ASB Technical Report 189, First Edition
202X

Forensic Reliability of eSignatures for a Determination of Authorship

DRAFT



This document is copyrighted © by the AAFS Standards Board, LLC. 202X All rights are reserved.
410 North 21st Street, Colorado Springs, CO 80904, www.aafs.org/academy-standards-board.

Forensic Reliability of eSignatures for a Determination of Authorship

ASB Approved Xxxxx 202X

410 North 21st Street
Colorado Springs, CO 80904

This document may be downloaded from: www.aafs.org/academy-standards-board

This document is provided by the AAFS Academy Standards Board. Users are permitted to print and download the document and extracts from the document for personal use, however the following actions are prohibited under copyright:

- *modifying this document or its related graphics in any way;*
- *using any illustrations or any graphics separately from any accompanying text; and,*
- *failing to include an acknowledgment alongside the copied material noting the AAFS Academy Standards Board as the copyright holder and publisher.*

Users may not reproduce, duplicate, copy, sell, resell, or exploit for any commercial purposes this document or any portion of it. Users may create a hyperlink to www.aafs.org/academy-standards-board to allow persons to download their individual free copy of this document. The hyperlink must not portray AAFS, the AAFS Standards Board, this document, our agents, associates and affiliates in an offensive manner, or be misleading or false. ASB trademarks may not be used as part of a link without written permission from ASB.

The AAFS Standards Board retains the sole right to submit this document to any other forum for any purpose.

Certain commercial entities, equipment or materials may be identified in this document to describe a procedure or concept adequately. Such identification is not intended to imply recommendations or endorsement by the AAFS or the AAFS Standards Board, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Proper citation of ASB documents includes the designation, title, edition, and year of publication.

This document is copyrighted © by the AAFS Standards Board, LLC. 202X All rights are reserved.
410 North 21st Street, Colorado Springs, CO 80904, www.aafs.org/academy-standards-board.

Foreword

Electronic execution of documents has become routine across commercial, governmental, and personal transactions, and a wide range of technologies now capture or represent a signature in electronic form. These technologies differ markedly in what they record about the act of signing, ranging from a record that anyone could reproduce to a high-fidelity capture of biometric data unique to the signer.

The legal validity of an electronically signed digital document and the forensic reliability of an electronic signature for a determination of authorship are distinct properties. The identity-proofing and fraud-prevention measures that a platform applies are likewise distinct from both: they serve the platform's decision to permit a transaction, and a measure adequate for that decision is not, for that reason alone, evidence from which authorship can be determined. An eSignature implementation can satisfy the conditions for legal validity while capturing no, or insufficient, information to determine the signer's identity and meet legal scrutiny. The signature and platform records that accompany it are assertions about who signed, not proof of it. For forensic purposes, the operative question is therefore the degree to which an eSignature implementation captures and preserves evidence by which those assertions can be examined after the fact. Whether a given implementation can support a determination of authorship depends on whether it preserves biometric data of the signer in a form available for examination and on the quality of the data it preserves.

This technical report provides a general overview of the types of electronic signatures currently deployed and of the principles that govern their relative forensic reliability for a determination of authorship. It is intended to assist forensic document examiners, the legal community, and others in understanding the distinctions among electronic signature implementations and the limits of what each can establish about the signer's identity.

The American Academy of Forensic Sciences established the Academy Standards Board (ASB) in 2015 with a vision of safeguarding Justice, Integrity, and Fairness through Consensus-Based American National Standards. To that end, the ASB develops consensus-based forensic standards within a framework accredited by the American National Standards Institute (ANSI), and provides training to support those standards. ASB values integrity, scientific rigor, openness, due process, collaboration, excellence, diversity and inclusion. ASB is dedicated to developing and making freely accessible the highest quality documentary forensic science consensus Standards, Guidelines, Best Practices, and Technical Reports in a wide range of forensic science disciplines as a service to forensic practitioners and the legal system.

This document was revised, prepared, and finalized as a technical report by the Forensic Document Examination Consensus Body of the AAFS Standards Board.

Questions, comments, and suggestions for the improvement of this document can be sent to AAFS-ASB Secretariat, asb@aafs.org or 410 N 21st Street, Colorado Springs, CO 80904.

All hyperlinks and web addresses shown in this document are current as of the publication date of this standard.

ASB procedures are publicly available, free of cost, at www.aafs.org/academy-standards-board.

Keywords: forensic document examination, eSignatures, electronic signature, digitally captured signature, dynamic data, biometric data, authorship

DRAFT

Table of Contents *(to be finalized upon document completion)*

1 Scope 1
2 Normative References 1
3 Terms and Definitions 1
4 Legal Validity and Forensic Reliability as Distinct Properties 3
5 Preserved Biometric Data as the Basis for Authorship Determinations 5
6 eSignature Implementations That Do Not Preserve Biometric Data 7
7 eSignature Implementations That Preserve Biometric Data 8
8 Signing Session Data in eSignature Platforms 14
9 Document Integrity as a Distinct Question 17
10 Summary 18
Annex A: Bibliography 20

DRAFT

Forensic Reliability of eSignatures for a Determination of Authorship

1 Scope

This technical report provides an overview of the types of eSignatures that are currently deployed and their relative forensic reliability for the determination of authorship. This report also addresses the signing session data generated by eSigning platforms and the limits on what such data establishes about the identity of the signer.

This report addresses the integrity of the signed digital document only to the extent necessary to distinguish it from the question of authorship. Whether a digital document has been altered after signing, and whether the binding between an eSignature and the document contents remains intact, are questions of document integrity that are distinct from those addressed in this report.

2 Normative References

There are no normative reference documents.

3 Terms and Definitions

For purposes of this document, the following definitions apply. Additional terms can be found in ASB Technical Report 071, *Forensic Document Examination Terms and Definitions*, 1st Ed., 2025.

3.1
audit trail
A record produced by an eSigning platform that aggregates information about a signing transaction into a single document.

3.2
authorship
The execution, by a particular individual, of the act that produced a retained signature.

3.3
biometric data
Data representing measurable physical or behavioral characteristics of an individual, recorded from a signing act or other biometric presentation.

NOTE Where only a static image of the signature is preserved, the biometric data are limited to the spatial form of the signature.

3.4
decoupling
The separation of a credential, identifier, or retained signature from the person, signing act, or document with which it is associated.

NOTE Examples include a credential used by a person other than its holder, an uploaded signature image supplied without any signing event the platform observed, and a retained signature reapplied to another document.

DRAFT

3.5
digitally captured signature
DCS
A signature executed on a device that records the signing act as time-sequenced biometric data representing the physical parameters of the act, usually including the spatial path of the signature, its temporal characteristics and, where the device senses it, the force applied.

3.6
dynamic data
Time-correlated biometric data recorded during a handwritten signing act.

NOTE 1 These data comprise the sampled position of the writing instrument, the associated time values, the pen-up and pen-down states and, where the device senses it, the force applied. Values such as velocity and acceleration can be derived from them.

NOTE 2 The term is used in its forensic handwriting sense, not in the information-technology sense of continuously updated data.

3.7
electronic signature
eSignature
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.
[15 U.S.C. § 7006(5)]

3.8
eSigning platform
The software service through which a record is presented for signature and through which the retained signature and associated transaction records are captured or received, as distinct from the physical device on which the signing act is performed.

NOTE Referred to in this document as "platform."

3.9
forensic reliability (for a determination of authorship)
The degree to which an eSignature implementation preserves biometric data from which a credible determination of authorship can be made after the fact through forensic examination.

NOTE In general evidentiary usage, reliability is the credibility and trustworthiness of proffered evidence.

3.10
hash
A string of numerical values used to substantiate the integrity of digital evidence or for inclusion/exclusion comparisons against known value sets or both.
[ASTM E1732-26]

3.11
legal validity
The condition of meeting the legal requirements for a document, agreement, or act to be recognized and given effect under applicable law.

NOTE For an eSignature implementation, the degree to which it meets the requirements of, is not prohibited by, and does not conflict with applicable legislation, such that the signed record has the same legal effect as a physically signed paper document.

3.12
media-dependent alternate style
MDAS
A habitual signature style, developed and reproduced by the signer on a particular input medium, that differs from the signer's conventional signature.

3.13
retained signature
The image, text, data, or other record of a signature that an eSigning platform or other system retains, as distinct from the act of signing that produced it.

NOTE Where the retained signature preserves biometric data, those data are the object of forensic comparison; where it does not, the retained signature records the signing event without recording who performed it.

3.14
Static image
A rendering of a signature that preserves its spatial form but not the dynamic data of the signing act.

NOTE 1 Variation in line width can appear in a static image but is not derivable as a representation of force.

NOTE 2 Platform rendering, including smoothing or "beautification," can alter the image's correspondence to the signing act.

4 Legal Validity and Forensic Reliability as Distinct Properties

4.1 Two Properties of an eSignature Implementation

This document addresses two distinct properties of an electronic signature implementation: legal validity (3.11) and forensic reliability (3.9).

Legal validity is governed by statutes including the Electronic Signatures in Global and National Commerce Act (ESIGN) [1], the Uniform Electronic Transactions Act (UETA) as enacted in most United States jurisdictions [2], the Electronic Identification, Authentication, and Trust Services Regulation (eIDAS) in the European Union [3,4], and analogous frameworks in other jurisdictions. Forensic reliability is not governed by any legal authority; it is a determination made on a case-by-case basis as to whether a given eSignature implementation preserves information that allows for a credible determination of authorship.

4.2 Relationship Between Two Properties

A wide range of eSignature implementations satisfy legal validity. ESIGN and UETA adopt technology-neutral approaches [1,2], and the eIDAS Regulation adopts a technology-neutral baseline within a tiered, risk-based framework [3], accepting as legally valid a range of acts that indicate the signer's intent to sign. These acts can include checking a box, typing a name, drawing on a touchpad,

uploading an image of a signature, signing on a digitizer pad, and applying a cryptographic key to a document.

Forensic reliability for a credible determination of authorship, however, varies across this same range of acts. Some of the acts listed above preserve no information capable of supporting an authorship determination. Others preserve the handwritten characteristics of the signer to a degree comparable to a wet-ink signature on paper. The two properties are not coextensive; an eSignature can be legally valid without being forensically reliable, and the legal frameworks listed above do not, in general, require that all legally valid eSignatures also be forensically reliable.

4.3 Handwritten Likeness Requirements

Most regulatory frameworks governing the legal validity of eSignatures do not impose a handwritten likeness requirement. The ESIGN and UETA Acts, which together govern most eSignature transactions in the United States, adopt technology-neutral approaches [1,2] under which the legal validity of an eSignature does not depend on whether the resulting signature bears the likeness of a handwritten signature. Comparable frameworks in other jurisdictions follow the same general approach.

Some legal frameworks impose a handwritten likeness requirement on certain categories of eSignatures. A handwritten likeness requirement specifies that an eSignature, to be valid in a particular context, must bear the likeness of the handwritten signature of the signer. California Assembly Bill 1977 (2025-2026 Regular Session, Irwin), enacted as Chapter 280, Statutes of 2026, imposes such a requirement on the electronic signatures of notaries public in the context of California's framework for online notarization, providing that a notary's electronic signature, which must include an image of the notary's handwritten signature, match the notary's handwritten signature on the official oath required under Section 8213(a) of the California Government Code [5]. The scope of the requirement is limited to the notarial signing capacity rather than to electronic signatures generally.

Technology-neutrality accommodates the broad range of electronic signing methods in use, which differ in their technical capabilities and the characteristics they capture, whereas a handwritten-likeness requirement constrains the range to methods that capture the signer's handwritten act. The eSignature industry's own compliance literature reflects a technology-neutral approach to electronic signing. The Electronic Signature and Records Association identifies technology neutrality as a core organizational principle [6], and the published compliance materials of major eSignature providers describe the ESIGN Act as technology-neutral and as favoring or requiring no particular signing technology [7,8,9,10].

The industry's technology-neutral position thus confirms that legal sufficiency is independent of whether the signing act captures any handwritten characteristics, which is precisely the separation of legal validity from forensic reliability that this report describes. A handwritten likeness requirement, where its terms require the eSignature to be produced through a handwritten act of the signer, aligns the legal-validity property with the forensic-reliability property in the contexts where it applies. The technical basis for this alignment is developed in Section 5.

5 Preserved Biometric Data as the Basis for Authorship Determinations

Authorship is a form of attribution. To determine the authorship of an eSignature is to attribute the act that produced it to the person who executed that act. In the context of eSignatures, the act can be clicking a button, typing a name, drawing a signature, or applying a cryptographic key.

Forensic attribution of the signing act has its direct basis in biometric data of the individual who executed the act, preserved by the eSignature implementation. A record that any person performing the same act would produce carries no information identifying who performed it and, by itself, supports no attribution. Preserved biometric data, by contrast, can be compared against known examples attributable to that individual and assessed for attribution.

The forensic reliability of an electronic signature is determined by the information that the implementation captures and preserves—any observable or measurable characteristic, including static morphology, dynamic data, and metadata, capable of contributing to a determination of authorship—and not by the terminology, assurance level, or classification assigned by the eSigning platform, the technical controls it employs, or the legal validity of the transaction.

Whether an implementation preserves anything unique to the individual depends on the nature of the act it records. Some acts produce the same output regardless of who performs them. Any person who checks a given box, types a given name, or selects a given font produces a record that is indistinguishable from one produced by another person performing the same act, and the record captures the choice that was made without recording who made it. Other acts impart characteristics particular to the person performing them. Any person who signs a sufficiently complex signature by hand produces a signature that differs from one produced by another, in accordance with the principle of individuality, through the combined effects of motor control, neuromuscular habit, learned form, and characteristic variation, in ways that a forensic document examiner can observe, measure, and compare [15,16]. The validation base for the examination of dynamic signature data is addressed in 7.5.

The preservation of biometric data, data representing characteristics particular to the person who produced them, provides the direct basis for an authorship determination. It marks the point at which comparison becomes possible; it does not predetermine what the comparison will establish. Where an implementation preserves no biometric data, it retains nothing individual to compare, and attribution of the signing act, where it can be made, rests on circumstantial evidence outside the retained signature, addressed in Section 8. Whether an implementation preserves biometric data partitions eSignature implementations into two analytical categories, which are addressed separately in Sections 6 and 7. Preservation, not capture, is the criterion: an implementation that captures a biometric presentation but does not preserve it falls within Section 6, and one that preserves biometric data falls within Section 7. Whether the eSigning platform itself captured the signing act or instead received a record of an act performed on another occasion is a distinct provenance property; it bears on reliability within the second category and is addressed in Section 7.

The significance of preserved biometric characteristics lies in their susceptibility to examination. Every eSignature implementation asserts, implicitly or explicitly, that a particular person performed the signing act; what varies among implementations is whether that assertion of attribution can be independently tested. Where the implementation preserves biometric data in a form available for examination, the assertion can be evaluated by comparison against known exemplars, by an examiner independent of the platform that generated the record. Whether the

comparison supports a determination is a further question, resolved by examination rather than by category; a signing act of simple construction can yield biometric data whose features, however faithfully captured and preserved, are too limited to distinguish the signer from other possible authors. Where a biometric mechanism participates in the signing process, but the biometric signal is not preserved in a form susceptible to examination, the record establishes only that the mechanism reported a result. That result can accurately reflect the underlying event, but its accuracy cannot be evaluated from the record, and the conditions under which the mechanism would report the same result for a different person cannot be excluded or assessed. The comparative reliability accorded to implementations that preserve biometric data accordingly reflects not a property of biometric technology in general, but the examinability of the preserved data, as the preserved data carry within them the evidence by which the implementation's assertion of attribution can be tested.

A recurring condition that limits attribution is decoupling, the separation of a retained signature, credential, or identifier from the natural person, signing act, or document with which it is associated. A cryptographic credential can be used by a person other than its holder; an uploaded signature image is supplied to the platform already separated from any signing event the platform observed; a retained signature can be decoupled from the signing session in which it was captured and reapplied to other documents; and the signing session data generated by a platform describe network endpoints, devices, credentials, and communication channels rather than the natural person operating them. In each case, the decoupled element remains associated with the transaction, while its connection to the person who performed the act can be established only by evidence beyond the retained signature or record itself. These conditions are addressed in Sections 6, 7.4, 7.8, and 8, respectively.

A determination of authorship is not a determination that the signer possessed the legal authority, intent, capacity, or authorization to execute the document. Nor does a determination of authorship establish that the signer reviewed, approved, or understood the document with which the signature is associated. Nor is a determination of authorship the same as the legal attribution of an electronic signature, which under the Uniform Electronic Transactions Act can rest on a showing of the efficacy of a security procedure (8.3) and associates the transaction with a credential, account, or verified identity rather than examining the signing act. These issues fall outside the scope of forensic document examination and can require legal, factual, or other technical analyses independent of the examination of the retained signature. A determination of authorship extends no further than the attribution of the signing act to the individual who executed it.

That eSignature implementations are not interchangeable in practice is a proposition that the eSignature industry itself recognizes. Under the technology-neutral frameworks of ESIGN and UETA, the major providers treat every electronic signature as carrying equal legal validity, whether produced by a click, a typed name, a drawn mark, or a cryptographic key. Operating under eIDAS, the same providers market a tiered product line of simple (SES), advanced (AES), and qualified (QES) electronic signatures in which only the qualified tier received, under eIDAS Article 25, the legal effect equivalent to a handwritten signature [3]. A single provider thus stratifies its offerings by assurance level when a framework demands it and presents them as equivalent when one does not; the equivalence asserted under ESIGN and UETA is a legal default rather than a statement that all electronic signatures are alike in substance.

Independently of the governing framework, providers' authentication guidance reflects the same recognition, advising that the strength and number of authentication methods applied to a transaction should increase with the risk and value of that transaction [11,12,13,14], an escalation that

presupposes the available methods are not equivalent in the assurance they provide. These measures, which can extend to identity proofing and fraud and risk prevention drawing on data that are not part of the transaction record, serve the platform's decision to permit a transaction, require additional verification, or refuse it; their design and adequacy are not evaluated in this report. A measure adequate for that decision does not, for that reason alone, serve as evidence from which authorship can be determined, and its outputs bear on authorship only as signing session data, to the extent that they are recorded in or produced from the transaction record (Section 8). Forensic reliability for a determination of authorship is a further stratification of the same underlying non-equivalence. The partition adopted in this report is drawn on a distinct axis; it distinguishes implementations by whether they preserve biometric data of the signer, a property independent of a signature's legal tier or cryptographic assurance level.

6 eSignature Implementations That Do Not Preserve Biometric Data

This section addresses eSignature implementations that preserve no biometric data of the signer. With the exception of cryptographic digital signatures, addressed at the end of this section, these implementations produce a signature that is not unique to the signer, because any person performing the same action produces the same output.

Implementations of this kind include the following:

a) click-to-sign and checkbox signatures, created when the signer activates a button or checkbox to indicate intent to sign, for which the retained signature is a record of the click event together with session data;

b) typed-name and font-rendered signatures, created when the signer enters a name that the platform retains as typed text or renders in either default or user-selected fonts, for which the retained signature is the text string or an image produced in the typeface; and

c) procedurally generated signatures, produced when the platform constructs a signature image from the signer's input or selections through an algorithm or template rather than from the signer's handwriting.

In each of these implementations, the retained signature carries information about the choices made by the signer but preserves no biometric data of the signer. Two signers performing the same action produce identical retained signatures, distinguishable only by the account and session data associated with each event. None of these retained signatures, standing alone, support an authorship determination; what can be established about the identity of the signer in such a transaction rests on evidence outside the retained signature, addressed in Section 8.

Cryptographic digital signatures present a distinct case. A cryptographic digital signature is created when a cryptographic key controlled by the signer is applied to a hash of the document content, producing a mathematical value that binds the key to the document. Public Key Infrastructure (PKI) provides the technical framework for issuing, managing, and verifying the keys used in this process. Under eIDAS, the advanced and qualified electronic signature tiers described in Section 5 rely on cryptographic mechanisms of this kind, and a qualified electronic signature additionally requires a qualified signature creation device and a qualified certificate issued by a qualified trust service provider [3].

The value produced by a cryptographic digital signature is unique to a key, not to a person. Its production requires control of the signing credential, so the value is not something any person could replicate, and the trust scheme governing a qualified electronic signature can, in principle, associate the credential with a single identified holder. Key uniqueness is not, however, biometric uniqueness. Even where a signature creation device requires a biometric presentation, such as a fingerprint, to activate the signing credential, the biometric is consumed at activation, and no record of it is preserved in the resulting signature. Such an implementation captures a biometric presentation but does not preserve it, and accordingly falls within this section.

A successful activation establishes that a biometric sample matching one enrolled on the device was presented at the time of signing; it does not identify the person who presented it. A device can permit the enrollment of fingerprints or other biometric patterns from more than one individual under a single credential, and neither the presented sample, the enrolled templates, nor the matching process is preserved in a form available for examination. A biometric activation requirement can reduce the likelihood that a credential is used by a person other than its holder, but a positive activation result, unaccompanied by preserved biometric data, is of limited value for establishing attribution, because the possibility that the credential was activated by a different enrolled person cannot be excluded from the record. The activation result is in this respect an assertion generated by the device, of the kind addressed in Section 8, rather than a record from which attribution can be independently assessed. A credential can also be transferred, compromised, or used by a person other than its holder, and the trust scheme relies on technical and administrative controls rather than biometric mechanisms for addressing these contingencies. The cryptographic signature is designed to establish whether a particular cryptographic key was used to sign a particular document, not who used it. Where no biometric data are preserved with the signature, it contains nothing for an examiner to compare for the purposes of determining authorship.

7 eSignature Implementations That Preserve Biometric Data

7.1 General

This section addresses eSignature implementations that preserve biometric data of the signer. In most of these categories, the signing process itself captures the act from which the data are recorded; in one, the uploaded or scanned signature image addressed in Section 7.4, the act is performed outside the platform and only a static record of it is supplied. Whether the platform captured the act is a provenance property that bears on the reliability of the preserved data and is reflected in the parameters set out in Section 7.2. The implementations in this section are amenable to a determination of authorship, with reliability that varies along several parameters.

7.2 Comparative Reliability Framework

The reliability of an authorship determination depends on the quality of the biometric data preserved by the implementation. The following parameters structure the comparison among the categories addressed in this section.

a) **Fidelity of motor behavior capture**: spatial resolution, sampling rate, and (where applicable) force resolution.

b) **Preservation of dynamic data**: the time-correlated biometric data of the signing act. Dynamic data can be lost when an eSignature is rendered as a static image only, even when the underlying capture process recorded the dynamic data.

c) **Susceptibility to reuse and transposition**: the ease with which the retained signature can be decoupled from its original signing event and applied to a different document.

d) **Susceptibility to a media-dependent alternate style (MDAS)**: whether the input medium induces a signature that departs from the signer's conventional signature, in which case meaningful comparison can require additional known standards produced under comparable conditions rather than conventional exemplars alone.

e) **Production of a signature consistent with the natural range of variation**: whether the signing process permits the signer to produce a signature in a manner consistent with the signer's habitual handwriting, such that the resulting signature falls within the natural range of variation observed across multiple instances of the signer's signature.

f) **Provenance of the signing act**: whether the act was performed and recorded within the signing session that the platform observed, or was instead performed on another occasion and supplied to the platform as a finished record.

The evaluation of these parameters depends upon the quality and completeness of the data made available for examination. In many implementations, the signature embedded within a Portable Document Format (PDF), printed document, or platform-generated report represents only a rendered version of the underlying signature record. Native platform records can preserve additional information, including dynamic data, metadata, timestamps, sampling characteristics, coordinate information, or cryptographic values, that is unavailable from the rendered output alone. Information that was not preserved during the signing process, or that has been discarded or omitted through rendering, conversion, compression, or other transformations, might not be possible to recover.

7.3 Drawn Signatures Retained as Static Images

A signature in this category is created when the signer draws a signature using an input device such as a computer mouse, a laptop touchpad, or a touchscreen operated with a finger or stylus, and the implementation retains only the resulting image rather than time-sequenced data. An implementation that records and retains the signing act as time-sequence data, regardless of the input device, is addressed in 7.5.

This implementation preserves biometric data of the signer, in the form of a drawn image, and therefore provides a basis for forensic comparison. The reliability of the examination can nonetheless be affected by the input device. Mouse and touchpad input devices can impose limitations on the signer's motor behavior, and the resulting signatures can exhibit reduced natural variation, distorted forms, and degraded fluency compared with the signer's habitual handwriting on paper. A signer might or might not also have an MDAS style specific to pointer-device or touchscreen input. Where the signer draws with a stylus on a touchscreen but the implementation retains only the resulting image, the motor act more closely approximates handwriting with a pen, and the constraints that mouse and touchpad input can impose on the signer's motor behavior can be correspondingly reduced.

Constraints due to the input device can vary, but the retained signature is only the resulting image, and its capture fidelity is correspondingly limited. The image preserves the pictorial form of the signature only at the resolution at which the path is rendered, and simple pointer devices typically do not sense the force applied. The rasterization process can further scale or distort the image, so that the rendered image might not reflect the actual proportions and movements of the original execution. Because a static image does not preserve the time-correlated data of the signing act, the velocity, acceleration, pen-up and pen-down sequence, and force variation that characterize the act cannot be measured from it, even where the input process registered the pointer's position over time. Where the image exhibits variation in line width or smoothing of the stroke path, the examiner ordinarily has no means of determining from the image whether that appearance derives from values sensed during the signing act or from a rendering effect introduced by the platform. Apparent variation in line width accordingly cannot be relied upon as a representation of force, even in an implementation where it is in fact derived from sensed values and is not evidence of the signer's actual motor behavior. These limitations can reduce the discrimination information available to the examiner, even when the resulting image does carry handwritten characteristics produced by the signer. As a stored image, the retained signature is also susceptible to reuse and transposition, a susceptibility common to the categories addressed in this section and discussed in 7.8.

7.4 Uploaded or Scanned Signature Images

An uploaded or scanned signature image is created when the image of a signature is provided to the eSigning platform, whether by scanning or photographing a signature from paper or by selecting a stored image file. The retained signature consists of the image file alone. The platform records the act of uploading the image, not the individual who executed the signature.

An uploaded image establishes that the uploader had access to the signature or an image of the signature. It does not establish that the individual who uploaded the image is the individual who executed the signature the image depicts. The act of uploading the image and the act of executing the signature are separate events, and the retained signature does not in any way establish that the same individual performed both. This category is accordingly a boundary case within this section; the image can preserve biometric data of the signer, but the signing act was neither performed within nor captured by the signing session the platform observed, and the provenance parameter set out in 7.2 is at its weakest for images of this kind.

Where the image depicts a genuine handwritten signature, it carries handwritten characteristics that can be compared against known exemplars, but the forensic value of those characteristics is constrained along the parameters set out in 7.2. The platform captures no part of the signing act; the information is confined to the static form preserved in the source image at its resolution, subject to any loss or distortion introduced in scanning, photographing, compression, or file conversion. The image does not record the dynamic data of the original act; rather, these features can be inferred only from the static form, and only to the extent that the image adequately reproduces them. Because the retained signature is a finished image decoupled from any signing event the platform observed, the susceptibility to reuse and transposition described above is intrinsic to this category, and is addressed further in 7.8. Where a printed copy of the document is examined without the platform's audit trail or other visible identifiers of the eSigning platform or process, an uploaded signature image can be indistinguishable from, and can be mistakenly interpreted as, a cut-and-paste signature.

7.5 Digitally Captured Signatures

A digitally captured signature (DCS) is created when the signer executes a signature on a device capable of recording the signing act as time-sequenced biometric data, such as a signature pad, a pen-enabled display, or a touchscreen operated with a stylus. The retained signature consists of the most comprehensive type of captured biometric data, which represents the spatial path of the signature together with its temporal characteristics and, on a device equipped to sense it, the force applied.

Among the categories addressed in this section, a digitally captured signature affords the highest fidelity of motor behavior capture. The device records the spatial path at high resolution together with the temporal characteristics of the act, so the captured data preserve the pen-up and pen-down sequence, and the values from which velocity and acceleration can be derived, together with, where the device senses force, the variation in force that characterizes the signing act.

The quantity and quality of the captured information can vary substantially among implementations depending on the sampling rate, coordinate resolution, force sensitivity, and software processing applied during and after capture. Accordingly, two DCS implementations cannot be presumed to possess equivalent forensic value solely because both capture dynamic data [18].

Whether these dynamic data are available to the examiner depends on the device, platform, and implementation. Some implementations retain the full captured data; others render the captured signature to a static image and retain only its static form, in which case the dynamic data are no longer available for examination, as noted in 7.2, and some store the captured data in an encrypted form that requires cooperation of the platform or vendor to access the data before it can be properly examined.

Where the signer executes the signature with a pen or stylus on a writing surface, the act more closely approximates signing on paper than does input through a mouse or touchpad. An MDAS is correspondingly less likely, and the signer is ordinarily able to produce a signature consistent with the natural range of variation in the signer's habitual handwriting. The captured data are also less susceptible to reuse and transposition than a static image, because a dynamic record is more difficult to decouple from its signing event and reapply convincingly, and the exact reuse of a captured record across documents is more readily detected. The susceptibility common to retained signatures in 7.8 is nonetheless not eliminated.

Procedures for the forensic examination and comparison of DCS, including terminology, equipment considerations, and the division of tasks between the forensic handwriting examiner and digital forensic specialists, are set out in the ENFSI *Best Practice Manual for the Forensic Handwriting Examination* and its Appendix 6 addressing DCS [17], and recommendations for capturing signature data in a manner suitable for forensic examination have been published [19].

The empirical validation base for the examination of dynamic signature data is comparatively recent and less extensive than that for conventional static signature comparison. Like any digital record, captured dynamic data can, in principle, be altered or fabricated, and techniques for synthesizing data continue to develop. The evidentiary weight of dynamic data therefore also depends on the integrity of the chain by which the data were captured, stored, and produced for examination, including whether the data have remained in their native format throughout. Conversion between file formats, platform migration, software updates, rendering processes,

encryption, compression, and other transformations can alter or omit information relevant to the examination.

Native dynamic data can also be discarded following execution, might not remain available indefinitely, or can be omitted from the records routinely provided to the parties to the transaction. The availability of dynamic data for examination can therefore depend on the timely preservation of native platform records.

The method by which a signature was originally captured is accordingly distinct from the information ultimately available for examination. The forensic reliability of an implementation depends on the information available rather than on the theoretical capabilities of the original capture technology; a signature originally captured as dynamic data but preserved only as a static rendering bears the characteristics of the retained static rendering rather than those of the original signing process.

7.6 Non-Handwritten Biometric Data Retained as Signatures

A signature in this category is created when the signing process captures a biometric presentation of a modality other than handwriting, such as a fingerprint or a facial image or video, and the implementation retains the captured sample itself as the signature. As throughout this section, the defining condition is preservation: the captured biometric data are preserved in a form available for examination, rather than consumed at the moment of capture or reduced to a recorded match result.

This preservation condition distinguishes the category from two configurations addressed elsewhere in this report. Where a biometric presentation activates a signing credential and no record of the presentation is preserved, as described in Section 6, the signature contains no biometric data to examine. Where a biometric sample is captured for identity verification and only the result of the matching process is retained, the record is an assertion of the kind addressed in Section 8. In each of those configurations, biometric data were captured but not preserved; in this category, the preserved data constitute the retained signature.

A preserved biometric sample bears characteristics particular to the person who produced it and accordingly provides the direct basis for comparison described in Section 5. The record is direct comparative evidence from which authorship of the captured act can be assessed. Its examination and comparison fall to the discipline competent to assess the modality at issue, such as friction ridge examination or facial identification, rather than to forensic document examination, and are outside the scope of this report.

The parameters set out in 7.2 apply to this category to the extent that they address the preservation and provenance of the captured record rather than the motor behavior of handwriting. The fidelity and completeness of capture, the retention of the captured data in its native form, the provenance of the act, and the susceptibility of the stored record to reuse and transposition bear on the reliability of the preserved data in the same manner as for the categories addressed above. The parameters specific to the handwritten signing act, including susceptibility to a media-dependent alternate style and the production of a signature consistent with the natural range of variation in the signer's handwriting, are modality-specific and do not translate to this category.

As with other categories addressed in this section, a determination of the authorship of the captured act is distinct from a determination that the act was performed in connection with the

document at issue. A preserved facial capture attributes presence at the captured event, and a stored biometric record can, like any retained signature, be decoupled from the session in which it was captured and applied to another transaction. The considerations addressed in 7.8 apply to this category accordingly.

7.7 Hybrid Implementations

A hybrid implementation combines elements of the categories addressed in Section 7 with cryptographic mechanisms of the type described in Section 6. A common configuration captures a DCS and cryptographically binds the captured data to a hash of the document content. Such an implementation remains amenable to forensic examination under the principles described in 7.5.

The reliability of a hybrid implementation for authorship determination is governed by the captured-act component. As described in Section 6, the cryptographic component addresses whether a particular key or credential was used and can associate the credential with its holder but does not directly answer the authorship question.

7.8 Reuse of Retained Signatures

A retained signature that preserves biometric data, including a drawn signature retained as a static image, an uploaded image, a DCS, a preserved non-handwritten biometric record, or the captured-act component of a hybrid implementation, can be stored on a device or within a platform and applied across multiple signing sessions. Some platforms retain a signer's captured signature and reapply it to subsequent documents as a convenience feature, rather than capturing a new act for each signing. Some implementations likewise capture a single signing act and render the resulting signature at multiple signature locations within the same document, such as at each signature and initial block, so that identical signatures within one document can reflect a single captured act rather than a separate act at each location.

The retained signature itself might not indicate whether it was captured during the signing of the document in question or on a prior occasion. An examiner can assess whether the retained signature is consistent with the signer's signature and can detect reuse where the same signature appears identically across multiple documents or at multiple locations within a single document, but in most cases cannot determine from a single instance when it was captured. This limitation applies to every category addressed in this section and bears on the weight assigned to the association between the signature and the specific signing event. Where identical signatures within a single document derive from one captured act, they carry the evidential value of that single act; unlike multiple independently executed signatures, they exhibit no natural variation among instances and do not constitute repeated exemplars of the signer's behavior.

For this reason, a determination that a retained signature was authored by a particular individual is not, standing alone, a determination that the individual executed or adopted the document with which it is associated. Authorship attaches to the signing act that produced the retained signature; where that act can have occurred on a prior occasion, the retained signature establishes who performed the act, not who applied its product to the document at issue. A retained signature that genuinely preserves the signer's biometric data can be applied to a document by the signer, or by any person or process with access to it, without the signer's participation in or knowledge of the transaction. The association between a genuine retained signature and the execution of the document with which it is associated is accordingly a distinct question from its authorship, and one that the retained signature alone can be unable to answer. Where transaction records or other

information beyond the retained signature demonstrate that it existed prior to the execution of the document at issue, the retained signature is thereby established as the record of an act performed on a prior occasion. In that circumstance, a determination of its authorship, however reliable, does not associate the signer with the execution of the document, and the comparison of its biometric data against known exemplars, whatever its outcome, does not answer the question of who applied the retained signature to that document. Whether the signer directed or authorized the application of the retained signature to the document is a distinct question that cannot be resolved from the retained signature alone.

The ability of an examiner to evaluate whether a retained signature was created during the execution of the document at issue, rather than during a prior signing session and subsequently reused, can depend on the availability of transaction records, platform logs, account records, audit trail information, or other information beyond the retained signature itself.

The inability to determine, from a single retained signature alone, whether the signature was executed contemporaneously with the document at issue is not evidence that it was reused. Rather, it reflects a limitation of the available evidence. Likewise, the appearance of identical signatures at multiple locations within a single document is not, without more, evidence of fabrication or transposition, as it can reflect the platform's replication of a single captured act.

8 Signing Session Data in eSignature Platforms

8.1 General

Sections 6 and 7 address the retained signature, including any biometric data it preserves, and its value for a determination of authorship. In addition to the retained signature, an eSigning platform typically generates data describing the circumstances of the signing transaction. Such signing session data, recorded by the platform, are commonly relied upon to describe the circumstances of the session rather than the identity of the signer. They include the network and device used to access the platform, the results of any identity-verification steps, and the logged sequence of events in the transaction. This section describes the principal categories of signing session data and the limits on what they establish about the identity of the signer.

8.2 Principal Categories of Signing Session Data

Signing session data generated during an eSigning transaction are commonly offered as evidence of the signer's identity. The principal categories can include:

a) Internet Protocol (IP) addresses associated with the signing session;

b) device profiles, including operating system, browser, and device fingerprint information;

c) account authentication records, including credential-based logins to the eSigning platform;

d) responses to knowledge-based authentication (KBA) questions drawn from public-record databases;

e) email and Short Message Service (SMS) verification records, including delivery and access timestamps;

f) government-issued identification verification results, including driver's license or passport image capture and matching;

g) biometric capture and matching results, including comparison of a captured facial image to the photograph on a presented identification document;

h) liveness detection results from biometric capture, indicating that a person was physically present at the time of capture;

i) geolocation data derived from IP addresses, device sensors, or both; and

j) audit trail entries documenting the sequence of events in a signing session.

These data are commonly summarized in an audit trail or similar document produced by the eSigning platform.

The categories listed above are those that commonly appear in the records of a signing transaction. They are not the full extent of the data that a platform and its identity-verification and fraud-prevention vendors can bring to bear on a transaction. Vendors publicly describe risk models drawing on thousands of features [33]. These include device intelligence, behavioral analytics, the tenure and risk history of telephone numbers, email addresses, and physical addresses, transaction velocity, and consortium data accumulated across many transactions, customers, and vendors. These data can legitimately inform a platform's decision to permit a transaction, to require additional verification, or to refuse it. In risk-based workflows, a vendor's risk assessment commonly determines which verification method is applied to the signer, and the transaction record reflects the method applied and its outcome rather than the inputs to the assessment [34,35].

8.3 Limitations of Signing Session Data as Evidence of Signer Identity

Each category of signing session data listed in 8.2 describes an aspect of the signing transaction or its technical environment rather than the natural person performing the signing act. Limitations of each are as follows:

a) IP addresses designate a network endpoint, not a person; an address can be shared among multiple users, masked by virtual private network (VPN) services, or spoofed;

b) device profiles describe a hardware and software configuration that is likely not unique and can be shared, reproduced, or virtualized;

c) account authentication records establish that valid credentials were presented to the platform; credentials can be shared, compromised, stored on a device accessible to others, or used by a person other than the credential holder, a decoupling of the credential from the natural person who holds it;

d) KBA responses identify the answer to a question, not the person who provided the response; current federal digital identity guidelines prohibit the use of knowledge-based verification for identity verification [23];

e) email and SMS verification records identify access to a communication channel, which can be delegated, intercepted, or compromised;

f) government identification verification results identify that an image of a document was presented and validated, not that the person presenting the document is the document's subject;

g) biometric matching results report that two biometric samples satisfy the platform's matching criteria, not that either sample necessarily belongs to the document subject, and are subject to the algorithm's false-positive and false-negative rates;

h) liveness detection results identify that a presentation passed the platform's liveness checks, not that the person presenting is the document subject, and are subject to defeat by presentation attacks;

i) Geolocation data identify the inferred location of a network endpoint or device, not the location of the natural person operating it; and

j) audit trail entries record the platform's account of the sequence of signing events, and their accuracy depends on the reliability of the processes that generated them (8.3).

The shared, dynamic, and maskable nature of these network, device, and credential identifiers, and the limits of knowledge-based, channel-based, document-based, and biometric verification, are documented in networking standards, the security research literature, the applicable digital-identity and biometric standards, including those addressing biometric error rates and presentation-attack detection, and the peer-reviewed literature [20,21,22,23,24,25,26].

The breadth of the data available to a platform does not extend to the record available for examination. Risk scores, reason codes, model features, and consortium data are typically retained by the vendor and are not part of the transaction records delivered to the parties to an eSigned document, and current federal digital identity guidelines direct that fraud checks be implemented so that unsuccessful applicants cannot infer the accuracy of the information they submitted [23]. Data that are not presented, disclosed, and preserved within the transaction record, or produced from the platform or vendor with documentation sufficient for independent evaluation, cannot be examined or tested and cannot support a determination of authorship. The disclosed records are evaluated on their own content, without inference from data that were not disclosed.

Several characteristics shared by identity verification technologies further constrain their value as evidence of identity. Commercial platforms rely on proprietary algorithms whose error rates are not consistently reported, and reported figures typically reflect controlled testing on benchmark datasets of authentic samples rather than the conditions of an adversarial signing event. The rate at which a platform fails to detect a counterfeit identification document is rarely reported; biometric matching error rates are typically measured on enrolled, cooperative subjects rather than on inputs containing presentation attacks [25]; and liveness detection systems have documented vulnerabilities whose failure rates against a given attack method are generally not known to parties relying on the result. Even where a presentation-attack-detection threshold is specified, the permitted tolerance is non-trivial; current federal digital identity guidelines set the threshold for remote biometric identity proofing at an impostor attack presentation accept rate (IAPAR) below 0.07, conformant to ISO/IEC 30107-3 [23,26], permitting a conformant system to accept approximately seven percent of impostor presentations under controlled testing conditions.

The availability of signing session data for later evaluation is subject to decay. Disputes concerning document authenticity frequently arise years after execution, by which time transaction records

might not have been retained, and the devices, accounts, and infrastructure to which they refer might no longer exist or be available for examination. Suitable known exemplars of a signer's signature, by contrast, might be obtainable after the fact. The two forms of evidence accordingly differ in temporal persistence, and the weight available from the signing session data can diminish with time in a way that the comparison of preserved biometric data against known exemplars does not. Identity-verification evidence retained by a platform can depend on account configuration, including whether its storage was enabled, and on the platform's retention and deletion practices [36]; its availability for later examination can therefore depend on a timely and specific preservation request.

These limitations do not render signing session data devoid of evidentiary value; rather, they affect the weight that can be assigned to such information and the strength of the inference regarding identity that it supports. Signing session data are, in this respect, circumstantial evidence of identity. Signing session data record the circumstances associated with the signing event but do not inherently always preserve characteristics of the individual who performed the signing act. An inference of identity from such data therefore requires one or more further inferences connecting the recorded account, device, credential, location, or other circumstance to that individual, and its strength depends on the extent to which other persons with access to those means can be excluded. Signing session data can corroborate or contradict a determination of authorship reached by other means and, where independent evidence establishes the connecting links, provide substantial support for an inference regarding the identity of the signer.

Preserved biometric data are, by contrast, different in kind. Because they record characteristics produced by the individual in the course of the act of signing itself, they bear directly on authorship and permit comparison with known exemplars attributed to the purported signer. They thus provide direct comparative evidence from which the identity of the person who performed the signing act can itself be assessed.

The two forms of evidence are complementary rather than interchangeable. Their relative weight in a particular matter is not fixed by category. Where an implementation preserves no biometric data, or where examination determines that the data it preserves are of insufficient complexity to distinguish the signer from other possible authors (Section 5), the signing session data associated with the transaction can provide stronger evidence of the identity of the signer than the retained signature itself. That circumstance does not change the evidentiary character of either: session data bear on identity through the circumstances that must be connected to the signer, whereas preserved biometric data bear on it through comparison of characteristics produced by the signer. The weight ultimately assigned to each depends on the strength and reliability of the evidence, and sufficiently discriminating biometric data provide the more direct forensic basis for assessing authorship.

Determining whether an item of signing session data is valid and the extent to which it can circumstantially identify a particular individual can require a combined examination by experts with expertise relevant to the data type at issue. None of these records is self-authenticating with respect to the person who performed the signing action. Each is an assertion, generated by the platform or its verification vendors, about the circumstances of the signing session, and the reliability of each such assertion is a matter to be established by evidence independent of the record that asserts it. The presence of authentication measures employed by an eSigning platform is not evidence that the resulting retained signature is itself capable of supporting a determination of authorship. That no single record is sufficient on its own is consistent with the guidance of the eSigning and identity-verification industry, which advises that the strength and number of

authentication methods applied to a transaction increase with the risk and value of the transaction, rather than reliance on any one method [11,12,13,14]. Signing session data are appropriately weighed cumulatively rather than in isolation. Multiple independent records can strengthen an inference regarding the circumstances of the signing session, but their combination does not transform circumstantial evidence into direct evidence of the identity of the individual who performed the signing act.

8.4 Evidentiary Admissibility Considerations

Where signing session data are offered for identification purposes, the proponent of the technology bears the burden of establishing the reliability of the underlying technology as an identifier under the applicable admissibility standard [27]. The considerations relevant to such a showing include, among others, the known or potential error rate of the technology, the existence and maintenance of standards governing its operation, whether the technology has been tested under conditions analogous to those of the deployment in question, whether the technology has been subject to peer review and publication, and the degree of acceptance within the relevant technical community. Where vendor risk or identity outputs are relied upon, the showing also includes production of the scores, reason codes, configuration, and retention status relied upon, together with the vendor's documented procedures and performance data [23]. In a comparable context, a court held that a party challenging the output of proprietary forensic software was entitled, on a showing of particularized need, to the software's source code and related documentation under a protective order [37].

These considerations are neither novel nor untested. The limitation of network identifiers has been recognized in similar legal contexts. In Cobbler Nevada, LLC v. Gonzales [28], the court observed that because multiple devices and individuals can connect through a single IP address, identifying the subscriber associated with that address "solves only part of the puzzle" as to who performed a given act. For other identifiers, the reliability showing is complicated by the absence of error rates measured under conditions analogous to the deployment. Reported error rates for biometric matching and liveness detection are commonly derived from controlled benchmark datasets that do not represent the uncontrolled conditions of a remote signing session, and operational error rates for the specific systems deployed by eSigning platforms are generally not publicly reported. Where a known or potential error rate cannot be established under analogous conditions, that absence bears on the admissibility showing rather than excusing it. These are to be tested under the applicable admissibility standard rather than presumed.

Legal frameworks governing attribution reach the same point. Under the Uniform Electronic Transactions Act, an electronic signature is attributable to a person if it was the act of that person, and that act can be shown in any manner, including by a showing of the efficacy of the security procedure applied [2]. The efficacy of a security procedure is accordingly a matter to be shown by the party relying on it, not presumed from the procedure's use.

An audit trail, when produced by an eSigning platform, summarizes a subset of the signing session data described in 8.2 in a single document. The audit trail aggregates platform records but does not, in itself, alter the identification characteristics of the underlying data, nor does it discharge the proponent's reliability burden. A platform-generated record of this kind can be admissible as a business record, but its admissibility does not establish the identity of the signer; rather, consistent with the treatment of computer-generated business records, inaccuracies in such records bear on the weight assigned to them rather than on their admissibility [29,30]. Procedures that render a platform-generated record self-authenticating for the purposes of admission authenticate the

record as the platform's record; they do not establish the truth of the identifications asserted within it. An audit trail is in this respect a collection of assertions, and its evidentiary value depends on the reliability of the processes that generated each assertion it contains. The audit trail is accordingly an investigative starting point rather than an endpoint: it identifies the assertions available for validation and the data sources from which that validation can proceed.

9 Document Integrity as a Distinct Question

Sections 5 through 8 address whether a signing act can be attributed to a particular individual. A separate pair of questions attaches to the digital document itself: whether the document has been altered after signing, and whether the binding between the eSignature and the document contents remains intact. These are questions of document integrity. They are distinct from the question of authorship, and neither answers the other. A determination that a retained signature was authored by a particular individual does not establish that the document associated with it is unaltered, and a determination that the binding between an eSignature and the document contents remains intact does not establish who performed the signing act, as described in Section 6.

Questions of document integrity are answered through digital forensics, file-format analysis, and cryptographic validation rather than through the examination and comparison of signature characteristics. Nothing in the examination of a retained signature, including the examination of dynamic data, addresses whether the contents of the document were modified after the signing act occurred. A matter presenting both questions can require a combined examination by specialists in the respective disciplines, consistent with the division of expertise described in 8.3.

An indication by a document viewer, eSigning platform, or validation service that a signature is valid and the document unmodified is an assertion generated by the software that renders it. The research literature has documented classes of manipulation in which validation software reported signatures as valid over documents whose displayed contents had been altered or replaced [31,32].

The integrity of a signed digital document is, like the identity of a signer, a property to be established by qualified analysis rather than presumed from a platform or viewer indication. The methods, tools, and standards governing such analysis fall outside the scope of this technical report.

10 Summary

Electronic signatures of equal legal validity are not, for that reason, equal in forensic reliability. The technology-neutral frameworks that govern most eSignature transactions accept a broad range of signing acts as legally sufficient, and that acceptance is a default rather than a statement that the resulting signatures are alike in substance. These two properties are distinct, and the legal validity of an eSignature establishes nothing about whether its authorship can be determined.

The direct basis for a determination of authorship is biometric data of the signer preserved by the eSignature implementation. Where none are preserved, attribution, where it can be made, rests on circumstantial evidence outside the retained signature. Signing session data describe the signing transaction or its technical environment rather than the natural person performing the signing act, and bear on authorship only through a further connection, which the data do not themselves establish, between that transaction or environment and the person who performed the act. The limitations of each category are set out in Section 8.2. Implementations that preserve no biometric data, including click-to-sign records, typed names, font-rendered and procedurally generated signatures, record a choice without recording who actually made it, and support no authorship

785 determination on the basis of the retained signature alone regardless of their legal effect. A
786 cryptographic digital signature is unique to a key rather than to a person; it answers whether a
787 particular credential was used, but not who used it.

788 Among implementations that do preserve biometric data, reliability varies along the parameters set
789 out in 7.2: the fidelity of capture, the preservation of dynamic data, the provenance of the act, the
790 susceptibility of the retained signature to reuse, the influence of the input medium, and the extent
791 to which the signing process permits the signer's natural range of variation. A digitally captured
792 signature whose dynamic data are retained and are available occupies one end of the range; a static
793 image detached from any signing event the platform observed occupies the other. What places an
794 implementation at the reliable end of this range is the preservation of the biometric signal of the
795 signing act in a form susceptible to examination. Dynamic data are the most complete preservation
796 of that signal among the categories this report addresses, not a claim that handwriting occupies a
797 privileged position among biometric modalities; the same measure applies to any biometric data
798 retained as the signature, subject to examination by the discipline competent to assess it. An
799 implementation that consumes a biometric presentation without preserving it produces an
800 assertion that a match occurred, not evidence from which attribution can be assessed.

801 Signing session data generated by eSigning platforms describe the circumstances of a signing
802 session rather than the identity of the signer. They are circumstantial evidence that can corroborate
803 or contradict a determination of authorship reached by other means and, where the connecting
804 links are independently established, can substantially support an inference regarding the identity of
805 the signer, but no such record is self-authenticating with respect to the person who performed the
806 signing act. An eSignature and the audit trail that accompanies it are assertions that a particular
807 individual executed a particular signing act. Neither the retained signature nor the record is self-
808 authenticating with respect to that individual's identity; the assertion is something to be validated,
809 not presumed. For the retained signature, that validation is forensic examination against known
810 exemplars, which addresses the authorship of the signing act; for the platform's records, it is an
811 independent showing of the reliability of the processes that produced them.

812 The question of whether an electronic signature is legally valid is distinct from the question of
813 whose signature it is. Answering the second question turns not on the legal framework governing
814 the transaction, nor on the authentication and security measures employed by the platform, but on
815 the information the implementation preserves and makes available for examination. Not all
816 eSignatures are equal in what they can establish about the identity of the signer, and no legal
817 framework makes them so.

818

Annex A
(informative)

Bibliography

The following bibliography is not intended to be an all-inclusive list, review, or endorsement of literature on this topic. The goal of the bibliography is to provide publications cited informationally, and publications relevant to the document.

Legal frameworks and legislation (Section 4)

1] Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001–7031 (2000).

2] Uniform Electronic Transactions Act (1999). National Conference of Commissioners on Uniform State Laws.[a]

3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, 2014 O.J. (L 257) 73.[b]

4] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, 2024 O.J. (L 2024/1183).[c]

5] Assemb. B. 1977, 2025–2026 Reg. Sess. (Cal. 2026), ch. 280, 2026 Cal. Stat.[d]

Technology-neutrality and industry compliance materials (Section 4)

6] Electronic Signature and Records Association. (n.d.). *Who we are*.[e]

7] DocuSign, Inc. (n.d.). *Electronic signatures and transactions in the United States* [White paper].[f]

8] OneSpan, Inc. (n.d.). *OneSpan Sign FAQ*.[g]

9] Adobe Inc. (n.d.). *Electronic signature laws & regulations: United States*.[h]

[a] Available from: https://www.uniformlaws.org/committees/community-home?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034
[b] Available from: http://data.europa.eu/eli/reg/2014/910/oj
[c] Available from: http://data.europa.eu/eli/reg/2024/1183/oj
[d] Available from: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB1977
[e] Available from: https://esignrecords.org/who-we-are/
[f] Available from: https://www.docusign.com/sites/default/files/esignatures_and_transactions_in_the_u.s._whitepaper_.pdf (accessed June 17, 2026)
[g] Available from: https://www.onespan.com/products/esignature/faq (accessed June 17, 2026)
[h] Available from: https://helpx.adobe.com/legal/esignatures/regulations/united-states.html (accessed June 17, 2026)

10] Dropbox, Inc. (n.d.). *A look at eSignature laws around the world*.[i]

Risk-based authentication guidance (Sections 5 and 8)

11] DocuSign, Inc. (n.d.). *Customer compliance and DocuSign*.[j]

12] Adobe Inc. (n.d.). *Identity authentication for electronic signatures*.[k]

13] OneSpan. (n.d.). *What is risk-based authentication (RBA)?*[l]

14] Federal Financial Institutions Examination Council. (2021). *Authentication and access to financial institution services and systems*.[m]

Handwriting individuality and forensic examination (Sections 5 and 7)

15] Huber, R. & Headrick, A. (1999). *Handwriting identification: Facts and fundamentals* (1st ed.). CRC Press.

16] Hicklin, R. A., Eisenhart, L., Richetelli, N., Miller, M. D., Belcastro, P., Burkes, T. M., Parks, C. L., Smith, M. A., Buscaglia, J., Peters, E. M., Perlman, R. S., Abonamah, J. V., & Eckenrode, B. A. (2022). Accuracy and reliability of forensic handwriting comparisons. Proceedings of the National Academy of Sciences, 119(32), e2119944119.[n]

17] European Network of Forensic Science Institutes, European Network of Forensic Handwriting Experts (ENFHEX). (2022). Best practice manual for the forensic handwriting examination (ENFSI-BPM-FHX-01, Ed. 04).[o]

18] Kalantzis N, Platt AWG. Digitally captured signatures: A method for the normalization of force through calibration and the use of the zeta function. J Forensic Sci. 2022;67(2):651–668.[p]

19] Heckeroth, J., et al. (2021). Recommendations for capturing signatures digitally to optimize their suitability for forensic handwriting examination. Journal of Forensic Sciences, 66(1).[q]

[i] Available from: https://sign.dropbox.com/blog/electronic-signature-laws-around-the-world-a-look-at-esignature-laws-by-country (accessed June 17, 2026)
[j] Available from: https://www.docusign.com/trust/compliance/customer-compliance (accessed June 17, 2026)
[k] Available from: https://www.adobe.com/acrobat/business/features/signer-identity-authentication.html (accessed June 17, 2026)
[l] Available from: https://www.onespan.com/topics/risk-based-authentication-rba (accessed June 17, 2026)
[m] Available from: https://www.ffiec.gov/sites/default/files/media/press-releases/2021/authentication-and-access-to-financial-institution-services-and-systems.pdf
[n] Available from: https://doi.org/10.1073/pnas.2119944119
[o] Available from: https://enfsi.eu/wp-content/uploads/2023/02/BPM-Handwriting-Ed.-4.pdf
[p] Available from: https://doi.org/10.1111/1556-4029.14927
[q] Available from: https://pubmed.ncbi.nlm.nih.gov/33206397/

Signing session data: networking, device, and credential limits (Section 8.2)

20] Srisuresh, P., & Holdrege, M. (1999). *IP network address translator (NAT) terminology and considerations* (RFC 2663). Internet Engineering Task Force.[r]

21] Perreault, S., Yamagata, I., Miyakawa, S., Nakagawa, A., & Ashida, H. (2013). *Common requirements for carrier-grade NATs (CGNs)* (RFC 6888). Internet Engineering Task Force.[s]

22] Eckersley, P. (2010). How unique is your web browser? In M. J. Atallah & N. J. Hopper (Eds.), *Privacy enhancing technologies* (pp. 1–18). Springer.[t]

Signing session data: identity proofing, biometrics, and presentation attacks (Section 8.2)

23] National Institute of Standards and Technology. (2025). *Digital identity guidelines: Identity proofing and enrollment* (NIST Special Publication 800-63A-4). U.S. Department of Commerce.[u]

24] National Institute of Standards and Technology. (2025). *Digital identity guidelines: Authentication and authenticator management* (NIST Special Publication 800-63B-4). U.S. Department of Commerce.[v]

25] Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face recognition vendor test (FRVT) part 3: Demographic effects* (NIST Interagency Report 8280). National Institute of Standards and Technology.[w]

26] International Organization for Standardization. (2023). *Information technology — Biometric presentation attack detection — Part 3: Testing and reporting* (ISO/IEC 30107-3:2023).[x]

Evidentiary admissibility (Section 8.3)

27] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

28] Cobbler Nevada, LLC v. Gonzales, 901 F.3d 1142 (9th Cir. 2018).

29] United States v. Catabran, 836 F.2d 453 (9th Cir. 1988).

30] United States v. Meienberg, 263 F.3d 1177 (10th Cir. 2001).

Document Integrity (Section 9)

31] Mladenov, V., Mainka, C., Meyer zu Selhausen, K., Grothe, M., & Schwenk, J. (2019). 1 trillion dollar refund: How to break PDF signatures. In *Proceedings of the 2019 ACM SIGSAC*

[r] Available from: https://www.rfc-editor.org/info/rfc2663
[s] Available from: https://www.rfc-editor.org/info/rfc6888
[t] Available from: https://doi.org/10.1007/978-3-642-14527-8_1
[u] Available from: https://doi.org/10.6028/NIST.SP.800-63A-4
[v] Available from: https://doi.org/10.6028/NIST.SP.800-63B-4
[w] Available from: https://doi.org/10.6028/NIST.IR.8280
[x] Available from: https://www.iso.org/standard/79520.html

Conference on Computer and Communications Security (pp. 1–14). Association for Computing Machinery.[y]

32] Mainka, C., Mladenov, V., & Rohlmann, S. (2021). Shadow attacks: Hiding and replacing content in signed PDFs. In *Proceedings of the Network and Distributed System Security Symposium (NDSS) 2021*. Internet Society.[z]

Signing session data: platform risk intelligence (Section 8)

[33] Socure, Inc. (2021, October 25). Socure announces Sigma Identity Fraud—The industry's most accurate identity fraud solution [Press release]. Business Wire.[aa]

[34] Socure, Inc. (2025, October 16). Socure and Docusign bring identity certainty to every signature with a frictionless experience for every signer [Press release].[bb]

[35] Kotch, M. (n.d.). Introducing ID Verification with CLEAR and Risk-Based Verification in Docusign. Docusign.[cc]

[36] Sammons, J. (n.d.). Retrieving ID verification data. Docusign Developers.[dd]

[37] State v. Pickett, 466 N.J. Super. 270, 246 A.3d 279 (App. Div. 2021).

Terms and definitions (Section 3)

[38] ASTM E1732-26. *Standard terminology relating to forensic science*. ASTM International. 2026.[ee]

[39] Organization of Scientific Area Committees for Forensic Science. (n.d.). OSAC lexicon. National Institute of Standards and Technology.[ff]

[y] Available from: https://doi.org/10.1145/3319535.3339812
[z] Available from: https://doi.org/10.14722/ndss.2021.24117
[aa] Available from: https://www.businesswire.com/news/home/20211025005580/en
[bb] Available from: https://www.socure.com/news-and-press/identity-certainty-to-every-signature (Accessed October 29, 2026)
[cc] Available from: https://www.docusign.com/blog/id-verification-with-clear-and-risk-based-verification (Accessed October 29, 2026)
[dd] Available from: https://www.docusign.com/blog/developers/retrieving-id-verification-data (Accessed October 29, 2026)
[ee] Available from: https://store.astm.org/e1732-26.html (Accessed October 29, 2026)
[ff] Available from: https://www.nist.gov/adlp/spo/organization-scientific-area-committees-forensic-science/other-work-products/osac-lexicon (Accessed October 29, 2026)

DRAFT



Academy Standards Board
410 North 21st Street
Colorado Springs, CO 80904

www.aafs.org/academy-standards-board