ABATECHSHOW2016
30 YEARS of LEGAL TECHNOLOGY INNOVATION
Hilton Chicago | Chicago, IL
March 16-19, 2016
www.techshow.com
#ABATECHSHOW

# E-Signatures, Authentication and Contracts

**Written by**
George Bellas, Bellas & Wachowski
Dan Puterbaugh, Adobe Systems

Presenters
George “Geo” Bellas: @GeoBellas
Dan Puterbaugh; @danrex

The ESIGN Act[1], signed by President Clinton on June 30, 2000, granted electronic signatures the same legal status as handwritten signatures throughout the United States. In 1999, the European Union published its electronic signature directive [2]and will transition to its recently passed Electronic Identification and Authentication Services regulation (eIDAS)[3] on July 1, 2016.

Under any legal structure, electronic signatures can greatly simplify the way attorneys and their clients gather, track and manage signatures and approvals. This paper reviews the basic tenets of U.S. and EU electronic signature law and addresses the admissibility of electronic signatures and records in US courts.

**Defining Signature Types**

Since there is still some confusion as to the different types of electronic signatures, it is critical to first understand the distinctions between the different types before reviewing the legal landscape.

*Electronic signatures*

Under nearly all legal frameworks, an electronic signature is any sound, symbol or process logically associated with a record, used by a person with the intent to sign. Like a handwritten signature, an electronic signature shows who signed, the processes used to sign, and the intent in signing. Although it is not required, electronic signatures sometimes include additional authentication methods, auditable signing workflows, or contain additional security designed to prevent tampering with the signed document.

*Digital (or Advanced Electronic) signatures*

A digital signature provides the same information about a signer that an electronic signature provides, but it also includes additional security measures to authenticate the identity of the signer and prevent tampering. A digitally-signed document, like a notarized paper document, provides parties with the assurance that a signer's identity has been authenticated by an objective third party. That third party is called a *certificate authority* (CA).

To get a digital signature, an individual has to authenticate their identity with a CA. This generally requires an in-person meeting during which the requestor provides one or more government-issued IDs to prove his or her identity. The CA authenticates the identifying information, and adds it to a secure database. Finally, the CA issues a token, smart card, or digital certificate that the individual can use to execute digital signatures.

*Qualified Signatures*

[1] 15 U.S.C. §§ 7001-31 (2000)
[2] Directive 1999/93/EC
[3] Regulation (EU) No 910/2014

Finally, there is the qualified signature. A qualified signature is a digital signature that is based on a certificate created by a government-accredited secure-signature-creation device. Qualified signatures are generally only used in the EU.

**The US – ESIGN and UETA**

Fundamentally, the ESIGN act provides that wherever the law requires a signature or record, an electronic signature or record will satisfy that requirement.[4] Stated differently, the ESIGN Act prevents denial of the legal effect, validity or enforceability of an electronically signed document or record solely because it is in electronic form. However, electronic signatures must still meet some essential requirements.

*Intent to sign* - Just as with a handwritten signature, a signer must show clear intention to sign an agreement. Most often, signers show intention by typing their name into a data field, drawing their signature on a touchpad, or clicking a button clearly labeled "I Accept."

*Consent to do business electronically* - ESIGN also requires some form of consent to do business electronically.[5] Under ESIGN this consent can be implied from the signer's actions, but most e-signature solutions have some form of this consent built into the electronic signature workflow. However, some jurisdictions outside of the US prefer explicit consent. As a result, one may want to include additional language making this consent explicit. For example, agreements can be modified to add the following clause above the signature block:

> *The parties agree that this agreement may be electronically signed. The parties agree that the electronic signatures appearing on this agreement are the same as handwritten signatures for the purposes of validity, enforceability and admissibility.*

*Record retention* - The ESIGN act enables electronic records to satisfy the record retention requirements that are imposed under other laws. These electronic records must accurately reflect the information in the document and remain accessible in a form that allows the record to be accurately reproduced for anyone who is entitled to access the document. Often this means providing a fully executed copy to the signer or permitting the signer to download a copy of the agreement.

*Opt-out* - Signers must be given an opportunity to refuse to sign an agreement electronically. The ESIGN act does not *require* that anyone accept electronic signatures. [6]

At the state level, 47 of the 50 states have adopted the Uniform Electronic Transactions Act (UETA). UETA's provisions are substantially similar to the ESIGN provisions. However, each state's adoption of UETA is slightly different. This is particularly important to note because ESIGN explicitly avoids pre-empting state laws on electronic

[4] 15 U.S. Code § 7001(a)
[5] 15 U.S. Code § 7001(c)
[6] 15 U.S. Code § 7001(b)(2)

signatures so long as those state laws do not directly conflict with the ESIGN act. [7] As a result, one should be familiar with the particular form of the adoption of UETA in that state. Some, like California, include substantial deviations from the model law.

**The EU - Directive 1999/93/EC and eIDAS**

In 1999, the European Commission published its first eSignatures Directive.[8] Since it was a directive (rather than a regulation), it allowed the member states of the EU to interpret the new law and impose their own restrictions, limitations and exceptions to it. The result was that electronic signature law in the EU became a patchwork of differing laws. Worse, none of the member states recognized the other member state's e-signature laws as valid. This fragmentation undermined the EU's goals of moving towards a single market.

As a result, on August 28, 2014, the European Commission published the Electronic Identification and Authentication Services regulation (eIDAS) as Regulation 910/2014. This new regulation establishes a new legal structure for electronic signatures, seals and documents throughout the EU and will come into effect on July 1, 2016.

As of that date, the existing EU Directive on electronic signatures will be replaced. Perhaps just as importantly, any laws of EU member states that are inconsistent with eIDAS will also automatically be repealed or replaced. The result will be that for the first time there will be a consistent legal framework and a single market for the recognition of electronic signatures across all of the EU member states.

Substantively, eIDAS is in two parts. The first section deals with government-issued identification and establishes a legal framework that will allow all EU member states to mutually recognize each other's identification systems.[9] This section targets the public sector and requires Member States to permit citizens from other member states to use their own electronic IDs to access online services. Private sector companies are not directly impacted by this portion of eIDAS.

The second section of eIDAS deals with electronic signatures.[10] It clarifies existing rules, but also introduces a new legal framework for electronic signatures and seals.

*Impact of the New Regulation on Electronic Signatures*

As noted above, on July 1, 2016, eIDAS will not only repeal the existing eSignatures Directive, it will also automatically replace any inconsistent national laws in Europe. Let's examine some of the important changes to the status of electronic signatures.

Article 25 of the Regulation maintains the fundamental legal rule that all electronic signatures and verification services shall be admissible as evidence in legal

[7] 15 U.S. Code § 7002
[8] Directive 1999/93/EC
[9] Regulation (EU) No 910/2014; Chapter II; Articles 6-12
[10] Regulation (EU) No 910/2014; Chapter III; Articles 13 et seq.

proceedings. This includes electronic signatures, seals, time stamps, registered delivery services and certificates for website authentication.[11]

eIDAS also includes a definition of the service companies that provide these electronic signatures, seals and stamps - Trust Services[12] It goes further and distinguishes between qualified and non-qualified Trust Services. Although these concepts were in the 1999 Directive, they are addressed in greater detail in the new Regulation. eIDAS provides a clearer definition of Trust Services and the requirements and supervision associated with them apply greater scrutiny to their operation than before. The objective of this scrutiny is to increase confidence in digital transactions and to encourage more people to use them by demonstrating their reliability and security as well as their clear advantages over handwritten signatures.

Electronic Signatures

Basic electronic signatures are unchanged under eIDAS. The fundamental standard - that an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form– is still the rule.[13]

Advanced Electronic Signatures

One key change in the new Regulation is the re-definition of Advanced Electronic Signature (AdES). This signature – as opposed to the basic electronic signature that is in place under the current Directive – allows unique identification and authentication of the signer of a document and enables the verification of the integrity of the signed agreement. Although these certificates have existed for many years, eIDAS enables the signer to use the latest technologies, like mobile devices, to accomplish this.

Qualified Electronic Signatures

The final type of signature available under eIDAS is the Qualified Electronic Signature (QES). While both Advanced and Qualified Electronic Signatures are uniquely linked to the signer, Qualified Electronic Signatures are based on Qualified Certificates. Qualified Certificates can only be issued by a CA which has been accredited and meets the requirements of eIDAS. Qualified Certificates must also be stored on a qualified signature creation device such as a smart card, a USB token, or a cloud based trust service.

QES are doubly important because this type of signature is the only form that is granted legal equivalence to a handwritten signature under eIDAS[14]. Further, only a qualified

[11] Regulation (EU) No 910/2014; Chapter III; Section 4.
[12] Regulation (EU) No 910/2014; Chapter III; Articles 13-28.
[13] Id. Article 25, subsection 1.
[14] Id. Section 2.

electronic signature is required to be mutually recognized across all the EU member states[15].

### Electronic Seals

Finally, eIDAS will introduce the recognition of electronic seals.[16] These are similar to electronic signatures but only available to legal persons such as corporate entities. This raises the interesting prospect of minimizing the importance of the "authorized signer" for a particular entity. Instead, there will simply be a seal that is associated with that entity and any use of that seal will be presumed to be binding on that entity.

## Admissibility for E-signatures: Verifying Signatories, Audit Logs, and Security

The Federal Rules of Evidence ("FRE"), and their state law equivalents, govern the admissibility of evidence, including the admissibility of documents that are presented, signed, secured, archived and retrieved by an electronic signature process. [17] Thus, in addition to meeting the requirements laid out in UETA and the ESIGN Act respectively to validate the signatures, the party seeking the admission of an electronic document into evidence also has the burden of satisfying admissibility requirements.

The standard for the authentication of evidence under the Federal Rules of Evidence is contained in Rule 901, which provides that "the requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."[18] Moreover, as stated throughout the case law regarding the admissibility of computer generated information, "reliability must be the watchword" in determining the admissibility of computer generated evidence. [19] The "factors must effectively address a witness' familiarity with the type of evidence and the method used to create it, and appropriately require that the witness be acquainted with the technology involved in the computer program used to generate the evidence."[20]

Certain Subsections of Rules 901 and 902 are particularly suited to address the admission of electronic signatures and records: 901(b)(1), (3), (4), and (9), and 902(7) and (11). While Rules 901(b)(1), (3), (4), and (9) require witness testimony to authenticate proffered evidence, Rules 902(7) and (11) allow for self-authentication. Magistrate Judge Paul W. Grimm's opinion in *Lorraine v. Markel American Insurance Co*. has become the gold standard for admissibility of electronic evidence, including signatures.[21]

---

[15] Id. Section 3.
[16] Id. Section 5
[17] Many states have adopted rules of evidence which track the FRE. References herein will be limited to the FRE.
[18] Fed. R. Evid. 901(a).
[19] *State v. Swinton*, 268 Conn. 781, 812 (2004).
[20] *Id.* at 813-814.
[21] *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534 (D. Md. 2007).

In *Lorraine*, the plaintiff's yacht was damaged, and as a result, a claim was made to recover insurance proceeds. The plaintiff challenged the amount of an arbitrator's award in plaintiff's favor. However, neither party provided an evidentiary foundation to enable the court to rely on the various emails and other electronic documents that were offered to either validate or contest the amount in question. [22] In a treatise-like opinion that spans over 100 pages, the court provided a thorough analysis addressing the admission of electronic documents into evidence, as well as examples of the essential elements of an effective "e-contracting" process. That process includes authenticating an electronic signature by verifying the identity of the person purporting to sign an electronic document, creating an audit trail for the entire electronic transaction process, and securely archiving and ensuring the retrievability of the electronic document. [23] Finally, as mentioned previously, depending on the type of document sought to be admitted into evidence, the party may be required to proffer testimony from a credible witness qualified to explain all three facets of the e-contracting process in order to authenticate the record bearing the party's signatures. Failure to satisfy the authentication requirements risks an unenforceable electronic document because of a court's refusal to admit the electronic document into evidence.

## Verifying Signatories-Adequate Procedures a Must

Verifying the identity of the parties to an electronic transaction is no doubt complicated by the fact that the parties may not have ever met one another in person. Instead, it may well be the case that they have always interacted remotely by computer or other electronic means. Just like an ink and paper agreement, the failure to verify the identity of a party signing an electronic agreement raises the risk of a forged signature.

Regarding authentication of e-signatures, the UETA provides that the signature is attributable to an individual if it can be shown in any manner to have been the act of that individual, including through the efficacy of a security measure. [24] Further, the UETA broadly defines a security measure as any procedure used to verify an e-signature, record or performance, including procedures that require the use of algorithms or codes, identifying words or numbers, encryption or callback or other acknowledged procedures. [25]

The identity of a signatory of an electronic agreement can be verified in several ways:

- Through use of a trusted sign-on process that involves providing a password, PIN or secured secret code to enable the parties to identify themselves; [26]

---

[22] Id. at 537.
[23] Id. at 542, 573.
[24] Uniform Electronic Transactions Act, (2009), UETA, § 9(a)
[25] *Id*. at § 2 (14).
[26] Bruce S. Nathan and Terrence D. Watson, *Electronic Signatures, Agreements and Documents; The Recipe for Enforceability and Admissibility*, The Credit and Financial Management Review, Volume 21, No. 1 (Second Quarter 2015) [hereinafter Recipe].

- Allowing an independent third party (such as a consumer reporting agency) to conduct an identity verification process based on personal data provided by the contracting parties to such third party; [27]
- Parties could require an answer to a shared secret question. This is typically done in conjunction with sending a link to a trusted email address, and thereafter, limiting access to the documents until the correct answer to the shared question is provided. [28]
- Having signatures notarized is another form of authentication of the identity of the signer. If there are documents required to be notarized, the electronic signature process should allow the notary verifying another signer's signature to enter the notary's signature and other credentials, in accordance with applicable state notary laws. [29]
- Court-admissible signature certificates offer judges and legal professionals a way to view and verify a document's validity data, audit logs, and signatory information – such as full name, signature, IP address, email address, and any other identifying details. Signature certificates are a significant component in authenticating signed documents in court.[30]
- Biometric Authentication identifies people based on intrinsic physical traits such as photograph, iris scan, and fingerprints, voice pattern, or a digitized image of a handwritten signature that is attached to an electronic message.[31]

The identity of the signer is an evidentiary issue, and can be proven in a variety of ways. For example, in *Zulkiewski v. Am. Gen. Life Ins. Co.,* the court found that the insurance company's authentication process, which involved association with an email address, and knowledge of certain personal information (e.g. mother's maiden name) were sufficient to establish the identity of the signer. [32]

Electronic security may also play a role in establishing identity. For example, in *Kerr v. Dillard Store Services*, the court declined to enforce an arbitration agreement purportedly signed by the plaintiff, because the defendant "did not have adequate procedures to maintain the security of intranet passwords, to restrict authorized access to the screen which permitted electronic execution of the arbitration agreement, to determine whether electronic signatures were genuine or to determine who opened

---

[27] Id.
[28] Id.
[29] Gregory T. Casamento, Patrick Hatfield, and Mike Hjorleifsson, *Enhancing the Admissibility and Enforceability of Electronically Signed Documents,* Bloomberg Law Reports-Technology Law, Volume 1, No.11 at p. 8 (Dec. 14, 2009) [hereinafter Enhancing].
[30] *Id.*
[31] Stephen E. Blythe, *Digital Signature Law of the United Nations, European Union, United Kingdom and United Stats: Promotion of Growth in E-Commerce with Enhanced Security,* 11 RICH. J.L. & TECH. 2 (2005), at http://law.richmond.edu/jolt/v11i2/article6.pdf.
[32] Zulkiewski v. Am. Gen. Life Ins. Co., No. 299025, 2012 Mich. App. LEXIS 1086 (Mich. Ct. App. June 12, 2012).

individual emails."[33] Further, the court reasoned that "it is not inconceivable [the secretary] or a supervisor logged on to plaintiff's account and executed the agreement," and thus that the employer had not proven by a preponderance of the evidence that the employee had signed the arbitration agreement. [34]

## Creation of an Audit trail to Preserve the Integrity of an Electronic Record

Next, the implementation of an audit trail that creates a record of all transactions to an electronic document, from steps taken to verify the identity of signatories and every transaction in between sealing a document, is vital to preserving the integrity of an electronic record.

The contents of an audit trail should include:

- the identity of users and how they were authenticated;
- date and time stamp for all transactions;
- identification of the person making any changes to the electronic record;
- the original, unmodified and modified terms to an agreement;
- the reason for the changes to the electronic agreement, record or other electronic document. [35]

The audit trail should record each step required to meet regulatory requirements such as the sequence and timing of presenting certain forms and the actual contents of records presented.[36] The preservation of this data in an audit trail will enable the custodian of the record or any other interested party to follow the history of the electronic transaction, recover any incorrectly updated or deleted data, investigate the cause when an electronic record is found to be incorrect, and correct any incorrect information in the electronic record.[37] By the same token, a "clean" audit trail that confirms the absence of any attempt to improperly access an electrically signed agreement after it has been agreed to by the parties, or any improper modifications to such an electronic agreement, will make it increasing difficult for a contracting party to repudiate the terms of the agreement on the basis that the terms are not the terms that were agreed to at the time of entry of the agreement.[38]

## Securely Archive and Ensure Retrievability of Audit Trail- Circumstances of Preservation and Qualified Witness Testimony the Focus

Lastly, critical in the analysis of admissibility and the overall enforceability of documents executed using a given electronic signature process is the requirement of a secure method to archive and retrieve the documents so they cannot be altered after signature.

---

[33] *Kerr v. Dillard Store Services, Inc*., 2009 WL 385863 (D. Kan. Feb. 17, 2009).
[34] *Id.*
[35] Recipe, *Supra* note 26.
[36] Enhancing, *Supra* note 29 at 10.
[37] Recipe, *Supra* note 26.
[38] *Id.*

In addition to the method or process, there must be a credible person qualified to give testimony to the accuracy of the computer systems in the retention and retrieval of the information at issue.[39]

The Ninth Circuit Bankruptcy Appellate Panel (the equivalent of a United States District Court), addressed both issues in *American Express Travel Related Services, Co. v. Vinhnee*. In that case, American Express sought to block the discharge of the full amount of its claims in the amount of $41,597.63 against a debtor in bankruptcy, which the debtor had scheduled for a lesser amount. American Express produced computer records along with a witness to testify regarding the computer system from which the records derived in order to prove the amount of the claims. Although there was no objection to the admissibility of the computer records, the court, on its own, required American Express to provide the ". . . authentication foundation regarding the computer and software in order to assure the continuing accuracy of the records."[40] The bankruptcy court refused to block the discharge of the full amount of American Express' claims against the debtor because of the court's refusal to admit American Express' computer records into evidence. This resulted from American Express' failure to properly authenticate its computer records supporting the amount of its claims.

On appeal, the Ninth Circuit Bankruptcy Appellate Panel affirmed the bankruptcy court's refusal to block the discharge of the full amount of American Express' claims. The court held that proof that a document being proffered into evidence is an accurate representation of the document as it originally was created is a condition for satisfying the authentication requirement for admissibility.[41] Citing FRE 901(a), the court further noted that "authenticating a paperless electronic record, in principle, poses the same issue as for a paper record, the only difference being the *format* in which the record is maintained: one must demonstrate that the record that has been retrieved from the file, be it paper or electronic, is the same as the record that was originally placed into the file."[42] **Here, the court stated that "the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the *preservation* of the record after its placement in a file, so as to assure that the document being proffered is the same as the document that originally was created."[43]**

Next, turning to the appropriate standard to determine the authenticity of an electronic document, the Ninth Circuit Bankruptcy Appellate Panel adopted an eleven-step foundation for computer records, referred to as the "Imwinkelried foundation." This requires proof of the following:

1. The business uses a computer.

2. The computer is reliable.

---

[39] *In re Vee Vinhnee*, 336 B.R. 437, 448 (B.A.P. 9th Cir. 2005).
[40] *Id.*
[41] Id. at 444.
[42] Id.
[43] Id.

3. The business has developed a procedure for inserting data into the computer.

4. The procedure has built-in safeguards to ensure accuracy and identify errors.

5. The business keeps the computer in a good state of repair.

6. The witness had the computer generate a printout of certain data.

7. The witness used the proper procedures to obtain the printout.

8. The computer was in working order at the time the witness obtained the printout.

9. The witness recognizes the exhibit as the printout.

10. The witness explains how he or she recognizes the printout.

11. If the printout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact. [44]

The court cited to these factors but placed particular emphasis on item no. 4 – *proving that the procedure has built-in safeguards to ensure accuracy and identify errors.* The court noted that this requirement includes the "details regarding computer policy and system control procedures, including control of access to the database, control of access to the program, recording and logging of changes, backup practices, and audit procedures to assure the continuing integrity of the records."[45]

Finally, concerning witness testimony, the *Vinhnee* Court found the testimony of the American Express witness to be vague, conclusory and unpersuasive. Specifically, the court noted that the American Express custodian needed to go beyond "merely identifying the makes and models of the equipment, naming the software, noting that some of the software was customized, and asserting that the hardware and software are standard for the industry, regarded as reliable, and periodically updated. [46] In order to assure continued accuracy of the records, the Court required additional foundational testimony regarding:

• The proponent's policies and procedures for use of the equipment, database and programs;

• How access to the pertinent database is controlled and, separately, how access to the specific program is controlled;

• How changes in the database are logged or recorded;

• The structure and implementation of backup systems; and

• Audit procedures for assuring the continuing integrity of the database.[47]

---

[44] Id. at 446.
[45] Id. at 446-447.
[46] Id. at 448
[47] Id. at 449.

## Conclusion

16 years after the passage of the ESIGN Act, some still see electronic signatures and records as somehow new. However, despite this perception, the legislation and case law surrounding their use in commerce and their admissibility in litigation is clear. Coming changes in the EU will only add to this clarity.