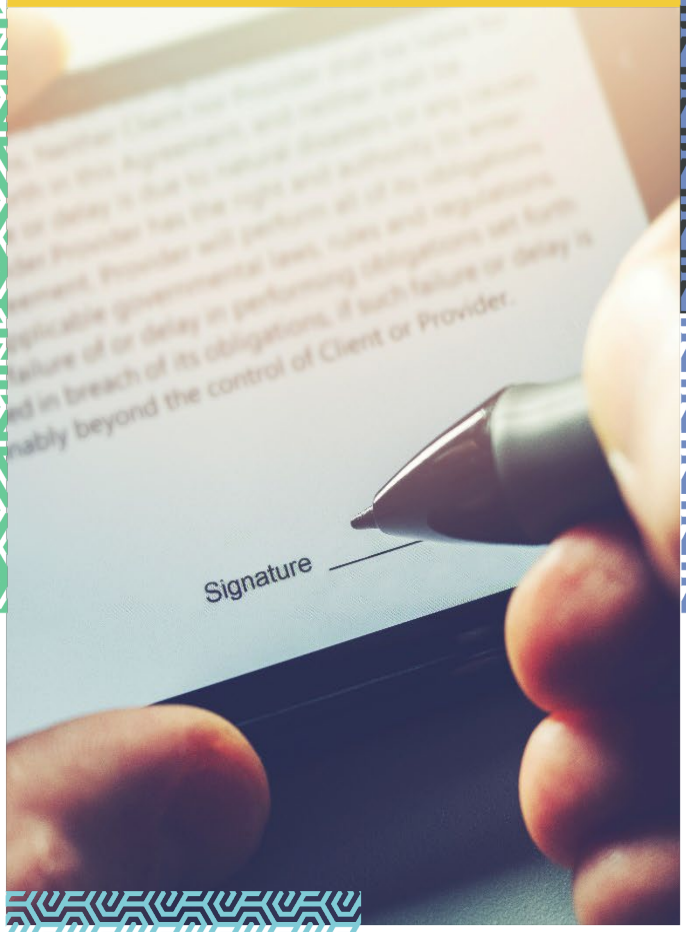
Risk control

Electronic Signatures



In partnership with

GALLAGHER BASSETT
GUIDE. GUARD. GO BEYOND.

Risk Management Partners
rmpartners.co.uk

Electronic Signatures

Introduction

Cybercrime regarded to be one of the greatest threats to organisations with a recent government survey reporting that half of businesses surveyed (50%) and around a third of charities (32%) surveys report having experienced some form of cyber security breach or attack in the previous 12 months[1].

Therefore, any organisation involved in entering into contracts and agreements via electronic means needs to have confidence in, and be trusting of, any communication that is sent in relation to that activity. This helps to ensure that documents sent electronically have not been altered in any way, that the sender can be easily recognised, and that the document maintains the necessary level of security.

Trust in business is key and can be enhanced using electronic signatures as they can prove the origin of the communication or document, show whether a message has been altered, and ensure confidentiality.

Electronic Signatures

Electronic signatures deliver a way to sign documents in the online world, much like we would sign a document with a pen in the real world. Electronic signatures come in many forms, including:

- Typewritten
- Scanned
- An electronic representation of a handwritten signature
- A unique representation of characters
- A digital representation of characteristics, for example, a fingerprint or retina scan
- A signature created by cryptographic means

Electronic signatures can be divided into three groups:

- **Simple electronic signatures** – these include scanned signatures and tick box plus declarations
- **Advanced electronic signatures** – these are uniquely linked to the signatory, can identify the signatory, and are linked to data within the signature that can detect any changes made
- **Qualified electronic signatures** – an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures

Electronic signatures are only as secure as the organisational processes and technology used to create them.

High value transactions need highly secure electronic signatures. Signatures used for these transactions need to be securely linked to the owner to provide the level of assurance needed and to ensure trust in the underlying system.

UK eIDAS Regulation

The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 (UK eIDAS Regulation)[2] established rules for UK trust services and establishes a legal framework for the provision and effect of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication[3].

Electronic trust services offer various means of enhancing security for electronic documents, communications, and transactions. For example, they can help verify that electronically sent documents have not been tampered with. By enabling the application and validation of these security measures, electronic trust services promote confidence in the secure transfer of information electronically.

There are five specific types of trust service covered by the UK eIDAS Regulations:

- Electronic signatures
- Electronic seals
- Electronic time stamps
- Electronic registered delivery services
- Website authentication certificates

As part of its supervisory duties, the Information Commissioners Office has the authority to take enforcement action in cases involving qualified trust services or when there is evidence of non-compliance with the regulations by any trust service provider operating in the UK.

Scope and Application

In considering changing signatory processes to electronic signatures; the first step necessary would be to review all processes and decide which documents and transactions may be suitable for using with electronic signatures (e-signatures / e-sigs).

Some documents may be automatically excluded due to the legal requirements regarding witnessing or other aspect of the legal process, but the remainder would need to be risk assessed to establish which transactions / documents would be classed as higher risk and therefore be subject to the use of secure e-signatures.

The organisation would need to specify criteria for higher risk documents. At present all e-signatures are admissible in the UK, so if there is a dispute, it is likely to come down to individual Courts to establish the degree of confidence in the authenticity of the e-signature. As a result, scanned images may carry very little weight, but if there is a verifiable audit trail showing that the signature was made in a certain location, at a specific time, possibly with a specific access authority (individual person), then the position potentially becomes much stronger.

A risk assessment is critical in establishing the risk appetite for 'getting it wrong' in terms of validity and what level of authentication is needed. It would be sensible to map the defined / scaled levels of security to the identified risk levels – ranging from a scanned image at the lowest level of security, through digitised signatures as a common-use security method, all the way up to e-signatures using cryptographic keys for high level security.

Forgery

Forgery is a clear and valid risk - especially where one or more of the signatories is not known to the organisation and the whole transaction is being conducted remotely.

In such cases, it will be crucial to obtain evidence of a signature that is connected to the individual(s). This process would be similar to the identification verification checks used in 'know-your-customer' procedures, but it would need to be expanded to include other parties such as consultants, suppliers, and contractors if it is to be used in that context.

Both organisations and their clients would want to know what measures have been taken to ensure that other parties seeking to use e-signatures are authorized to do so. They will want to confirm if these parties have the authority to bind and sign contracts.

A simple scan of a signature would be relatively easy to forge, as there is no connection to the actual document. In contrast, a digitized signature can be linked to specific details such as the time, place, IP address, and the authority or person behind it. Therefore, an e-signature platform that can achieve this level of verification in a straightforward manner would be an excellent starting point for effective risk management.

If systems are hacked; the signatures could be used to create false documents or agreements, so robust cyber-risk controls all round should be applied. Reputational damage could ensue if signatures are seen to appear on something that organisations would not wish to be associated with.

There is always the possibility that even where the true signature has been applied with intent at the time, if someone is looking for excuses to break out from an existing contract, they could claim forgery or other technical breach if they (or their advisers) have a full understanding of how the security processes work and what would easily nullify a contract.

Version Tracking and Control

It is possible for there to be numerous versions of signed documents in circulation, especially if some parties are comfortable with e-signatures but others prefer to wet sign and do organisations have to manage the process and ensure everyone ends up with the correct version, duly signed by all parties. It will be important to maintain a record of the signing process, culminating in the final signed version.

This type of control may already be in place as part of a wet signing process, but many e-signature platforms claim to keep the audit trail and manage version control so appropriate choice of software with control in mind is essential.

Linked to this, there would be scope for someone to claim that even though their signature is correct, the document has been altered after signing, so the linkage of the digitised signature to the time and version of the document would hopefully prove effective in rebutting any such claims. A full audit trail showing all versions and stages that occurred during the transaction will be helpful in this regard so look for a package / platform that has this facility, and in a way that's easy to reproduce and follow.

Compliance and Data Protection

Where legal, regulatory or an organisation's own compliance framework for transactions requires certain protocols to be followed, proof of this for internal control, compliance, and internal or external audit, will be necessary. Again, an e-signature platform with the ability to provide full traceability should effectively mitigate the risk of failure to comply.

At the higher risk / higher security level, there may be some personal details hidden in any data keys used to link that signature to the individual. That means data protection controls will come into play so it will be necessary to ensure that existing data protection controls extend to this new form of data asset.

Ease of Use

There is potential for a varied level of adoption depending on how complex the e-signature system / platform is to use. Generally, the higher the level of security, the more complex the process will become which could be off-putting to users.

The ability to vary the level of authentication according to an assessed level of risk will be helpful in this regard. A straightforward digitised signature might be sufficient in 95% of cases, but for higher risk matters, then digital signatures with cryptographic keys may be preferred. A system that could do both would be helpful, otherwise different e-signature platforms may be needed. If it's not easy to use, and organisations may end up with a mix of e-signatures and wet signatures which then has a knock-on effect back to the version control / traceability risks referred to above.

Email Security

All the security afforded through an e-signature platform / system and process could be completely undermined if the email system used is insecure, and so internet security is critical. Cyber risk controls and possibly a framework such as Cyber Essentials (or Cyber Essentials Plus) might be used to assess and control the environment in which the electronic signature platform is to operate.

Critical Date Management

If signing dates are linking in any way to contractually binding dates, e.g. review of contractual terms, then errors from misunderstandings and mismatched dates could lead to claims.

Errors in this area are known to be costly so it would be important to get the date management aspects correct and ensure there is a mutual understanding amongst the parties. An effective e-signature platform should be able to control this via the version controls and traceability described above.

Summary

There is a risk that claims could arise if contracts become invalidated or unenforceable which could have financial repercussions for all signatories and other beneficiaries. There may also be potential tax implications. International law is another important consideration.

In summary, most of the risks that could arise can be addressed through the adoption of a secure digital signature platform coupled with strong cyber-risk controls. The skill will be in selecting a system / package which balances security with ease of use, and possibly allows variable authentication levels according to the risk level of the document / transaction concerned.

Many of the risks already exist with paper and wet signing, it just becomes more apparent when examining the process in more detail. The aim should be to make the e-signature process equal to or better in terms of risk control. It may even lead to better compliance as all the data captured could be reported on for breaches at 100% inspection levels which would not normally be achieved by a standard inspection process.

References

1. Cyber security breaches survey 2024, available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024
2. The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019, available at: https://www.legislation.gov.uk/uksi/2019/89/made
3. What is the eIDAS Regulation? Available at: https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/

Further information

For access to further RMP Resources you may find helpful in reducing your organisation's cost of risk, please access the RMP Resources or RMP Articles pages on our website. To join the debate follow us on our LinkedIn page.

Get in touch

For more information, please contact your broker, RMP risk control consultant or account director.

contact@rmpartners.co.uk

Message of Thanks…

A message of thanks to QBE Risk Solutions, European Operations Financial Lines for their assistance in the production of this guidance document.

Risk Management Partners

The Walbrook Building
25 Walbrook
London EC4N 8AW

020 7204 1800
rmpartners.co.uk

FP1405-2024