TradeTech Solutions

A TTS eGuide to Electronic Identification, Authentication and Trust Services

eIDAS – An Introduction

Covering: eSignatures, eSeals, eTimeStamps, WACs and eDelivery

January, 2023

Foreword

This eGuide provides a brief introduction to Electronic Identification, Authentication and Trust Services – eIDAS.

eIDAS covers:

- eSignatures (Digital Signatures).
- eSeals.
- eTimestamps.
- WACs.
- eDelivery.

Here we set out what they are and what practical benefits they offer – together with some considerations you should take into account when using them.

The terms used above may seem unusual and complex. However, the rationale behind these services is very simple to facilitate trade by:

1. Reducing costs.
2. Providing greater efficiency gains.
3. Increasing trust between parties that may not know each other.
4. Improving user experience.
5. Increasing security and liability.

eSignatures (Digital Signatures)

First of all, these are ***not*** scanned copies of written signatures.

There are three categories of eSignatures:

1. Simple Electronic Signatures.
2. Advanced Electronic Signatures (AdES).
3. Qualified Electronic Signatures (QES).

Simple Electronic Signatures

A simple “electronic signature” is defined as “data in electronic form that is attached to or logically associated with other data in electronic form and which is used by the signatory to sign”.

Advanced Electronic Signatures

An AdES is electronic signature which meets the following four requirements:

1. It is uniquely linked to the signatory;
2. It is capable of identifying the signatory;
3. it is created using electronic signature-creation data that the signatory can, with a high level of confidence, use under his or her sole control; and
4. It is linked to the signed data in such a way that any subsequent change in the data is detectable.

Qualified Electronic Signatures

A QES is an AdES that has been created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

For legal purposes, clearly, a Qualified Electronic Signature is the preferred option. The 5 key benefits of QES eSignatures are:

1. Speed.
2. Confirmation that a party has signed a particular document.
3. They provide proof of identity.
4. Proof of authority to sign.
5. They are legally binding (in the UK).

In order to be able to issue QES it is necessary for companies to use the services of a Qualified Trust Service Provider. In the UK, the ICO is responsible for certifying Qualified Trust Service Providers.

eSeals

Electronic seals "eSeals" are similar in function to a traditional business stamp. These can be added to an electronic document to guarantee the origin and integrity of the document. Therefore, Electronic seals allow companies and other corporate bodies to 'seal' electronic documents and certify them as genuine, in the same way as an individual can use an electronic signature.

Qualified Trusts Service Providers can also issue eSeals.

eTimestamps

Electronic Timestamps "eTimestamps" link an electronic document, such as a purchase order, to a particular time, providing evidence that the document existed at that time.

Qualified electronic time stamp services must be operated by a qualified trust service provider and are required to meet the UK eIDAS requirements for qualified electronic time stamps.

WACs

Website Authentication Certificates (WACs) are electronic certificates that prove to your customers that your website is trustworthy and reliable. They ensure that the website is linked to the person to whom the certificate is issued. They also help avoid data phishing.

Once again, qualified website authentication certificates must be issued by a qualified trust service provider and are required to meet the UK eIDAS Regulation requirements for qualified web authentication certificates.

eDelivery

Electronic Registered Delivery Service (eDelivery) is a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the

transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations.

Similar in concept to recorded or registered post. They provide proof that information was sent and received electronically, and that it was not intercepted or altered on the way.

In the UK, eDelivery services are offered by qualified trust service providers.

Practical Considerations

See LawBite's Legal Document Management System.

How should your eSignatures be delivered?

- **Email Delivery**
  Many signing solutions rely on email-based delivery of an agreement without requiring any additional form of identity verification.
- **Scribble on a screen**
  This, in many cases, is the typical replacement for paper-based signatures and is familiar for the users. Unfortunately, this gives no assurance of the signer's identity.
- **SMS OTP**
  SMS OTP is the process of sending a random code to a mobile number, and this code is input to show that it has been received. This proves that the user signing has access to the device, but does not provide verified identification.
- **Signing with a third-party Electronic ID**
  Private individuals in some countries, (particularly in the Nordics, Italy, Spain and Benelux regions) have access to third-party electronic identities (such as BankID), as provided by their governments or banks. These eIDs can be used to sign electronic agreements.
- **Signing with identity documents**
  Some signing solutions leverage ID document scanning (such as passport or driver's license) or NFC reading of the document as a way to verify the signer's identity.

Document Security & Future Proofing Agreements

When generating digital signatures, digital certificates are involved. A digital certificate often has an expiry time, after which it is no longer valid.

Digital signatures are based on mathematical algorithms, which can be attacked by advances in mathematics, software and hardware. The algorithms used for digital signatures 10 years ago, are no longer secure, and it is simple to forge a document which looks like it was signed 10 years ago.

If the agreement could be expected to last a number of years, it may be advisable to print out a copy. This ensures that if the original program used to read and write the document is no longer available, the hard copy is still there for all to read.

Choosing your eSignature Solution and Service Provider

The questions you should ask yourself are:

1. How many electronic signatures do you expect to do?
2. What are your use cases? B2C, B2B, C2C, B2E (employee)?
3. How sure do you need to be on the identity of those signing?
4. Do you have any business system workflow you need to integrate with?
5. How future-proof do you need your signed agreements to be?
6. Can you trust your provider?
7. Is your Service Provider an ICO Qualified Trust Service Provider?
8. Do you need to guarantee the day and time of signature?
9. Do you envisage signing multiple documents with one signature?
10. Do you need multiple people to sign single documents?
11. Do you want to forward agreements for signing?
12. Will you be signing cross-border documentation?
13. Is the addition of long-term validation information important?

Legal Basis for eIDAS in the UK

The legal basis for the commercial use of these services in Europe has been underpinned by the European Union's (Electronic Identification, Authentication and Trust Services (eIDAS) Regulation, 23rd July, 2014 that took direct effect in EU member states in July 2016.

As a consequence of Brexit, on 31 December 2020, eIDAS was incorporated (with minor amendments) into UK domestic law in accordance with section 3 of the European Union (Withdrawal) Act 2018 (**UK eIDAS**). UK eIDAS largely mirrors eIDAS save for those provisions which the UK government has deemed "*inappropriate or redundant*". Amendments include the removal of references to "Member States" and the repeal of the interoperability framework for national electronic ID (**e-ID**) schemes. This means that the UK's national e-ID scheme, GOV.UK Verify, is no longer a participant in the EU interoperability framework for national e-ID schemes under eIDAS.

UK eIDAS applies to the whole of the UK. However, Scotland also has its own separate statutory regime for electronic signatures which sets it apart from England, Wales and Northern Ireland.

Special Legal Considerations

Legal advice should be sought when transacting with:

- Public sector bodies.
- Signing certain legal and financial documentation.

(Some documents still may require handwritten signatures.)

Cross-Border Documentation

Although many countries now have legislation in place authorising the use of eSignatures – indeed the EU has issued directives covering the whole of the EU to that effect. The implantation of such legislation does not necessarily precisely reflect UK law. Therefore, we would also suggest that you take legal advice before relying on the acceptance of cross-border e Signatures.

Disclaimer

TradeTech Solutions does no offer legal advice. This eGuide simply serves as an introduction to eIDAS. As an added precaution, please note that his is an area where changes in laws and regulations can be expected both in the UK and abroad. If you have ***any*** legal questions, you should contact your lawyer – or LawBite.