

eIDAS AND
E-SIGNATURE
A LEGAL
PERSPECTIVE:
ELECTRONIC
SIGNATURES IN THE
EUROPEAN UNION

WHITE PAPER

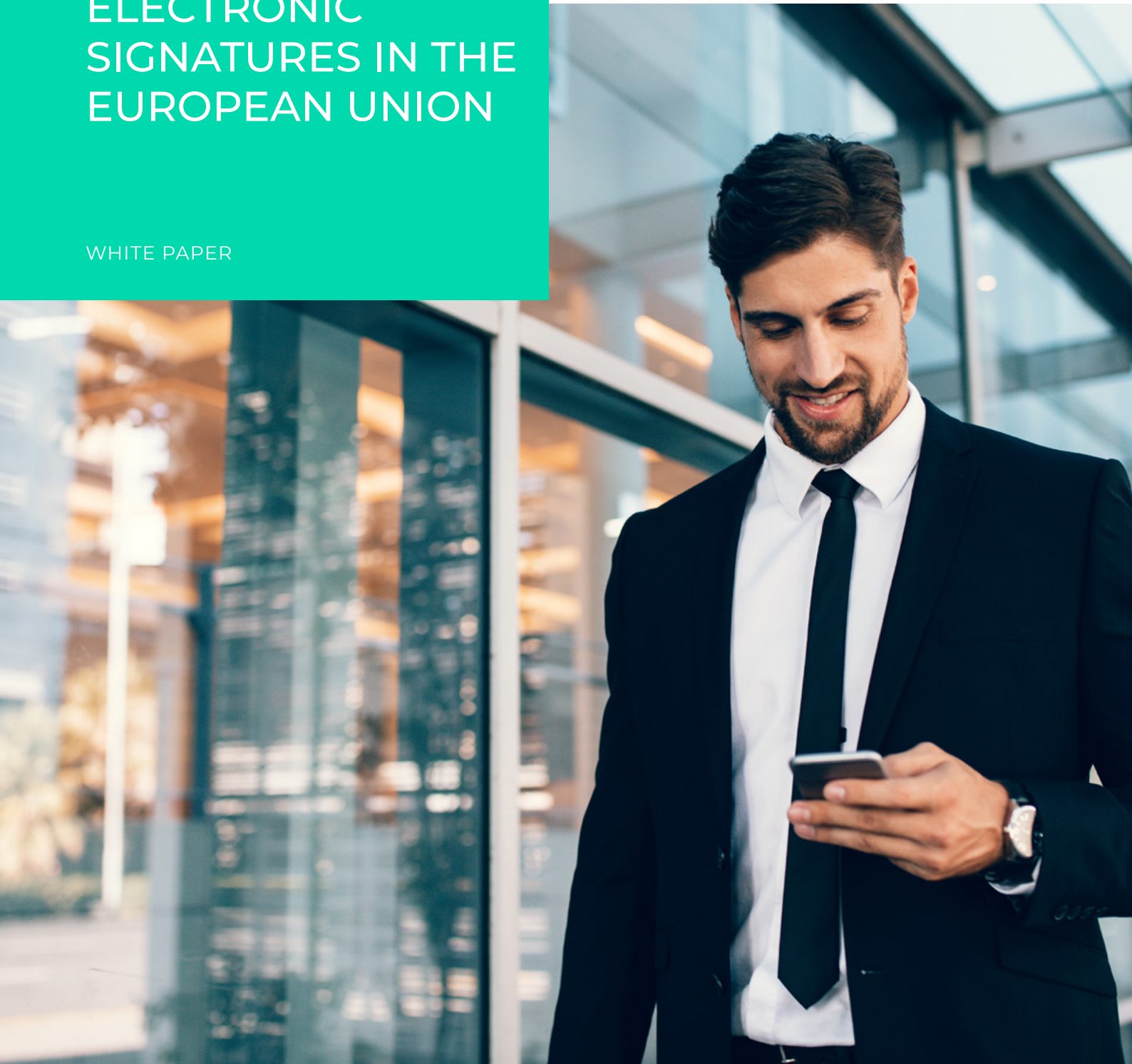


TABLE OF CONTENTS

Part 1: Introduction	3
Key Highlights of the eIDAS Regulation	4
Legal Effect of Different Types of Signatures	6
Regulation of Trust Services	7
Legal Best Practices	8
Part 2: Compliance With the Regulation	9
Advanced Electronic Signatures	9
Qualified Electronic Signatures	10
Format Standards	12
Additional Evidence	12
Conclusion	13
E-Signature Solution Checklist	14

About the Authors

This paper is a collaboration between Lorna Brazell of Osborne Clarke LLP and OneSpan. In part one, Osborne Clarke provides a legal opinion on the legal validity of electronic signature in the European Union. Part two has been prepared by OneSpan, and summarizes best practices recommendations for legal compliance when implementing e-signatures.



PART 1

Introduction

The 2014 Regulation on Electronic Identification and Trust Services for Electronic Transaction in the Internal Market¹ (“eIDAS”) went into effect throughout the European Union (“EU”) on 1 July 2016, replacing the 1999 Directive on electronic signatures² (“the Directive”). Although the Directive had not been the subject of any disputes in its 16-year history, neither had it been a success. Its objective, to enable the widespread use of electronic signatures to conduct business across borders within the EU, was not met.

There Are Three Key Reasons for This:

- I. Most EU Member States’ laws do not specify any form of signature for commercial contracts other than guarantees or contracts assigning real property.
- II. Many people mistakenly believed that the Directive mandated the use of advanced electronic signatures supported by a qualified certificate³ in order for an electronic signature to be legally effective. In fact, the Directive says the opposite. Courts may accept any form of electronic signature as having legal effect. However, in the case of a qualified electronic signature, the court has no choice but to accept it. That said, the cost and administrative burden of implementing the technology required for qualified electronic signatures has outweighed the potential benefits of being able to use them.
- III. There was a divergence between Member States as to the regulatory regime with which signature or certification providers should comply. As a result, signatures produced using certification services approved in one Member State risked not being recognized as compliant in another.

Since the Directive’s mechanisms have been so little used, it is not surprising that there is no European case law to give guidance on how it should be interpreted.

The flaws in the Directive have not held up the development of cross-border commerce in the EU. In 2015, the Court of Justice of the European Union (“CJEU”) ruled that the terms of a B2B ‘click-wrap’ agreement may be legally binding even if the clicker/signer has not read the terms of the agreement. In that case *El Madjoub*, a car dealer, sought to enforce an online contract for purchase of a used car, through proceedings in his local German court. He was defeated, because he had clicked to indicate his acceptance of unread terms. Those terms turned out to include submission to the jurisdiction of the Belgian courts. The CJEU held that he was bound by those terms despite not having read them, because he had had the opportunity to read them and clicked his agreement to them. Accordingly, the simplest form of electronic signature imaginable – using a cursor to click a button – can have legal effect, and most B2B or B2C transactions can be completed without handwriting-equivalent signatures, provided that there is satisfactory evidence, in whatever form, to prove that each party had agreed to be bound.

Nevertheless, the European Commission concluded that the lack of harmonization between Member States still represented a potential barrier to the internal market. Accordingly, by introducing the eIDAS Regulation and leaving Member States no latitude for implementation or interpretation, they hope to ensure that documents signed electronically will now be accepted throughout all 28 Member States of the EU, regardless of national, legal, or regulatory approaches.



Under eIDAS, any of the three categories of e-signature can be legally effective; the difference between them is only what evidence it will take to reassure a court that the signature is genuine and intentionally applied to the particular document.



Key Highlights of the eIDAS Regulation

eIDAS is much broader in scope than the Directive, since in addition to signatures, it also encompasses electronic identification, delivery, archive services, and website authentication.

Signatures

eIDAS defines the same three categories of e-signatures as did the Directive. There are:

- Electronic signatures
- Advanced electronic signatures (“AES”)
- Qualified electronic signatures (“QES”)

The approach to all three is explicitly technology-neutral. The Regulation does not stipulate that any specific technology must be used, only the criteria that a signature must meet. However, the requirements for qualified certificates suggest only digital certificate technology is most suitable.

Under eIDAS, an electronic signature includes any data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signer to sign. Furthermore, an electronic signature cannot be denied admissibility in evidence or legal effect merely on the grounds that it is in electronic form or does not meet the requirements for qualified electronic signatures.

Accordingly, for a large range of use cases, such as the online car purchase agreement in the CJEU decision above, electronic signatures which are neither advanced nor qualified can be legally effective, provided that available evidence establishes:

1. That they are attached to or logically associated with the signed document
2. That the signer intended to use the electronic signature to sign – that is, identify him or herself and indicate acceptance, approval, or merely notice of the contents of the document

It follows that AES are also capable of legal effectiveness as signatures, since by definition an AES captures much of the necessary evidence. An AES must be:

1. Uniquely linked to the signer
2. Capable of identifying him or her
3. Created using electronic signature creation data that the signer can, with a high level of confidence, use under his or her sole control
4. Linked to the signed data in such a way that any subsequent change in the data is detectable

This is not to say that evidential questions cannot be answered by other means. For example, if a name is typed at the end of a document and saved on a computer kept in a business environment, circumstantial evidence as to the people who had access to that computer may be sufficient to establish that the person who typed the name was indeed the person named. But an AES requires technology which would not be available to a passing co-worker who mischievously attempted to sign in a colleague’s name, and so reduces the prospect of such a challenge being mounted, let alone successful. (The definition does not attempt to circumscribe what technology that might be.)




QES are based on AES which must meet these additional requirements:

1. Be created using a QES creation device
2. Be supported by a qualified certificate

QES creation devices are largely the same as secure signature creation devices under the Directive, with an added requirement that the confidentiality of the electronic signature creation data is reasonably assured. Similarly, the definition of qualified certificate is largely in keeping with the equivalent definition in the Directive.

The provision of both eIDAS and the Directive that qualified electronic signatures must be recognized as legally equivalent to handwritten signatures, without recourse to additional evidence, can now be seen as simply a confirmation that the evidence captured by an advanced electronic signature, with the addition of some form of identity verification and appropriate cybersecurity, must be accepted as sufficient evidence. This does not imply, however, that QES cannot be challenged, just as handwritten signatures can be if evidence demonstrates that the creation device had been purloined, or some kind of fraud used to deceive the signer into signing a document.

Notably, recital 51 to eIDAS expressly states that a signer should be able to entrust QES creation devices to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure the signer has sole control over the use of the data. In other words, signature authority can be delegated as long as suitable organizational checks and balances are in place. Recital 52 acknowledges the possibility of remote electronic signature provision (such as cloud-based services), subject to suitable management and administrative security procedures, trustworthy systems, and products, to guarantee that the signer has sole control.

eIDAS REQUIREMENTS		
Electronic Signatures	<p>The electronic signature must be:</p> <ul style="list-style-type: none"> • Applied by the person associated with the signature • Applied in a manner that demonstrates the intent of the signer • Associated with the document or data the signer intended to sign 	 Additional supporting evidence required
Advanced Electronic Signatures (AES)	<p>This form of e-signature adds four additional requirements. The advanced electronic signature must:</p> <ul style="list-style-type: none"> • Be uniquely linked to the signer • Identify the signer • Be under sole control of the signer • Detect changes to the document or data after the application of the AES 	 No additional supporting evidence required
Qualified Electronic Signatures (QES)	<p>This is an advanced electronic signature that, in addition, must be:</p> <ul style="list-style-type: none"> • Created using a QES creation device • Supported by a qualified certificate (that is issued to the signer in a form he or she can keep under his or her control) 	

Electronic Identities

eIDAS addresses questions of electronic identities (eIDs), but it does so only in the limited context of eIDs used for citizens' interactions with public administration, such as accessing healthcare or paying taxes. No system of eIDs is mandated, since not all Member States have any form of national ID card in place. Rather, for those Member States that wish to have their eIDs recognized across borders, eIDAS seeks to ensure mutual recognition of existing eID schemes. To do this, it defines different identity assurance levels and obliges each Member State to accept eIDs issued by another Member State, provided that the eID meets the identity assurance level required for its service access. This approach could be characterized as enabling rather than imposing harmonization. This is the context in which most private sector initiatives, such as iDIN, BankID, it'sMe, NemID, FranceConnect, etc., are created. These services are based on an individual having already been enrolled by the government of a Member State. eID then happens through:

- A bank's KYC process
- BankID
- NemID
- Or the identification of a public service, such as FranceConnect

Their solutions are therefore interoperable throughout the European community. It is likely to take some years before a majority of Member States accept eIDs issued abroad as evidence of entitlement to access their public services.

Like the Directive, eIDAS does not affect the validity of existing signature arrangements within closed systems and is silent on the question of public administration. A number of Member States carved electronic communications with public bodies out from their general laws implementing the Directive, but that will no longer be possible. Even in those Member States that do not have eID schemes, it will be possible to sign official documents electronically.

eIDAS has been on the statute books for two years before its effective date in July 2016 to leave time for various preparatory work to be done. In particular, the European Commission was tasked with preparing technical specifications, standards, and procedures to ensure that mutual recognition is effective in practice as well as in law. The list of eID schemes that accept mutual recognition will only be published a year from the preparation of those materials, which are not yet complete. Further time will have to elapse before the relevant provisions of eIDAS come into effect.

Legal Effect of Different Types of Signatures

Under eIDAS, any of the three categories of e-signature can be legally effective; the difference between them is only what evidence it will take to reassure a court that the signature is genuine and intentionally applied to the particular document.

- A simple form of e-signature, such as a typed name or PDF copy of a handwritten signature, is easy to forge, and so a court is likely to require substantial additional evidence to demonstrate that it was in fact applied by the person named to the asserted document.
- An AES is much more difficult to forge and more tightly associated to the signed document, and so the supporting additional evidence required will be considerably less.
- A QES, on the other hand, requires no additional evidence, since by Article 25 eIDAS, the court is mandated to accept its equivalence to a handwritten signature. In fact, a QES shifts the burden of proof to the signer - unlike an AES, which, if contested, requires the Trust Service Provider to demonstrate that the signature is legally effective. Of course, it may be necessary to demonstrate that the QES is indeed meeting the QES requirements.

In order to assess the suitability of any form of signature for use with a particular document, the first question to ask is why the signature is required. Where the laws do not specify a signature at all to give it legal effect, courts are less likely to require elaborate forms of signature. Simple e-signatures or AES should be acceptable in such circumstances.

Similarly, where the signature indicates receipt of information as where there is a statutory requirement to give a customer notice of certain facts, a simple e-signature or AES should suffice.

Where the signature has legal effect to bind the signatory, lower risk will arise if a more formal mode of signature – AES or QES – is used, since the formalities of these signatures automatically capture much of the evidence necessary to assure a court of their authenticity. But if the parties agree between themselves what form of electronic signature is appropriate to use, then this will be taken into account in any court proceedings.

eIDAS has no impact on national legal requirements regarding what documents require signature to give them legal effect since this is a matter of a wide variety of laws – those governing wills, land transfers, guarantees, electoral processes, etc. It remains necessary to check national legal requirements on a case-by-case basis to verify whether a document requires signature, and if so, for what purpose (notice, legal effect or other).

eIDAS does, however, override national laws on the admissibility of evidence on the specific point of admissibility of electronic signatures. Regardless of national rules of evidence in all other respects, under Article 25(1) a court cannot deny an e-signature admissibility of evidence in legal proceedings solely on the grounds that it is in electronic form or does not meet the criteria for QES.



An electronic signature cannot be denied admissibility in evidence or legal effect merely on the grounds that it is in electronic form or does not meet the requirements for qualified electronic signatures.



As a result, eIDAS explicitly acknowledges that forms of e-signature other than QES should be given legal effect in appropriate circumstances. Further, it acknowledges that a Member State's courts have an obligation to consider the evidence and circumstances in order to come to a conclusion rather than simply dismiss electronic signing other than QES out of hand. Over time, decisions of the CJEU will begin to establish norms for the cogency of evidence of electronic signatures other than QES.

Regulation of Trust Services

The proliferation of disparate national standards and systems for regulation and supervision of certification service providers was one reason why the Directive failed to encourage cross-border use of e-signatures, since Member States devised widely divergent requirements for the sector. For example, the UK elected to leave the industry to regulate itself whereas Germany and Italy introduced rigid statutory requirements. In the circumstances, it was hardly surprising that certificates from one country were not expected to be recognized in another, and very few suppliers offer cross-border certificates in the sense of certificates supporting signatures of entities of any nationality other than that of the service provider itself.

This, then, is a key objective of eIDAS: to enable Trust Service Providers (TSPs) of all kinds to offer cross-border services, including suppliers of certificates to support e-signatures.

The Directive was concerned solely with e-signatures and supporting certificates, and so used the term certification service provider. This is too narrow for eIDAS, which concerns a wider range of electronic services, including validation and preservation services for signatures, seals (both ordinary and advanced), time stamps, delivery services, and also website authentication. Therefore the collective term TSP has been introduced.

It is considered necessary to prescribe legal and technical operational standards for all TSPs since they occupy a unique position in any transaction in which two parties – consumers, citizens and businesses – participate. There is no exact "hard copy" equivalent to a party which, without participating in the transaction as such, is nevertheless instrumental in enabling it to be effected. The nearest role is that of the notary who verifies and certifies the identity of a contracting party for the purpose of a remote transaction. Notaries are regulated under their professional standards.

There are two categories of TSPs: ordinary and qualified (QTSP). A QTSP is a TSP providing one or more qualified trust services, such as creation, verification, and validation of qualified e-signatures, and which is granted qualified status by a supervisory body nominated by a Member State. Both categories can supply any kind of trust service.

All TSPs must conform to appropriate security standards to prevent and minimize the impact of any security incident and inform stakeholders of the adverse effects of any incident.⁴ Where a security breach or data loss causes a significant impact on the trust service or personal data stored, TSPs must notify the supervisory body within 24 hours of becoming aware of the incident. Affected customers must also be notified without undue delay.

In addition to the security requirements, eIDAS imposes liability on TSPs for any damage caused intentionally or negligently to any person through the TSP's failure to comply with its obligations.⁵ Notably, this is not limited to the parties to the transaction; it could be a third party (a parent or subsidiary company for instance). The claimant has the burden of proving that the damage was caused by intention or negligence, unless the TSP is a QTSP, in which case intention or negligence is presumed. Of course, a QTSP has the right to counter the presumption of intention or negligence.

Unlike the scheme under the Directive, both 'ordinary' TSPs and QTSPs are able to limit their liability to relying parties for the issue of a certificate.

Under the Directive, only QTSPs were able to impose such limits. Liability is limited to the extent of any limitations on the use of their services (which the TSP may have given its customers advance notification of), provided that those limitations are also recognizable to third parties. What may be required for a limitation to be "recognizable" is unclear, but notice in a readily accessible form is likely to be effective.

In addition to meeting security standards, QTSPs are required to:

- Undergo regular audits
- Apply procedures appropriate under national law to tasks, such as verifying identities
- Employ suitably qualified staff and use trustworthy systems both for processing and storing data
- Maintain liability insurance
- Keep proper records
- Maintain an up-to-date termination plan to ensure continuity of service if the QTSP goes out of business.⁶

Most of these are, of course, sound business practices. Nothing prevents a TSP from complying with the requirements and applying the approved standards for trustworthy systems and products, without applying for QTSP status.

A QTSP does not need to be "qualified" in respect of all of the trust services it offers, and this will be made apparent in the published, trusted list. Accordingly, a QTSP could be qualified for the purpose of website authentication, for instance, without being qualified for electronic delivery or e-signatures.

The advantages of acquiring the QTSP status are essentially around marketing. The fact of being supervised by a government agency and granted that status should assist in persuading potential customers that their services are, indeed, to be trusted. Their QTP status will be public through publication of the relevant Member State's trusted list of QTSPs. The only additional right available to QTSPs and unavailable to TSPs is the use of the new EU trust mark for qualified trust services.

Legal Best Practices

As mentioned above, electronic signatures are perfectly acceptable in many contexts without necessarily even requiring the technical features of AES, let alone QES. In the contractual context, a signature is no more than one form of evidence that the terms were agreed to. Other evidence, such as a chain of internal authorizations prior to signature, may be available and may be sufficient to ensure the agreement is enforceable.

However, most Member States have national laws requiring particular categories of document to be signed. Consumer credit contracts are among the most common form

requiring signature, along with contracts for the sale of real estate and guarantees - or more generally speaking, documents that require a written signature as proof of consent. There are also legal requirements of signature for many corporate and banking documents. These categories are not in themselves harmonized under EU law and so will vary from country to country. As a result, it is necessary to check for each proposed use case whether a corporate, banking or other type of document does need to be signed under the applicable law.

Fortunately, eIDAS does harmonize the status of all documents in electronic form as admissible evidence. No court can refuse to admit a document solely on that basis. In addition, the legal recognition of electronic registered delivery services is advanced. Courts are prohibited from denying legal effect and admissibility to data sent or received using such a service solely on the grounds that the service is purely electronic in form, whether or not the service in question is a qualified service.

Notably, eIDAS elevates qualified electronic registered delivery services beyond equivalence with public postal services to equate to transmission of materials by courier. A qualified electronic registered delivery service confers:

- The integrity of the data it transmits
- Sending of the data by the identified sender and receipt by the identified addressee
- Accuracy of the date and time of sending and receipt indicated by the service

This amounts to a complete proof of service – unless there is evidence otherwise. The data transmitted must be secured by an AES in transit to eliminate any risk of tampering and a qualified electronic time stamp (which also requires an AES) must be applied. Reliance in this context on AES rather than QES illustrates that the eIDAS intends AES to be treated as sufficient guarantee of integrity of data.

⁴ Article 19

⁵ Article 13(1)

⁶ Article 24



PART 2

Compliance With the Regulation

eIDAS contains many different provisions for compliance. Under eIDAS, an electronic signature in its broadest sense includes any data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signer to electronically sign. Commonly referred to as the basic or simple e-signature, this form of e-signature is legally admissible, but eIDAS does little to define how such a signature can meet its requirements.

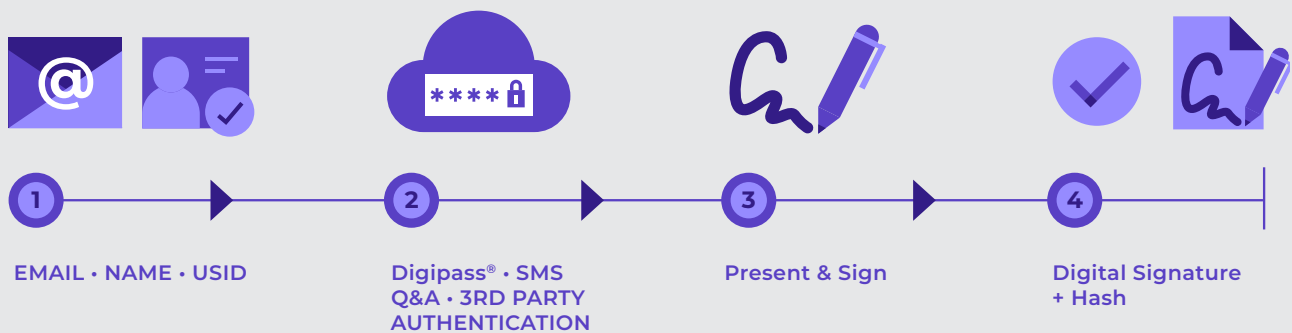
However, both AES and QES define additional requirements for higher levels of reliability. The OneSpan Sign solution meets all eIDAS requirements for electronic signatures, including AES and QES.

Advanced Electronic Signatures

OneSpan Sign complies with AES requirements under eIDAS by controlling access to the signer's electronic signature creation data during the e-signing workflow.

- Prior to signing, the signer is identified and provides his or her name and email address. This information is securely added to OneSpan Sign as part of the electronic signature creation data. A unique signature identifier (USID) associated to the signer is created and added to the electronic signature creation data in OneSpan Sign
- The documents to be e-signed are securely added to OneSpan Sign
- The signer must enter OneSpan Sign by successful authentication through one of OneSpan Sign's supported authentication methods or access points
- Once authenticated, the signer enters an online session with the documents and executes one or more acts of signing as required
- Each electronic signature is created with the signer's electronic signature creation data, which is only accessible through authentication plus signature time and date stamps or as meta-data related to the electronic signature session
- Each electronic signature is then secured by a digital signature

FIGURE 1. ADVANCED E-SIGNATURE WORKFLOW



OneSpan Sign Meets the AES Requirements as Follows:

- 1. It is uniquely linked to the signer.** In order to create his or her electronic signature, the signer must be authenticated by OneSpan Sign (or by the organization using the service, such as a bank, in the capacity of Registration Authority) to access and apply his or her electronic signature creation data to sign a document. The resulting electronic signature is uniquely linked to the signer.
- 2. It is capable of identifying the signer.** The electronic signature incorporates a signer's signature data, which is only added after identifying the signer. In this case, all identity and transaction data is stored in an evidence file that is accessible to all signers.
- 3. It is created using electronic signature creation data that the signer can, with a high level of confidence, use under his or her sole control.** The signer's electronic signature creation data contains his or her name, email address, and the USID which can only be accessed and used by the signer following his or her successful authentication by OneSpan Sign. Since OneSpan Sign supports multiple methods of authentication, one or more can be selected to set security commensurate with the risk involved in the signing process.
- 4. It is linked to the signed data in such a way that any subsequent change in the data is detectable.** Each electronic signature is secured by a digital signature containing a hash value unique to the signed data and the signer's electronic signature creation data.

It is important to note that OneSpan Sign digital signatures for AES are different from those created by qualified certificates in QES. OneSpan Sign digital signatures for AES use a single set of keys and a single digital certificate to digitally sign all transactions for all signers. Each electronic signature is differentiated by the signer's electronic signature creation data including name, email address, USID and authentication data. In this case, the signature creation device is a Hardware Security Module (HSM) attached to the OneSpan Sign service where the digital signatures are created.

Notes on Using AES and Authentication With OneSpan Sign

OneSpan Sign includes the following native authentication:

- OneSpan Sign account login using a password via the web or a mobile client
- Entering OneSpan Sign from an email notification link where the user was authenticated by the email system. This can be augmented by adding a shared secret or a one-time passcode transmitted through SMS
- Third-party authentication supported through SAML, OAUTH or through the API key

Two-factor authentication can be added with OneSpan Digipass products. OneSpan Sign also supports the use of standards-based digital certificates on smart cards and USB devices for e-signing, including qualified certificates.

During the course of an e-signing transaction, the signer controls access to the online session at all times and may interrupt a session and return at a later time using the same authentication method. As a result, OneSpan Sign provides the signer with a high level of confidence that the signature data remains under his or her sole control.

Verifying the Validity of an E-signature

Verification of the electronic signature can be accomplished in a number of ways. First, the OneSpan Sign digital signature can verify the integrity of the e-signed document using Adobe Reader with no need for special plug-ins, as the OneSpan Sign digital certificate is linked to the Adobe root certificate found in Reader. The signer's ID is also protected and verifiable within Reader.

The electronic signature creation data (name, email address, USID) can be validated by comparing it with the original data stored in the OneSpan Sign system. OneSpan Sign is fully secured and can only be accessed after successful authentication of the signer.

The data can also be validated through a file of probative-value evidence in which all transaction data are archived and time-and date-stamped (a form of static audit trail – see "Additional Evidence" on the next page) which is exported from and digitally signed by the OneSpan Sign system. The electronic signature data format conforms to ETSI TS 102 778-2 PAdES Basic.

Qualified Electronic Signatures

OneSpan Sign also complies with the requirements for QES. A QES is based on a digital signature created through a signature creation device using a unique key and digital certificate known as a qualified certificate assigned to an individual person. The qualified certificate and associated key must be obtained from a Qualified Trust Service Provider (QTSP) and must be provided on a supported smart card or USB device to use with a computer system. When using OneSpan Sign to e-sign with a QES, the smart card or USB device must be connected to the computer or mobile device accessing the OneSpan Sign service.

As with the AES, OneSpan Sign controls and manages the use of a qualified certificate during an e-signing workflow:

- Prior to e-signing, the documents are securely added to OneSpan Sign and associated to the signer
- The signer must enter OneSpan Sign by successful authentication through one of its supported authentication methods or access points
- The signer enters an online session with the documents and executes one or more acts of signing as required
- As each document is e-signed, the electronic signatures are secured by digital signatures created using the qualified certificate and associated key to create the QES
- The digital signatures are created on the supported smart card or computer system with attached USB device, and in each case requires at least a user ID and password for access

OneSpan Sign Meets the QES Requirements as Follows:

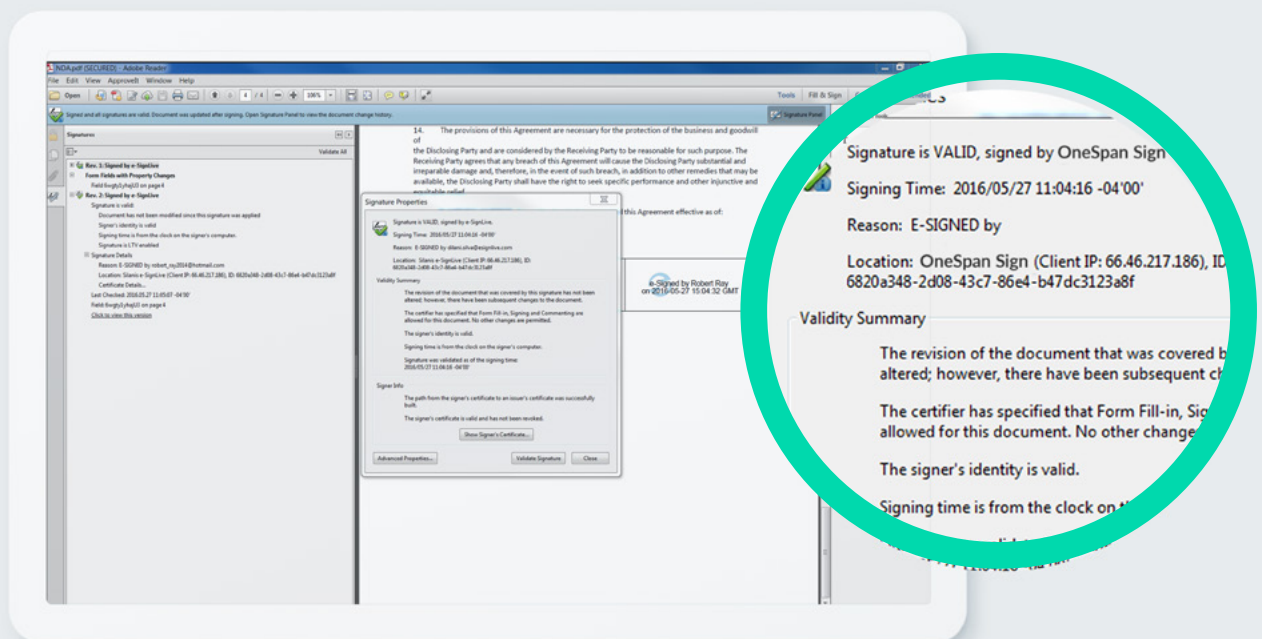
1. **It is based on an AES.** All requirements for the creation of a QES also meet the requirements for an AES
2. **It is created by a qualified electronic signature device.** While OneSpan Sign manages and controls all aspects of the e-signing workflow and security, the actual digital signing using the qualified certificate must take place on a supported smart card or computer system with attached USB device. This is the qualified electronic signature device as defined in the Regulation.
3. **It uses a qualified certificate for electronic signatures.** As described above, having such a certificate is a requirement
4. **The QES must be created by a QTSP.** With the QES, OneSpan Sign requires the user to provide his or her qualified certificate on a smart card or USB device issued by a third-party QTSP. While OneSpan Sign enables and controls e-signing with the certificate and device, the requirement for digital signing is met by the issuing third-party QTSP

OneSpan Sign can support qualified certificates issued by any TSP as long as it is based on the X.509 digital certificate standard. Unlike other e-signature providers, OneSpan Sign can use certificates from any issuer. This also enables organizations to leverage certificates issued by their own public key infrastructure (PKI), from their own Certification Authority (CA).

Format Standards

Under eIDAS Article 27, the European Commission is empowered to establish

FIGURE 2. E-SIGNATURE VERIFICATION WITHIN ONESPAN SIGN



additional technical standards and reference formats for AES, where these are to be used in the public sector. A decision in September 2015 introduced these formats.

The European Telecommunications Standards Institution (ETSI) signature standards include:

- Cryptographic Message Syntax Advanced Electronic Signature (CAAdES)
- XML Advanced Electronic Signature (XAAdES)
- Most recently, PDF Advanced Electronic Signature (PAdES)

Both CAAdES and XAAdES permit signature solutions which either define a place within the digital signature data format to hold the original data, or make use of a “packaging” format into which both the electronic signature and the original data are placed side by side.

OneSpan Sign produces e-signed PDF documents based on either AES or QES that conform to ETSI TS 102 778-2 PAdES Basic.

Additional Evidence

Depending on the use case, an organization may opt for the simple, advanced, or qualified e-signature. As mentioned previously, AES and QES provide progressively stronger evidence of the signer’s identity and should be chosen according to the level of risk involved in the process. For example, an internal signing process such as an expense report authorization would not involve the same level of risk as a remote bank account opening and, as such, does not require the same type of evidence and signature. In fact, a bank account opening is governed by several compliance rules that are integrated into the transaction itself, such as the description of the underwriting process or the acceptance of general conditions, or even the steps inherent to anti-money laundering (AML) procedures.

It is worth noting, however, that none of the forms of e-signature discussed in this article provides evidence of:

- How the signing process occurred
- The intent of the signer

OneSpan Sign supplements all three types of e-signature with electronic evidence in the form of dual audit trails to further secure the enforceability of electronically signed contracts and agreements. This includes:

- **The static audit trail** (what the signer signed): This audit trail contains the digital certificate used to sign, as well as the signature block image, time stamp and USID. OneSpan Sign offers two types of static audit trails. The first is the embedded audit trail, where key audit information is securely embedded in the e-signed document – no need to manage documents, signatures and evidence separately. The second is the Evidence Summary Report. This is a detailed audit log of the entire e-signature transaction that is available as a complete PDF document associated to the transaction.

- **The visual audit trail** (how and what the signer signed): With OneSpan Sign, each web page displayed in the browser and all actions taken by each signer are recorded, including moving to the next document or web page, clicking on a button, applying an e-signature, and downloading completed copies of documents. The date and time is recorded for each action, as is the IP address of each participant in the transaction. This provides a body of evidence that can be used to track the entire transaction, and thus define how an electronic record was presented, reviewed and signed. The organization can pull up the visual audit trail and play it back screen-by-screen at any point to prove what happened, like a security camera.

Using the web or mobile applications to present and control the signing of documents allows organizations to create a best user experience while ensuring compliance with laws related to the business transaction.

However, in legal disputes involving web-based processes, the entire process and content presented in the browser can be disputed even if the organization has the final, secured e-signed PDF documents. For this reason, it is not advisable to rely on a static audit trail to convincingly prove intent was established and the right process was followed. A static audit trail alone will not deter people from claiming:

- “Someone may have tampered with the system.”
- “I wasn’t presented with that information.”
- “I didn’t understand what I was signing.”

To safeguard against this, OneSpan Sign’s visual audit trail captures the full signer experience (i.e., all web pages, documents, disclosures, and other on-screen information, as well as emails and SMS messages sent, together with the time and date of each event). A cryptographic link ensures that the visual audit trail has not been tampered with and corresponds uniquely to the e-signed document. This unique capability has allowed OneSpan Sign’s customers to deflect numerous potential legal disputes before they escalate to litigation.

Conclusion

OneSpan understands the unique requirements of the European market and has been automating customer-facing transactions for regulated organizations for more than 20 years. At OneSpan Sign, our technology and expertise is based on insights gained through implementations at leading banks around the world, insurance carriers, healthcare providers and government agencies – as well as evidentiary and admissibility best practices.

See the e-signature evaluation checklist on the next page >>

¹ Regulation (EU) No 910/2014

² Directive 1999/93/EC

³ In this context, a certificate is a guarantee from a third party that the identity of the holder of the signature has been properly verified

⁴ Article 19

⁵ Article 13(1)

⁶ Article 24



OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.

This whitepaper is not intended as legal advice or legal interpretation of E-SIGN, UETA or any other laws or regulations. The information presented here is for general purposes only, and does not constitute legal advice.



Copyright © 2019 OneSpan North America Inc., all rights reserved. OneSpan™, Digipass® and CRONTO® are registered or unregistered trademarks of OneSpan North America Inc. and/or OneSpan International GmbH in the U.S. and other countries. All other trademarks or trade names are the property of their respective owners. OneSpan reserves the right to make changes to specifications at any time and without notice. The information furnished by OneSpan in this document is believed to be accurate and reliable. However, OneSpan may not be held liable for its use, nor for infringement of patents or other rights of third parties resulting from its use. Last Update September 2019.

CONTACT US

For more information:

info@OneSpan.com

OneSpan.com/Sign

E-Signature Solution Checklist

Selecting the right e-signature solution for your organization depends on a number of factors. Understanding the key criteria and how to rapidly get to the right decision is essential in effectively using e-signatures for your intended use cases.

Here are key considerations as you evaluate the various solutions in the market as they relate to the eIDAS Regulation and EU-specific requirements. Verify that the provider and solution:

	Complies with the latest EU eIDAS Regulation for e-signatures, AES and QES
	Supports qualified certificates based on the X.509 standard – from any TSP
	Supports certificates from an organization’s own PKI
	Supports AES by using strong authentication and server-based digital signing to secure and bind the signature to the document
	Supports QES for documents with multiple signers
	Offers a wide range of built-in authentication options (e.g., SMS text code, challenge-response, knowledge-based, digital certificates, support for strong two-factor authentication with solutions such as Digipass, and more)
	Supplements the e-signatures, AES and QES with dual audit trails – e.g., static audit trails and visual audit trails – that illustrate what was signed and how it was signed
	Creates a digital signature and hash for each signer in the transaction – tamper-sealing the document between signers and meeting PAdES requirements
	Ensures document integrity directly from the e-signed document – independently of the solution provider and without having to connect to their service
	Supports the languages that you operate and do business in – for both senders and signers
	Has responsive technical support and customer success teams – serving customers during local business hours
	Addresses data residency with flexible deployment options (e.g., on-premises or on a public or private cloud in your country or region in the EU)