ascertia | IDENTITY PROVEN TRUST DELIVERED

Choosing the right type of e-signature for your business

Not all e-signatures are equal!
This guides helps you understand the differences and determine what is best for your business.

SigningHub

1) Introduction

What this e-Book delivers

One of the most confusing aspects for an organisation wishing to deploy an e-signature solution is understanding the technical jargon that different providers use. There are many e-signature schemes being offered in the market, with significant differences in terms of security and trust, legal acceptance, ease of use, interoperability and costs.

However there is very little documentation that explains these different techniques and thus allows them to be compared and assessed for their suitability in meeting a particular business purpose. This eBook provides the key information that helps business managers and technical architects understand the various types of e-signature that exist.

Not all e-signatures are equal!

This eBook analyses the common e-signatures types:

- Basic e-signature marks
- Biometric e-signatures
- e-Signatures with witness digital signatures
- e-Signatures with unique digital signatures (advanced digital signatures)
- EU Qualified e-signatures (or their equivalent in various global locations)

The following sections of this eBook discuss each of these e-signature types in terms of security and trust, legality, ease of use, interoperability and costs. A star rating scheme is used for easy analysis. ★★★★★

This approach will help you to understand the different concepts and then perform a risk-based approach in determining which is the right e-signature scheme for your business. As a result you won't get caught out by implementing an e-signature solution which is not fit for purpose.

The one constant in business processes is "change", so as soon as you deploy e-signatures for one purpose another business requirement will emerge. It is therefore important to choose a e-signature solution that is capable of supporting your needs today and yet also has a flexible architecture that can support your future business requirements.

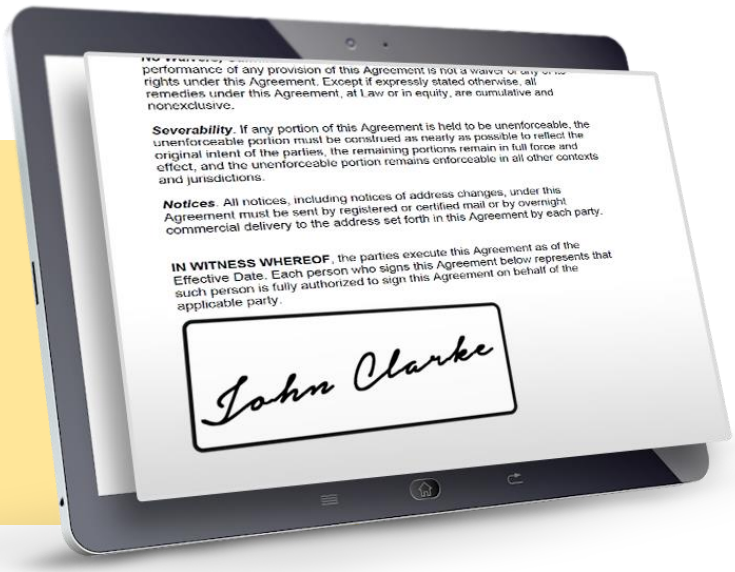
2) Basic e-Signatures

A basic e-signature can be any mark placed on a document to indicate the signer's consent, for example it could be a mouse squiggle, a signature drawn on a touch screen, an uploaded image, a signature typed in a special script font, a typed name or even an email address.

Security & Trust ★☆☆☆☆

A basic e-signature provides virtually no security! This is because it can be easily copied from one document to another. It doesn't protect the document from change once it has been applied. It doesn't identify the signer uniquely and can be easily repudiated as "that's not my signature".

The signer just makes a "mark" on the document



Properties:

1. No protection of the document itself
2. Signer can claim the e-signature was copied from another document
3. Signer can claim the document was changed after they had e-signed
4. Signer can claim that this is not their signature

Legality ★☆☆☆☆

In most jurisdiction even a basic e-signature can be admitted in a court of law as evidence, for instance in the EU eIDAS Regulations and US ESIGN Act. The issue is these signature marks do not provide any conclusive evidence and can be easily disputed because of the lack of security and trust.

Ease of Use ★★★★☆

Basic e-signatures are easy to apply, there is no need to register the user in advance or request them to login. The document can simply present the document in a web browser and ask the user to type or draw their signature.

2) Basic e-Signatures *(continued)*

Interoperability ★☆☆☆☆

There are no interoperability issues because a basic e-signature is just an image or other mark, however the point is that there is no mechanism for a verifier to determine if the e-signature can be trusted (hence a low interoperability rating).

Cost ★★★★☆

Basic e-Signatures are a low-cost option both in terms of infrastructure requirements and the user uses any modern browser. The only exception to this is if you want the end-users to draw the signature on a signature pad. In this case either a general purpose mobile device is needed (such as an iPad) or a special-purpose signature pad can be used (such as Wacom, Signotec).

> "Convenient but not useful for business documents"

Overall Conclusions ★☆☆☆☆

We do not recommend this type of e-signature for any serious e-business application because they provide no meaningful security. The typical use for these e-signatures is for low value applications where there might be other contextual evidence and/or there are no documents that require on-going protection. As typical example is signing for goods delivered to the home of office.

For any serious e-business use, the minimum recommended level is higher than this, for example a basic e-signature protected by at least a witness digital signature (explained in a later section).

3) Biometric signatures

These types of e-signatures are creating by gathering some biometric information that is unique to the user and then attaching this to the document. This could include fingerprints, iris scan or the most common example is measuring the physical aspects of the actual signature drawing process e.g. measuring the speed, pressure, pen incline and shape/size of the signature using a specialist hardware tablet and stylus.

Security & Trust ★★☆☆☆

Although biometric signatures sound very secure they are actually very susceptible to spoofing through replay attacks. Hacking of the actual signing device is also an issue. An even bigger concern is how do you verify the biometric signature? Who is trusted to securely hold the specimen data to compare the captured biometric data? How is this verification database initially populated and protected from hacking? There are also security issue in the trade-off between false-positive and false-negative results from biometric mechanism itself.

Legality ★★☆☆☆

Biometric signatures are acceptable in a court, but just like basic e-signatures, their weak security and interoperability do not provide convincing proof.

Ease of Use ★☆☆☆☆

This is a big problem as specialist devices are needed to capture the biometric information and to verify the data. This prevents their effective use in most remote locations such as signing document from home or on the move.

3) Biometric signatures *(continued)*

Interoperability ★☆☆☆☆

A major issue with biometric signatures is that they are based on proprietary techniques and popular document viewing applications like Adobe® Reader simply can't verify them. Specialist software is needed to sign documents and verify these signatures and this acts as a major constraint that prevents their general purpose use.

Cost ★☆☆☆☆

Biometric signature schemes are comparatively expensive because they require specialist hardware and software.

> "Interesting, but only for closed schemes"

Overall Conclusions ★☆☆☆☆

This type of e-signature cannot be recommended for general purpose e-business application because of the underlying security, interoperability and cost issues. They are useful for certain use cases where both the signer and verifier operate in controlled environment and have the necessary equipment.

4) E-signatures with witness digital signatures

Witness Digital signatures are created by getting the user to first create a basic e-signature and then adding a long-term digital signature applied by the service provider. The Witness Signature secures the user's e-signing and the document. The timestamp identifies the precise time the user signed.

After e-signing, the whole document is digitally signed using the service provider's Witness Signing key

Properties:

- The date/time of the user's e-signature action is identified and recorded by the witness signature timestamp
- The document cannot be altered without detection since it is protected by the digital witness signature

Security & Trust ★★☆☆☆

Usually the service provider authenticates the user using a single or multi-factor authentication techniques. The user then makes their e-signature mark which is bound to the document and protected by the service provider digital witness signature. This ensures the document integrity and means that it can't be altered in ay way without detection. A weakness of this approach is that the digital signature by itself does not authenticate the actual user, for that the recipient/verifier needs to rely on the service provider's logs. Therefore such signatures can be disputed if not implemented properly and do not by themselves provide the full security and trust one expects. Each e-signature should be protected by a long-term digital witness signature.

Legality ★★☆☆☆

Acceptable in court and depending on how adequate the service providers logs are in terms of detail and tamper-protection, these can provide good legal acceptability. However you need to watch out for what happens to the legal evidence backing your signed documents when you no longer use the services of the solution provider or they go out of business! Without these logs there is no evidence on whether it was a particular user who performed the signing action or not!

4) E-Signatures with witness digital signatures *(continued)*

Ease of Use ★★★★☆

This approach has the same ease of use as basic e-signatures since there is no difference from the user perspective (the service provider signature is applied automatically). The documents can be signed from anywhere at any time.

Interoperability ★★☆☆☆

Basic e-signatures protected with a standard digital signature such as PAdES are recognised and implemented in many third party PDF document readers such as Adobe® Reader. However since the signature doesn't contain strong user authentication information this e-signature technique loses its advantage in the area of interoperability. The long-term digital witness signature protects the document for years into the future.

Cost ★★★★☆

There is a great advantage in that no specialist hardware devices or software need to be provided to end-users. There is also only a single service provider digital witness certificate and thus there is no need to issue digital certificates to each end-user. This makes this signature techniques very cost-effective.

"Useful but could be more secure"

Overall Conclusions ★★½☆☆

We recommend this as the entry level e-signature scheme. It provides a reasonable level of assurance as long as the service provider processes and procedures are secure in terms of authenticating users and managing the associated logs. Security is strengthened when the user is identified in the reason for signing field and when a long-term digital witness signature is used.

Identifying and protecting each user's e-signature mark provides strong integrity assurance about what each signer saw and a timestamp confirms when each person signed. This is much more appropriate than adding a service provider signature at the end of the workflow process once all users have e-signed!

5) E-signatures with personal digital signatures

This is a special type of cryptographic digital signature that is created using a signing key under the sole control of the signer. The user's digital certificate clearly identifies them as the signer. Such solutions require a unique signing key to be provided for each user. The EU eIDAS regulation calls these "**advanced electronic signatures**". It is usual for a visible signature appearance to be created as shown below with the user's e-signature and additional text identifying their name, reason for signing and date/time. All this is bound and secured within with the original document.

John digitally signs the whole document using his own private signing key and includes his e-signature

Properties:

- The user's identity is bound within the document - no one else can sign on behalf of this user
- The document can't be altered in any way without breaking the signature
- The user can't deny having signed the document

Security & Trust ★★★★★

These signatures provide a high-degree of security since any changes to the document after signing will be clearly shown when the digital signature(s) fail to verify. Furthermore the digital signature could only have been created by the user since it required a key under the sole control of the owner. Users can be authenticated before accessing their key using various single-factor or multi-factor options. A user's signing key can be held locally on a smartcard/token, centrally in a secure Hardware Security Module (HSM) or encrypted database, or within the user's mobile device.

For added security each user's identity can captured and bound to their signing certificate after strong checks with well-known industry identity providers. Certificates can be issued by the organisation or by well-known trusted third party Certificate Authorities.

5) E-Signatures with personal digital signatures *(continued)*

Legality ★★★★☆

This approach provides high assurance and strong non-repudiation in a court of law when implemented properly. It is extremely hard for a signer to claim that they did not signed a document when all the required evidence is embedded directly into the document. This includes independent proof of the time of signing from a timestamp authority and proof that the signer's certificate was not revoked at the time of signing. Such signatures do not require strong reliance on service provider logs, although these can also be used as additional evidence if required.

Ease of Use ★★★★☆

Traditionally such e-signature schemes are thought of as being complex to establish and roll-out. However new approaches deliver all the required technology is much simpler ways for central installation. This means that users can just use web-browsers or mobile apps to view and sign documents. In such scenarios, users' signing keys are securely managed centrally using an HSM or a protected database. Each signing key is encrypted under a password which only its end-user owner knows. Overall ease of use can be same as e-signatures with witness digital signatures.

Interoperability ★★★★★

Because industry standard digital signature techniques are used such as ISO 32000, ISO 19005 ETSI PAdES formats there is very good interoperability. User identities can be assured by using well known Certificate Authorities (CAs), and Adobe® Reader now contains a pre-defined list of over 50 high trust global CAs.

Cost ★★★★☆

Solutions using centrally held keys and certificates are much more cost effective than older smartcard based approaches. Using unique certificates per user can be an additional cost when using third party CAs, however the use of solution internal CAs or existing Enterprise CAs can bring these cost down dramatically. Some financial organisations are also doing the vetting work for external CAs, as a by product of their detailed KYC / AML checks and this results in lower costs.

Overall Conclusions ★★★★☆

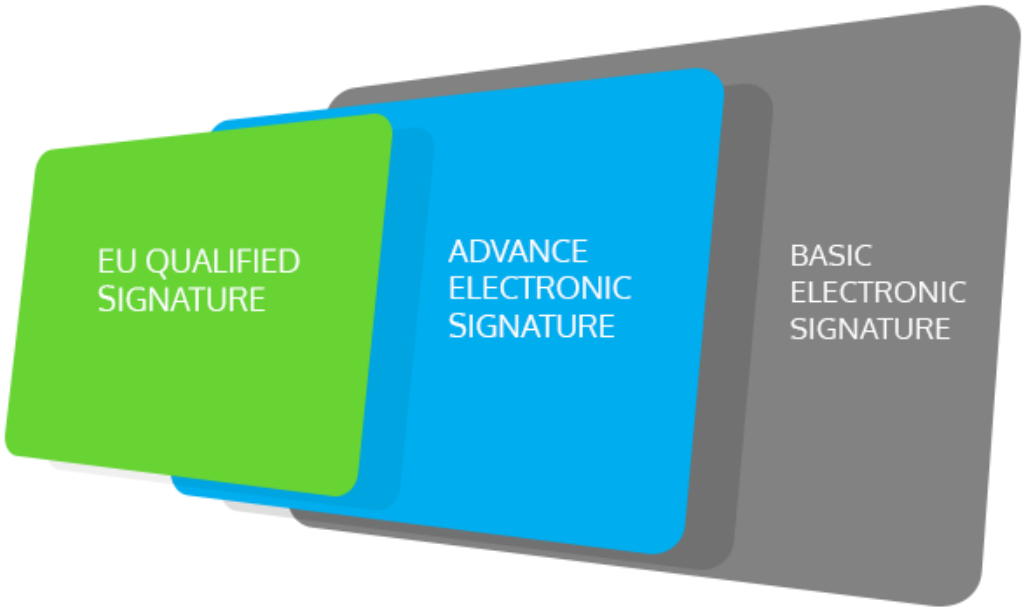
This is the recommended approach since it scores highly on all the criteria. You should bear in mind that advanced electronic signatures can be implemented in many different ways. Ensure you review how the cryptographic key material is created, saved and used.

Long-term signature formats ensure that important business documents can be verified well into the future (e.g. 10+ years is often a legal requirement). This means using standards such as ETSI PAdES Part 4 LTV with appropriate certificate lifetimes.

6) EU Qualified signatures

Qualified Electronic Signatures are a special class of advance electronic signatures described in the last section. They require the highest-level of security: the user's certificate must be issued by a Qualified CA which meets EU standard requirements and is regularly audited; and the user's signing key must be held in a certified tamper-resistant hardware device (referred to in the EU eIDAS regulation as a Qualified Signature Creation Device or QSCD).

Different e-Signature levels



Security & Trust ★★★★★

Qualified Electronic Signatures offer the highest level of security because the entire process of signing and verifying is standardised and assured to high-levels. The specified controls cover the trusted CAs, which are used to issue e-identity certificates to end-users. There are many such Qualified CAs in Europe. The user signing keys are highly protected inside certified hardware devices. Trying to dispute a qualified e-signature made using your key under your own control is almost a futile exercise!

6) EU Qualified signatures *(continued)*

Legality ★★★★★

At this high-trust level a qualified signature is by EU regulation automatically equivalent to hand-written signature in a court of law. The burden of proof is on the signer to prove be that the signature is not theirs! Again all the verification evidence is embedded inside the document itself, so the service provider logs act as only as a secondary level of evidence.

Ease of Use ★★★☆☆

Because qualified e-signatures can be created using a fully server-side solution the ease of use can be the same as e-signatures with witness digital signatures. However the provision of Qualified Certificates to a person requires strict face-to-face registration and vetting processes, which can be cumbersome for the user. As a result Qualified signatures are marked down in this category.

Interoperability ★★★★★

A high score is given because this approach uses a standards based approach following ISO 32000, ISO 19005, and ETSI PAdES signatures. Multiple solutions exist for creating and verifying such qualified signatures from various providers.

Cost ★★☆☆☆

Because of the stringent face-to-face registration processes, getting a Qualified Certificate from a Qualified CA is expensive. As a result this can push up the price of an EU Qualified Signature significantly when compared to advanced digital signatures based on normal certificates issued by general purpose or in-house CAs.

Overall Conclusions ★★★½☆

We recommend EU Qualified Signatures where there is a specific need for the highest level of security. This is often applicable where citizens are signing documents where there is no underlying contractual agreements to fall-back on and the risk of non-repudiation is high.

7) Conclusions

The following table summarises our conclusions:

Signature Type	Description	Rating
Basic e-signature	Only contains the user's mark on the document. No security, not suitable for serious use.	★☆☆☆☆
Biometric signature	Uses specialist hardware devices to measure physical properties of the signing process. Proprietary and therefore suitable only for closed environments.	★☆☆☆☆
e-Signature with witness digital signature	User makes their e-signature mark and then service provider protects the document with a digital signature using one central signing key. Digital signature does not authenticate the user. Need tor rely on service provider logs for that.	★★½☆☆
E-Signature with personal digital signature	Each user has their own signing key. User makes e-signature mark and then secures document with their own digital signature. These are advanced long-term signatures linked to authenticated user e-Identity, so directly authenticate the user.	★★★★☆
EU Qualified e-Signatures	Highest level of security and assurance due to use of trusted cryptographic hardware, trusted process and procedures and independent audits.	★★★½☆

Thanks for reading!

Having determined the right type of signature, the next step is finding the right solution…

Get the ultimate checklist for comparing solutions!

Key Questions to Ask e-Signature Suppliers

Start using SigningHub Today!

Free Trial

"How-to" demo videos: https://www.signinghub.com/how-to-videos/

Quick tour of SigningHub: https://www.signinghub.com/how-it-works/

Integration and API access: https://www.signinghub.com/website-integration/

Buy SigningHub now: https://www.signinghub.com/service-plans/

The SigningHub Team

info@SigningHub.com

www.SigningHub.com

Signed by: Liaquat Khan
Signed at: 2015-09-15 11:38:21
Reason: I approve this document

Liaquat Khan