected against manipulation by all external individuals. However, they are susceptible to time based manipulation by trusted insiders who have



control over the computer systems which manage the data and clocks providing time. It has been said that the “ability to control time in a computer system translates into the ability to alter, create or recreate history.”¹⁹ The second and most reliable cryptographic method is a Trusted Time Stamp. It differs from a generic Time Stamp by providing a verifiable cryptographic association between time from a trusted time source and data, irrespective of who controls the data or computer systems generating time. Cryptographically bound trusted time stamps are part of the ANSI Standard X9.95-2005.

The Trusted Time reliability metric is composed of the following parameters:

- 1) **Source:** What is the level of confidence that the time associated with a data event is the actual time and that it has not been modified? Trusted time stamping standards are intended to ensure the reliability of the time source used by a computer system, referred to as National Timing Authorities (e.g., NIST) and the time stamp created and associated to data. For further information on trusted time stamping, see Internet Engineering Task Force technical specification RFC 3161 and the American National Standard for trusted timestamp management and security ANSI Standard X9.95-2005.

The FDA 21 CFR Part 11 defines the requirement for trusted time stamps as follows:

“Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records.”²⁰

- 2) **Real Time:** The real time nature of critical verification checks are important to Signatories and Relying Parties who depend on the results to make decisions. For example, the act-of-signing process discussed in Section 6.2 has a stage called Signatory Validation. A successful signature execution is predicated on a positive certificate status verification result (a valid certificate at the time-of-signing). If signature execution is allowed to proceed based on a Certificate Revocation List based verification check, there is a risk that the Signatory’s certificate was in fact revoked at the time-of-signing allowing for an unreliable signature to be created.
- 3) **Binding:** What is the reliability of binding between time and data events occurring before, during and after the signed record formation process? These unique data events occur over time creating the transaction audit trail.

6.4 The Digital Chain of Evidence

Section 6.1 through 6.3 discussed the Electronic Signature Assurance risk management framework which is composed of three segments — Signing Module, Act-of-Signing, and Signed Record. Each segment, in turn, was defined by a process that was evaluated by a set of reliability metrics. The Digital Chain of Evidence (DCOE) is constructed from the concatenation of the reliability metrics from each segment, as illustrated on the next page.



The Digital Chain of Evidence



The DCOE is a generic construct of evidence that does not prescribe a level-of-reliability. It simply offers as evidence the electronic data associated with a signed record, its audit trail in combination with details as to how the signing module was provisioned and how the act-of-signing occurred. The DCOE can be used to evaluate the overall reliability of a signed record by evaluating how the Signing Module (Section 6.1) was provisioned, how the Act-of-Signing was executed (Section 6.2) and how the signed record was constructed and stored (Section 6.3). This is, in turn, accomplished by assessing the parameters that characterize each metric of reliability, as illustrated below. The DCOE is only as strong as its weakest link. For example, if a Signatory loses the sole control over the act-of-signing, the signed record is not reliable irrespective of the strength of the rest of the chain.

Digital Chain of Evidence Reliability Metrics & Parameters





7. The Digital Chain of Admissibility: Meeting Legal Standards & Regulatory Requirements

As mentioned previously, the DCOE does not prescribe a level of reliability. The electronically generated data forming the Digital Chain-of-Evidence may be “offered as evidence” in a court-of-law but whether it will be “admitted into evidence” requires demonstrating that it is sufficiently reliable. The key question becomes — what is sufficiently reliable?

Guidance on the standards of evidence to be met is provided by the Federal Rules of Evidence.²¹ However, this guidance must be interpreted with the ever increasing context of electronic records. This subject is considered beyond the scope of this white paper and the reader is referred to the recent work on digital evidence by the American Bar Associate.²²

In general, the level-of-reliability must be appropriate for the purpose of the signed record, the legal significance of the act-of-signing, and the nature and level of the risks, including consideration of the damages that can ensue from the failure of any Signatory to fulfill its obligations. Consequently, the level-of-reliability should be established on a case by case basis.

Level of Assurance: Legal Standard



The UN Model Law articulates the required level-of-reliability as follows:

“Where the law requires a signature of a person, that requirements is met... if an electronic signature is used which is as reliable as was appropriate for the purpose for which the data message [agreement] was generated...”²³

²¹ Federal Rules of Evidence: <http://judiciary.house.gov/media/pdfs/printers/109th/31310.pdf>

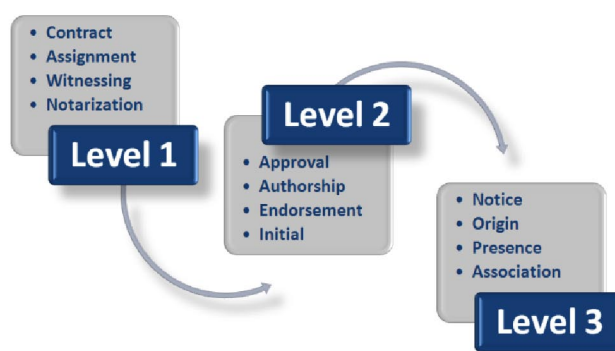
²² Working draft on “Foundations for Digital Evidence,” American Bar Association, publication expected Nov. 2007.

²³ UNCITRAL Model Law on Electronic Signatures Article 6.1



Without the context of what is being signed, the purpose of a signature is undetermined. The level-of-reliability is associated with the purpose of the act-of-signing — the intent of what is being signed. The act-of-signing has a number of intended effects, some with more legal significance than others, as illustrated below. Consider the following intended effects of signing.

Legal Significance of the Act-of-Signing



Clearly there is a difference in the legal significance between signatures with the intent to assign legal ownership of intellectual property (Assignment) as compared to a log of an attendance to an event (Presence). Consequently, the purpose and legal significance of the act-of-signing establishes its commensurate level-of-reliability. If the purpose of a signed record is to provide internal “approval,” the level-of-reliability does not necessarily have to abide by the same external legal standards as accountability can be taken care of by established corporate practices and policies.

The appropriate signed record level-of-reliability can be defined as follows:

“... sufficiently reliable commensurate with the legal significance of the act-of-signing and the nature and risk of the transaction.”²⁴

The Digital Chain-of-Evidence is intended to be designed to a prescribed level of reliability. For example, if the objective is to ensure that signed records are deemed admissible into evidence in a court-of-law, the chain must be designed to meet both the requirements set forth by electronic signature legislation and the legal standards established by precedence. Similarly, in the case of regulated processes such as New Drug Applications submitted electronically, the reliability will be governed by 21 CFR Part 11. Consequently, the chain must be designed to meet the general requirements of 21 CFR Part 11 or the more specific requirements established under the SAFE standard.²⁵ Note, both the legal and SAFE standard are aligned with the core objective of legal admissibility. Different standards and their level of assurance are conceptually illustrated in the figure on the next page.

²⁴ Jacques R. Francoeur

²⁵ <http://www.safe-biopharma.org>



Signed Record Level of Assurance



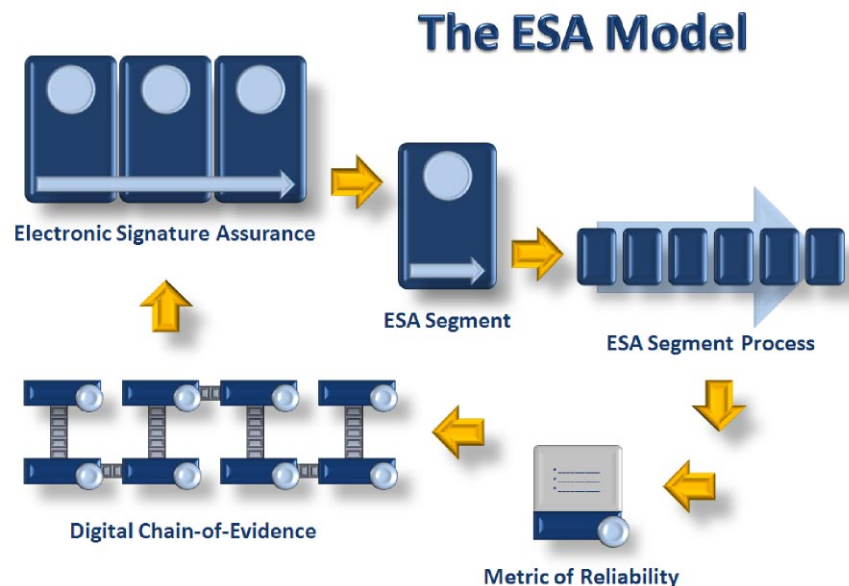
A Digital Chain-of-Evidence designed to meet the legal standard is referred to as the **Digital Chain-of-Admissibility**.

It is important to differentiate between “closed” and “open” signing communities. A closed signing community is one that relies on regulations and trading partner agreements to establish the signed record formation process and the necessary level-of-reliability. That is, the level-of-reliability of a signed record executed by partners governed by a trading partner agreement will be governed by what was agreed. An open signing community is one which relies on laws and legal standards to establish the necessary level-of-reliability. That is, the legal admissibility of a signature for “agreement” purposes between legal entities in an open environment, not governed by a trading partner agreement, will be governed by state and federal electronic signatures laws and established precedents.



8. Conclusion

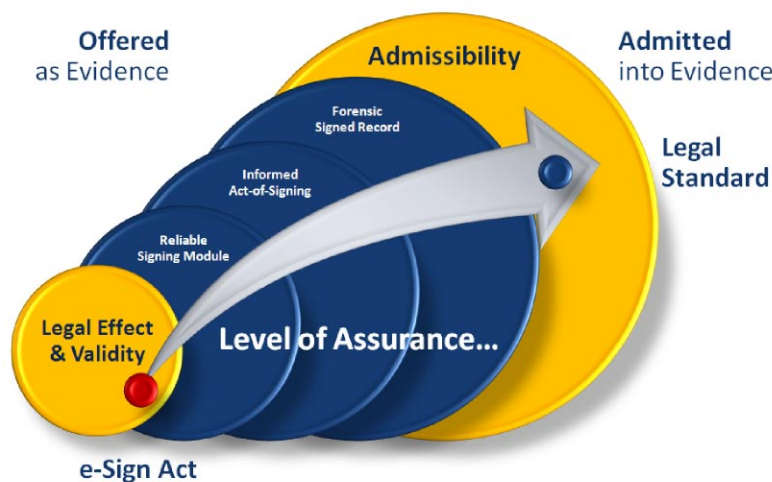
In order to ensure that digitally signed records will be admitted into evidence (deemed legally admissible) the level of reliability of the signing method must be architected to a prescribed level. To achieve this, reference architecture is required to identify and define the elements that contribute to the reliability of a signed record. Electronic Signature Assurance is an electronic signature risk management framework that defines a measurable reference architecture called the Digital Chain of Evidence. Electronic Signature Assurance is composed on three segments, Signing Module, Act-of-Signing and Signed Record. Each segment in turn is defined by a process that defines the critical stages that contribute to reliability. Each segment has reliability metrics that can be used to evaluate the reliability of the segment process. The concatenation of the reliability metrics forms the reference architecture — Digital Chain of Evidence. This model and architecture is illustrated in the figure below. The Digital Chain of Evidence can be designed to meet a specific level-of-reliability, such as legal standards, resulting in a Digital Chain-of-Admissibility.





Electronic signature legislation such as the U.S. e-Sign Act ensures the non-discrimination of electronic signatures and records solely on the grounds of being in electronic form. It does so by ensuring their legal effect and validity. The requirement for admissibility is predicated on the level-of-reliability of the signed record and its formation process. The objective is to start from legal effect and validity, as provided by electronic signature legislation, and reach legal admissibility, a prerequisite of enforceable signed records, by designing a Digital Chain-of-Evidence that is sufficiently reliable to meet the legal standard, as illustrated in the figure below.

The Path to Admissibility



The method of achieving the admissibility standard is to ensure: the Signing Module is sufficiently reliable (a strongly vetted Signatory and trustworthy Signing Module provisioning process); a responsible act-of-signing, involving a clear state-of-mind at the time-of-signing (informed consent, purpose of signature, intent to sign, awareness of obligations or responsibilities); and a clear act of initiation (Signatory was the only individual that could have initiated the act-of-signing); the signed record was constructed, preserved and rendered in a way demonstrates accuracy, completeness and verifiable authenticity.

In summary, a reliable electronic signature application is one that captures, preserves, retrieves, verifies, makes available and renders in human readable form anytime during the retention period, the authentic content, context, intent, identity and time to a level-of-reliability commensurate with the legal significance of the act-of-signing and the nature and risk of the transaction.



About the Author

*Jacques R. Francoeur (B.A.Sc., M.A.Sc., MBA)
VP, Professional Services, ProofSpace*

As Vice President of Professional Services at ProofSpace, a company specializing in high assurance digital evidence, Francoeur is responsible for professional services and thought leadership. As a domain expert and evangelist in trusted electronic business and legal admissibility of electronically stored information, Francoeur regularly authors white papers and makes presentations internationally.

As Executive Director of the Bay Area CSO Council, a nonprofit member-based organization, Francoeur manages a trusted virtual community of leading Bay Area Chief Security Officers (CSO), and hosts private and public CSO round tables.

Previously, as Sr. Marketing Manager and Information Assurance Evangelist at Adobe Systems, Francoeur was responsible for field enablement, customer advocacy, messaging, and executing go-to-market strategies for Adobe's Enterprise Rights Management and Digital Signatures solutions.

Francoeur founded TrustEra and Forensic Signature Corp., specializing in the fields of enterprise electronic risk management and high assurance digital signatures, respectively. Francoeur also served as an instructor of Trusted e-Business and Trusted e-Systems at the University of California, Berkeley Extension. His 20-year career in the technology industry also includes a stint as KPMG's National Privacy Support Manager, Director of Trust Practices at NetFront Communications, and Director of Trust Practices at CertifiedTime (under contract).

Francoeur is an experienced public speaker and established author and is often invited to speak on the legal, regulatory and technical aspects of electronic business assurance, including digital accountability, digital trust management and digital signatures. Francoeur holds a Bachelor's degree in Aerospace Engineering and a Master's degree in Applied Science from the University of Toronto. He earned his MBA from Concordia University in Montreal.



ProofSpace
900 Clancy Ave NE
Grand Rapids, MI 49503
(312) 933.8823