Industry
Working
Group

Electronic Execution of Documents

Industry Working Group Interim Report

1 February 2022

Industry
Working
Group

Electronic Execution of Documents

Industry Working Group Interim Report

1 February 2022

Contents

Executive Summary

i. In its Report *Electronic Execution of Documents* (2019), the Law Commission concluded that electronic signatures were valid for the vast majority of business transactions and legal processes. Nevertheless the Report also recognised that numerous uncertainties existed which have hindered the use of eSignatures and limited the confidence of professionals and individuals in their use. These uncertainties potentially hold back some parties from adopting electronic signatures. The 2019 Report recommended that a multi-disciplinary group of business, legal and technical experts should be convened to consider the practical and technical issues involved, and to identify potential solutions. The group's task was to produce best practice guidelines and make proposals for further reform and development. Members of the group were appointed through public competition and the group started work in 2021. This is its Interim Report.

ii. The Covid-19 pandemic in particular demonstrated that the use of existing technology can be extended to accommodate issues of immediacy and lack of physical presence, such as the way that witnessing the signing of wills can currently be done remotely (whereas pre-pandemic this was not legally possible).[1] The same approach applies to electronic signatures generally.

iii. The three objectives of the Interim Report are (a) to analyse the current situation in England and Wales, (b) to set out simple best practice guidance which can followed immediately, using existing technology, and (c) to make recommendations for future analysis and reform. In doing so, the group has addressed the majority of its terms of reference, but not those dealing with international issues, which will be dealt with in the final Report in 2022. It is hoped that the other devolved administrations would adopt best practice as suggested for England and Wales, but that is outwith the scope of this Report.

Analysis of the situation today

iv. Under the eIDAS Regulations, the law currently provides for three levels of electronic signature. The group's view is that these levels of signature provide a useful framework. They are:
   a. Simple or Standard;
   b. Advanced Electronic Signature (AES); and
   c. Qualified Electronic Signature (QES).

[1] For further details, see Appendix 3, "Deeds".

v. The details are explained in the Report and the limited uptake of AES and QES in this jurisdiction is also addressed. The Report sets out how the formality requirements for some common documents can be fulfilled using these techniques, addressing a number of uncertainties and misconceptions which arise. The Report then briefly summarises the existing technology that is available and explains how it can be used.

vi. The Report's objective in this section is to de-mystify electronic signatures and demonstrate how they can be incorporated into transactions of all kinds, including those involving vulnerable individuals.

vii. It is clear that the foundations necessary for a cultural shift in document execution are already present. It is equally clear that a number of catalysts are required in order to ensure that such a change can be realised in a way which is both effective and timely. Widespread adoption across all layers of society will not happen overnight, but increased awareness of what can be done, how it can be done, and the advantages of doing so must only assist.

Best practice guidelines

viii. There are today a broad range of options available to anyone wanting to use an electronic signature to execute a document. Most documents can be executed in this way. In order to clarify how to navigate the available landscape, five principles are identified. Details about each are set out in the Report. They are:

a. Agree as early as possible that a document is to be executed electronically and the procedure for doing so. Determine the optimal form of electronic signature for the transaction, and in particular which eIDAS category (Qualified, Advanced and Simple) is required. This should be a matter of user-choice (depending on nature of parties/risk level/value/personal circumstances) and larger users should establish policies in relation to this.

b. Use a signing platform that provides a minimum set of security/safety/functionality with a strong audit trail that demonstrates an intention to sign by the signatories. Such platforms should as a minimum include ability of signing parties to download/retain executed documents. In particular storage, so-called 'shelf life' of documents and their audit trail details should be clearly identified by the signing platform to enable informed choice by signatories.

c. Consider whether additional evidence to record the fact that the signatory is approving the document is necessary and/or appropriate.

d. Where possible, provide multiple options to vulnerable customers or counterparties so that these groups can adopt a method of signing that suits their needs.

e. Authentication should be easier for those with secure digital identities, but this should not be essential.

ix. These principles are addressed primarily to legal professionals, both in-house and in private practice, and to business people. They are simple in nature and can be taken on board at the early stage of a transaction. Critical steps are to agree to use eSigning in the first place and then to determine which sort of approach to use. Detailed guidance on the factors to consider in making these decisions is provided in the Report.

x. The Working Group considers that digital identities should be made available as a matter of priority to all members of society who wish to have one. This will facilitate the uptake of electronic signing, particularly QES, and help modernise the approach to execution of documents in general. It will also match the position in some other European countries where are these are provided to citizens as part of their national ID schemes.

xi. The position of vulnerable individuals is considered and practical guidance is set out. Our view is that by following this guidance, electronic signatures have a role to play in the execution of documents by vulnerable individuals. They can be used with safety and with confidence.

xii. Following this path will facilitate the widespread adoption of the appropriate kind of electronic signature for the right kind of document.

Recommendations for future analysis and reform

xiii. The major recommendations in this Interim Report are:

a. The group supports the concept that QES, particularly if underpinned by a regulated digital identify trust framework, would be capable of fulfilling the same objectives as physical witnesses and attestation of documents, such as deeds.

b. A growing number of agreements are now performed in an automated way, as smart contracts. Since smart contracts often necessitate the use of an electronic signature, the increased use of these contracts will lead to a greater uptake of electronic execution practices. Therefore, the goal of showing how electronic execution can be undertaken simply and effectively is ever more important.

c. A cross-border database of permissible regulatory and execution modes should be established, starting with major trading partners. The database could be maintained by government or a not-for-profit industry organisation offering subscription access.

d. The group fully supports the work by DCMS to set up a trust framework as this will facilitate the use of electronic signatures in future.

e. Government should take steps now to adopt the use of electronic signatures in its transactions with third parties, whether providers of goods or services to government or the public. Government should also ensure that as many official

documents[2] as possible, which the public may have to execute, can be executed electronically (examples include Lasting Powers of Attorney and wills). The group considers that the Government acting as an "early adopter" in this way can only encourage the widest possible use of electronic signatures within society, ultimately saving costs and time, and demonstrating that this jurisdiction is fully embracing digital capabilities.

f. Standardisation is likely to facilitate the use of electronic signatures. Both the HMLR's Practice Guide on the execution of deeds, and the Ministry of Justice's Modernising Lasting Powers of Attorney project are good examples of how this might work.

g. The group recommends that the temporary provision allowing remote witnessing of wills be extended permanently.[3]

xiv. The group were split in their views on whether official certification or so-called "kitemarking" ought to be imposed on platform providers further to build confidence. The pros and cons of this are set out more fully in the report.

Conclusions

xv. The exercise of considering the legal and the technological issues simultaneously has proven to be valuable in achieving the Group's objectives. A principal conclusion of this Interim Report therefore is that both legal reforms and technological advances will be far more effective if they are developed in step with one another. It is a method that will continue to shape and inform the second phase of work. That phase will focus on the challenging but inescapable issues of how electronic signatures function in the context of cross-border transactions, and how best to use electronic signatures so as to optimise their benefits when set against the risk of fraud.[4]

xvi. The benefits of electronic execution of documents include speed, clarity, simplicity and security. Appropriate electronic signatures are a safe and effective way of entering into legally binding transactions of all kinds. These include anything from major financial transactions to the sale of goods to consumers. The technology and legal framework already exist to allow electronic signing by anyone from a major corporation to an individual. HM Land Registry already permits sales of property to be conducted using an electronic signature[5] and is currently conducting a pilot to remove the need for witnessing certain documents.[6] Vulnerable people are also able to use electronic signatures in appropriate circumstances. The technology and the approaches which are already available can be adopted by legal professionals and those in the business community without difficulty and so the foundations necessary

---

2 Forms specified by the state – such as Lasting Powers of Attorney and wills.

3 For further details, see Appendix 3, "Deeds".

4 Points (5) and (7) of the Group's Terms of Reference.

5 Practice Guide 8. For further details, see Appendix 3 to this Interim Report, "Real Estate contracts".

6 For further details, see Appendix 3 to this Interim Report, "Real Estate contracts".

for a cultural shift in document execution are already present. The group's clear view is that electronic signatures can and should be used today on a wide scale, and that members of society should have confidence in doing so. To achieve this widespread adoption requires an increase in the awareness of what can already be done, how it can be done, and the advantages of doing so. The group is committed to doing everything it can to facilitate this transformation.

Introduction

a. Background and formation

1. In its report *Electronic Execution of Documents* (2019),[7] the Law Commission concluded that eSignatures were valid for the vast majority of business transactions and legal processes:

   "An electronic signature is capable in law of being used to execute a document (including a deed) provided that (i) the person signing the document intends to authenticate the document and (ii) any formalities relating to execution of that document are satisfied".

2. The Report also recognised, however, that uncertainties remain regarding the mechanics of executing documents electronically. Additionally, these uncertainties may have had an impact upon the degree of confidence users (both professional and individual) have in terms of adoption or increased use of electronic signatures. As the Report expressed it:

   "parties will also need to consider the evidential weight (or probative value) which may be given to that signature if there is a dispute about, for example, who in fact signed the document, whether they intended to be bound, or about the content of the document."

3. The Law Commission therefore recommended that a multi-disciplinary group of business, legal and technical experts should be convened to consider the practical and technical issues involved, and to identify potential solutions, both by producing best practice guidelines and by making proposals for further reform and development.

4. In October 2020, the Government accepted this recommendation, indicating that it regards the Industry Working Group as playing a vital role in improving the conduct of both domestic commerce and international trade in the digital age. A public appointments competition was therefore advertised, with the selection exercise conducted by a public appointments panel chaired by Fiona Rutherford, the Director of Access to Justice. Successful applicants (all of whom are unpaid and acting pro bono) were notified in the spring of 2021.

---

7 https://www.lawcom.gov.uk/project/electronic-execution-of-documents/

5. The Group was chaired initially by Mr Justice Birss, who then became Lord Justice Birss in February 2020, together with Professor Sarah Green (Law Commissioner for Commercial and Common Law) and Mr Justice Fraser (High Court Judge and the former Judge in Charge of the Technology and Construction Court). When Birss LJ became the Deputy Head of Civil Justice, Mr Justice Fraser took over that role, with oversight continuing from Birss LJ. Professor Green and Mr Justice Fraser co-chair the whole Group.

6. The other members of the Group are (in alphabetical order):
   - Catherine Goodman
   - Simon James
   - John Jolliffe
   - Chris Jones
   - Simon Law
   - Michael Lightowler
   - Eoin O'Reilly
   - Charlotte Ponder
   - Jonathon Read
   - Neil Singer
   - Quintus Travis
   - Elizabeth Wall

7. A short description of each of their expertise is at Appendix 1. The Working Group met a number of times throughout the year, predominantly on a virtual basis, and also had the benefit of presentations from both industry names not represented in the Group, and government departments. The Working Group has approached its terms of reference on a platform and technology-neutral basis.

b. Terms of Reference

8. The Industry Working Group was asked to:
   i. consider how different technologies can help provide evidence of identity and intention to authenticate when documents are executed electronically;
   ii. consider the security and reliability of different technologies used to execute documents electronically;
   iii. produce best practice guidance for the use of electronic signatures in different commercial transactions, focusing on procedural steps to be followed, evidence, security and reliability where documents are executed electronically;
   iv. produce best practice guidance for the use of electronic signatures where individuals, in particular vulnerable individuals, execute documents electronically;

v. consider challenges arising from the use of electronic signatures in cross-border transactions and how to address them;
vi. consider potential solutions to the practical and technical obstacles to video witnessing of electronic signatures on deeds and attestation;
vii. consider how these potential solutions can protect signatories to deeds from potential fraud; and
viii. make recommendations to Government and to others on proposals in areas where the group consider reforms should be made.

c. Structure of this report

9. This report is divided into three further chapters. Chapter 2 analyses the current situation in the United Kingdom. The working group proposes that the existing legal framework provided by the eIDAS Regulation should be used. The different kinds of eSignatures are described and the reasons for the limited uptake of more sophisticated eSignatures are examined. The formal requirements relevant to different contexts and what is possible with current technology are also addressed in detail.

10. Chapter 3 focuses on best practice, addressing for instance how to decide whether an eSignature is appropriate and, if so, which kind is best suited to the situation at hand. The steps to follow are then explained. and best practice relating specifically to vulnerable individuals is dealt with in detail.

11. Chapter 4 sets out the working group's recommendations for further analysis, development and reform. These are divided into legal aspects, technical issues and other kinds. The question of accreditation and kitemarking, an issue on which the working group did not reach agreement, is also explained.

d. Conclusions

12. A principal conclusion of this Interim Report is that both legal reforms and technological advances will be far more effective if they are developed in step with one another. Otherwise, it will be very difficult to suggest legal requirements that are capable of being met, and technological solutions that are likely to be valid.[8]

[8] See also "Law and Technology Approach" in Schrepel, Thibault and Schrepel, Thibault, Smart Contracts and the Digital Single Market Through the Lens of a 'Law + Technology' Approach (October 21, 2021). European Commission, Available at SSRN: https://ssrn.com/abstract=3947174

13. The aim of the Industry Working Group is to facilitate and increase the electronic execution of documents. To that end, this Interim Report analyses how best to promote the transition from the current legal and technological environment to a future state in which the electronic execution of documents is performed effectively, routinely and with high levels of confidence. It identifies potential areas of legal reform and of technological development with a view both to changing the culture of document execution in England and Wales, and, specifically, increasing adoption of electronic execution. In so doing, the Report addresses as much of the Terms of Reference set out above as can be accomplished in the immediate term. Points (V) and (VII), the final two points, which are concerned with cross-border transactions and the prevention of fraud, will be the focus of the second phase of the Group's work.

14. This Interim Report is not only aspirational. It also provides a set of best practice guidelines to assist parties involved in executing documents in identifying the most effective, secure and efficient means of employing electronic signatures under current legal and technological conditions. Those guidelines have been formulated to allow parties to reach decisions based on their own particular circumstances, taking into account, for example, the nature and value of the transactions with which they are concerned, the resources available to them and the demographic within which they operate. This is intended to provide parties with the certainty that is currently lacking (or perceived to be lacking) in terms of how electronic signatures can be used and what they can achieve. In particular, concerns expressed to the Group from a wide variety of sources as to the need for evidential support to demonstrate the authenticity and reliability of signatures demonstrated that, even within the professional field, there is still a range of views as to efficacy and reliability.

15. Electronic execution and identification are issues which are currently attracting a considerable amount of attention in several different contexts, across different jurisdictions, and for a variety of purposes. Whilst it stands alone as a complete analysis in relation to its Terms of Reference, therefore, this Interim Report should also, where appropriate, be read alongside those publications and analyses with purposes complementary to its own.

16. Another important point to note is that modern technology moves at an increasingly astonishing speed. Technology companies and software providers develop and launch products at a pace that is rarely matched by law makers. The aim of the Working Group is to provide sufficient pointers to best practice that anticipate future changes in product availability, without stifling the innovation that is inherent in this field. The UK currently occupies an advanced position in its readiness to embrace new technology, as demonstrated (as a single example) by the Digital Trade Deal announced between the UK and Singapore on 9 December 2021.[9] This is said to be

[9] https://www.gov.uk/government/news/uk-agrees-worlds-most-comprehensive-digital-trade-deal-with-singapore

the first digitally-focused trade agreement ever signed by a European nation. It includes a commitment to digitise more trade administration documents, permit electronic signatures, electronic contracts and electronic invoicing processes, and work towards mutual recognition of electronic authentication and signatures.

17. In order to match the innovation in this sector, and also the increasing use (by some) across the world of the new technologies available to execute legal documents, speed is of the essence. It is important, for a legal jurisdiction to reach the forefront of this (and remain there) that recognition of the assistance that available systems can provide to performing traditional tasks is widely accepted. eSignatures are an example of this. Equally, this cannot come at the expense of sectors of society with more restricted access to such methods. What is suitable for the multi-million City law firm does not necessarily fit with the vulnerable individual without access to a hi-tech IT department. The Working Group has tried to balance these different issues in its work.

18. In addition to building on the Law Commission Statement on Electronic Execution of Documents[10] and the Government Statement in response,[11] for example, this Interim Report occupies a degree of common ground with:
    - The Department for Culture, Media and Sport's *UK digital identity and attributes trust framework*[12]
    - HMLR's Practice Guide on the execution of deeds[13]
    - The work of the Open Identity Exchange (OIX)[14]
    - The Ministry of Justice's Modernising Lasting Powers of Attorney (MLPA) project[15]
    - The Information Commissioner Office's position paper on the UK Government's proposal for a trusted digital identity system[16]
    - LawtechUK's *Smarter Contracts* project[17]
    - Tech London Advocates Blockchain Legal & Regulatory Guidance[18]
    - Law Commission's Advice to Government: Smart Contracts[19]

---

10 https://www.lawcom.gov.uk/project/electronic-execution-of-documents/

11 https://questions-statements.parliament.uk/written-statements/detail/2020-03-03/HCWS143 (2020)

12 https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework (2021). This initiative aims to establish a "trust framework", with a view to providing a "trust mark" to data-handling organisations that follow the rules of the framework. This allows data-handling organisations to show that they have been recognised as having robust processes, thereby enabling users to have confidence in trusting their digital identity to them. It is currently in alpha (prototype) format, so as to invite further feedback from private users, government and industry.

13 Practice Guide 8.

14 https://openidentityexchange.org/members/anon/new.html?destination=%2Findex.html

15 https://sites.google.com/digital.justice.gov.uk/opgmlpa/home

16 https://ico.org.uk/media/about-the-ico/documents/2619686/ico-digital-identity-position-paper-20210422.pdf

17 https://lawtechuk.io/explore/smarter-contracts

18 Blockchain: legal and regulatory guidance (second edition) | The Law Society

19 Smart contracts | Law Commission 2021

Analysis of the current position

19. In order to examine the reasons for low uptake of electronic signature technology and explain what is available, it is necessary to start with a brief summary of the current law and practice relating to electronic signatures.

a. Current law and practice

20. The principal function of a signature is to demonstrate an authenticating intention on the part of the signatory. What is required therefore is something which is not purely oral and which evidences that authenticating intention. A handwritten signature on paper documents purports to authenticate a text, show an intention to be bound by that text, and to provide evidence as to the identity of the party who is so bound. Whilst handwritten signatures were for a long time the best practical means of doing this, they have never been the ideal solution, susceptible as they are to problems such as forgery, duress and mistaken association. Technology now offers an alternative in the form of electronic signatures, some of which are capable of greatly reducing the risks inherent in the handwritten form.

21. The Law Commission Report[20] on which the formation and terms of reference of the Industry Working Group is based sets out the following statement of the current law in its Executive Summary. The full analysis underlying this statement can be found in Chapter 3 of that Report.
    i. An electronic signature is capable in law of being used to execute a document[21] (including a deed) provided that (i) the person signing the document[22] intends to authenticate the document and (ii) any formalities relating to execution of that document are satisfied.
    ii. Such formalities may be required under a statute or statutory instrument or may be laid down in a contract or other private law instrument under which a

---

20 See above, fn 6.

21 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ("eIDAS") Article 25(1), Article 3(10) and Recital 49. Also *J Pereira Fernandes SA v Mehta* [2006] EWHC 813 (Ch), [2006] 1 WLR 1543 at [28]; *Orton v Collins and others* [2007] 1 WLR 2953 at [21], *Lindsay v O'Loughnane* [2010] EWHC 529 (QB) at [95]; *Green (Liquidator of Stealth Construction Ltd) v Ireland* [2011] EWHC 1205 (Ch) at [44]; *WS Tankship II BV v Kwangju Bank Ltd and another; WS Tankship III BV v Seoul Guarantee Insurance Co; WS Tankship IV BV v Seoul Guarantee Insurance Co* [2011] EWHC 3103 (Comm) at [153] and [155]; and *Kathryn Bassano v Alfred Toft, Peter Biddulph, Peter Biddulph Ltd, Borro Loan Ltd, Borro Loan 2 Ltd* [2014] EWHC 37 (QB) at [42] and [43].

22 Or, as the case may be, the person on whose behalf the document is being signed.

document is to be executed. The following are examples of formalities that might be required: (i) that the signature be witnessed; or (ii) that the signature be in a specified form (such as being handwritten).

iii. An electronic signature is admissible in evidence in legal proceedings.[23] It is admissible, for example, to prove or disprove the identity of a signatory and/or the signatory's intention to authenticate the document.[24]

iv. Save where the contrary is provided for in relevant legislation or contractual arrangements, or where case law specific to the document in question leads to a contrary conclusion,[25] the common law adopts a pragmatic approach and does not prescribe any particular form or type of signature. In determining whether the method of signature adopted demonstrates an authenticating intention the courts adopt an objective approach considering all of the surrounding circumstances.

v. The Courts have, for example, held that the following non-electronic forms amount to valid signatures:
   a. signing with an 'X';[26]
   b. signing with initials only;[27]
   c. using a stamp of a handwritten signature;[28]
   d. printing of a name;[29]
   e. signing with a mark, even where the party executing the mark can write;[30] and
   f. a description of the signatory if sufficiently unambiguous, such as "Your loving mother"[31] or "Servant to Mr Sperling".[32]

vi. Electronic equivalents of these non-electronic forms of signature are likely to be recognised by a court as legally valid. There is no reason in principle to think otherwise.

vii. The courts have, for example, held that the following electronic forms amount to valid signatures in the case of statutory obligations to provide a signature where the statute is silent as to whether an electronic signature is acceptable:

---

23 Electronic Communications Act 2000, s 7.

24 This is the case for both electronic and non-electronic signatures.

25 As the Law Commission has concluded is most likely the case in respect of wills: Making a Will (2017) Law Commission Consultation Paper No 231, para 6.15.

26 *Jenkins v Gaisford & Thring (1863)* 3 Sw & Tr 93. Also S Mason, *Electronic signatures in law* (4th ed 2016) para 1.38.

27 *Phillimore v Barry (1818) 1 Camp 513, Chichester v Cobb (1866)* 14 LT 433. Also *J Pereira Fernandes SA v Mehta* [2006] EWHC 813 (Ch), [2006] 1 WLR 1543 at [26].

28 *Goodman v J Eban LD* [1954] 1 QB 550 page 557.

29 *Brydges (Town Clerk of Cheltenham) v Dix* (1891) 7 TLR 215; *Tourret v Cripps* (1879) 48 L J Ch 567.

30 *Baker v Dening* (1838) 8 Ad & E 93.

31 *In re Cook* [1960] 1 All ER 689.

32 *In re Sperling* (1863) 3 Sw & Tr 272.

a. a name typed at the bottom of an email;[33]
b. clicking an "I accept" tick box on a website;[34] and
c. the header of a SWIFT message.[35]

viii. Our view is that the requirement under the current law that a deed must be signed "in the presence of a witness" requires the physical presence of that witness.[36] This is the case even where both the person executing the deed and the witness are executing / attesting the document using an electronic signature.

UK eIDAS: Simple, Advanced and Qualified eSignatures

22. The eIDAS Regulation[37] created a uniform regime for electronic identification and trust services throughout the EU. In the UK, the eIDAS Regulation was supplemented by the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 and section 7 of the Electronic Communications Act 2000 and was on-shored (with amendments) as part of the Brexit process. From 1 January 2021, the electronic identification (e-ID) provisions of eIDAS were repealed and the UK lost access to the interoperability framework for e-ID.[38] The first section of the eIDAS Regulation deals with electronic identification systems and establishes a legal framework that allows for mutual recognition of identification systems between Member States, although given what has occurred since the UK left the EU this no longer applies to the UK as it did before. The second section is concerned with Trust Services and electronic signatures.

23. Under Article 25(1) of UK eIDAS, an electronic signature cannot be denied legal effect (either in terms of legal validity or admissibility as evidence) solely because of its electronic nature. It distinguishes between the three levels of electronic signature:
    i. Simple
    ii. Advanced Electronic Signature (AES) and

---

33 *Golden Ocean Group Ltd v Salgaocar Mining Industries PVT Ltd* [2012] EWCA Civ 265, [2012] 1 WLR 3674 at [32]. Also the following in which the court has said that, in principle, an email chain containing an electronic signature would be sufficient: *J Pereira Fernandes SA v Mehta* [2006] EWHC 813 (Ch), [2006] 1 WLR 1543 at [30]; *Orton v Collins and others* [2007] 1 WLR 2953 at [21], *Lindsay v O'Loughnane* [2010] EWHC 529 (QB) at [95]; and *Green (Liquidator of Stealth Construction Ltd) v Ireland* [2011] EWHC 1205 (Ch) at [44].

34 *Kathryn Bassano v Alfred Toft, Peter Biddulph, Peter Biddulph Ltd, Borro Loan Ltd, Borro Loan 2 Ltd* [2014] EWHC 37 (QB) at [43] and [44].

35 *WS Tankship II BV v Kwangju Bank Ltd and another; WS Tankship III BV v Seoul Guarantee Insurance Co*; *WS Tankship IV BV v Seoul Guarantee Insurance Co* [2011] EWHC 3103 (Comm) at [155].

36 Law of Property Miscellaneous Provisions Act s 1 and Companies Act 2006 s 44(2)(b); N P Ready, *Brooke's Notary* (14th ed 2013), para 11-09; *Halsbury's Laws of England* (2012) vol 32 *Deeds and other Instruments* para 236; *Freshfield v Reed* (1842) 9 M&W 404, 405; *Ford v Kettle* (1882) 9 QBD 139, 144 to 145.

37 Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market

38 The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019, SI 2019 No. 89.

iii. Qualified Electronic Signature (QES)

24. These are the three levels of signature which the Industry Working Group has decided to adopt. Our view is that there is no need to introduce different categories or levels in the current circumstances. An electronic signature is defined in UK eIDAS Regulation Article 3 as:

"data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign".

eIDAS defines three types of electronic signatures[39]

Standard Electronic Signature	**Advanced Electronic Signature (AES)**	**Qualified Electronic Signature (QES)**
Basic signature in electronic form • No identity verification of signatory required • Used in many common transactions	**Adds identity verification** • Links signatory identity to the signed document • Signature record can show evidence of tampering	**Requires heightened identity verification** • Special legal status: equivalent to handwritten signature • Sometimes required by law • Reverses the burden of proof

A: Simple Electronic Signatures[40]

25. The simple electronic signature is the most basic form of electronic signature. It is also currently the most widely used in the UK. Simple electronic signatures take many forms, such as "writing" using a finger or stylus, attaching a text or digital image, typing a name or symbol, or using a recognised signature software platform.

B: Advanced Electronic Signatures (AES)

26. The crucial feature of Advanced Electronic Signatures (AES) is that they require a link between the signature and the signatory, with a view to providing a degree of identity authentication. AES meet the extra requirements set out in UK eIDAS Regulation Article 26, which require the following of a signature:
    a. it is uniquely linked to the signatory;
    b. it is capable of identifying the signatory;
    c. it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

39 Graphic reproduced with the permission of DocuSign.

40 Sometimes called "Standard Electronic Signatures".

d. it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

27. Most AES currently rely on Public Key Infrastructure (PKI) to meet these requirements, the technical process for which is explained below.[41] A Certificate Authority (CA) will also be involved as a trusted party to create, manage and store the relevant keys.

C: Qualified Electronic Signatures (QES)

28. The most secure type of electronic signature, the QES builds on the features of the AES by requiring both additional technological protection as well as the involvement of a third party in the form of a Qualified Trust Service Provider (QTSP).

29. QTSPs are regulated by UK eIDAS through The Information Commissioner's Office (ICO). Those wishing to become QTSPs must apply to a conformity assessment body, and those bodies in turn must be accredited by the United Kingdom Accreditation Service (UKAS).[42] Although UK eIDAS retains many aspects of the EU Regulation, including allowing the legal effect of EU eIDAS qualified services to continue to be recognised and used in the UK, no reciprocal agreement currently exists. This means that UK eIDAS Regulation QTSPs are not automatically recognised and accepted as equivalent within the EU.

30. To be a QES, a signature must first fulfil the requirements of an AES. It must also be accompanied by a Qualified Certificate (QC) provided by a QTSP. The purpose of the QC is to verify the identity of the holder, and to prove that he or she is both a real person and the same individual who has created the account. The signature itself must also have been created by means of a Qualified Signature Creation Device (QSCD), the technical process for which is explained below.[43]

31. QES are the only electronic signatures which have the same legal effect as a handwritten "wet ink" signature; that is, they carry a presumption of authenticity. ("Wet-ink" is a phrase that is generally used to refer to signatures that are performed in the traditional way by writing or signing with a pen. As a colloquial expression, it appears to be increasingly widespread in its use.)

---

41 See below, under sub-heading "Current technological capabilities".

42 Appointed in September 2021 to accredit certifying bodies using ISO 17065:2012. See https://www.ukas.com/.

43 See below, under sub-heading "Current technological capabilities".

b. Limited uptake of AES and QES in the United Kingdom

32. Currently, neither AES nor QES is widely used to execute documents governed by English law. This section considers potential reasons for this, and reflects on whether those obstacles to adoption are more apparent than real.

Technical barriers to adoption

33. eIDAS seeks to enhance trust and legal certainty in electronic transactions, in part by providing a common framework for secure electronic interactions. QES are provided as a means of facilitating pan-European acceptance of eSignatures, but in doing so demand strict standards of identity assurance and security. The requisite sophistication of these technical requirements might currently constitute one of the most significant barriers to widespread adoption. Although this sophistication is probably of less concern to larger commercial organisations, it may act as a disincentive to SMEs and individuals. Even professional users (such as City law firms, for example) might initially be discouraged by the perception of complex technical requirements, especially as there is usually a need for speed and efficiency in high-volume legal transactions.

34. The Working Group considers that such perceptions, however, are for the most part outdated. The electronic execution technology now available is able to reduce friction in the signature process and, ultimately, increase convenience to users.[44] Whilst the use of such technologies will undoubtedly require some behavioural and organisational changes to begin with, it ultimately offers considerable advantages over wet ink alternatives. The Covid-19 pandemic and increased use of more virtual ways of working and doing business, particularly in 2020 when Government regulations restricted or even prevented physical meetings, has accelerated the pace of change in this respect in the business sphere.

Lack of accessible guidance

35. To understand the nature of a QES, and the standards that must be met, a potential user must navigate complex legislation, including definitions such as “Qualified Trust Service Provider” and “Qualified Electronic Signature Creation Device”, which in turn must be read together with several annexes of detailed requirements. There has historically been no user-friendly guidance provided by non-interested and non-commercial parties to help translate the legislative requirements into practical terms.

---

44 See below, under sub-heading “Current technological capabilities”.

36. It is also not easy to navigate the QES signing technologies or platforms available on the market.[45] Researching potential options is time-consuming and daunting for those without a certain level of technical knowledge. As a consequence, only those organisations with high volumes of documents will have the incentive to invest: any efficiency-related cost-savings require a sizeable document flow. It is also difficult in advance for some, particularly private individuals, to ascertain the full costs involved in doing so.

37. This situation is already slowly improving with, for example, the work of the Open Identity Exchange,[46] initiatives such as those being run by DCMS,[47] and the work of this Group. There is little doubt, however, that more accessible guidance, produced by a trusted and independent source, would encourage greater adoption of electronic execution procedures.

Protracted signing process

38. The term "eSignature" connotes a quick and easy signing process. Most users want a solution that makes signing documents as straightforward as possible and does not take a lot of effort to initiate. Ideally, the act of signing with an eSignature would be quicker and easier, or at least no more onerous in terms of time and effort, as the equivalent means of execution using a "wet-ink" signature. The identification aspect of QES could be seen to add additional steps to the familiar "print, sign, scan and email" process. Unless a signatory is familiar with using an electronic ID (which, in England and Wales, is unlikely), they may find the identification process time-consuming and potentially invasive. In the UK, for example, it involves a video ID check, in which the signatory is observed physically holding their passport by an employee of the Qualified Trust Service Provider.[48] The process is much easier, and more commonly accepted, in those countries that already have a government-backed electronic ID system (e.g. Belgium and Italy).[49]

39. The UK Government is, however, already working towards the development of a framework for digital identities,[50] an initiative that looks set to reduce the burden of the identification process, at least to a level commensurate with other European jurisdictions. As outlined below, the costs of investing in sophisticated forms of

---

45 The first ever UK Qualified Trust Service Provider was only certified by the ICO in July 2021: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/07/ico-approves-the-first-uk-eidas-regulations-qualified-trust-service-provider/

46 See above, fn 10.

47 See above, fn 8.

48 See below, under sub-heading "Current technological capabilities".

49 Some jurisdictions, such as Belgium, provide citizens with the relevant electronic ID associated with their identity card, which include a QR code unique to that citizen.

50 https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework.

electronic signature need always to be weighed against the level of advantage that they bring.

Complicated identification requirements and options

40. As well as being cumbersome from a signatory's perspective, the identification and validation process adds a further layer of complexity for those instigating a QES solution. There is no standardised pan-European identification process, so the different offerings from different providers using different means of identification require further research time. Entities looking to implement a QES solution for individuals from more than one jurisdiction will need to use more than one identification provider; this inevitably adds to this implementation time. Since the identification process requires the processing of personal data, there are also data compliance issues, which have, in turn, further time implications.

41. An analysis of the extent to which this presents an obstacle to electronic signature adoption, and the best means to address it, will be a focus of the Final Report.

Concerns in relation to certain cross-border transactions

42. Many jurisdictions (such as the US) do not have a QES equivalent. Parties from those jurisdictions (and their advisers) would find the complexity of the QES process quite difficult to comprehend, given how dissimilar it is to their own (simpler) regime.

43. This issue will also be addressed in the second phase of the Group's work, to be presented in the Final Report. That work stream commenced when this Interim Report was being drafted and aims to report later in 2022.

Evidential concerns

44. Whilst the QES identification and validation process could be seen as time-consuming from the document sender's perspective, and cumbersome from the signatory's perspective, it may yet not be sufficiently definitive for those concerned about the link between the signatory and the eSignature. Whilst the technical security requirements for a QES are stringent, the requirements for the identification element of that process, in the view of the Working Group, currently lack consistency, in that different EU member states interpret them differently and allow / disallow different ID methods for companies based in their country.

45. This is another potential concern that will be examined as part of the next stage of the Group's work.

46. The ID verification process involved with a QES could itself be said to be open to identity fraud, and the ability to call on expert evidence from a handwriting expert

may be seen by some as providing better protection. However, since technology now exists that combines QES and handwritten signing forensics, this is a concern that is likely to diminish over the medium term. It is also, generally, only as a last resort that handwriting experts would usually become involved in verification even for a wet-ink signature.

47. The security of any private key is only as secure as the signatory is prepared to ensure. The signatory may access the private key via a password or an electronic token, but this could be shared with others if the signatory so wished (or taken for use by others even if they do not). There is a greater chance of this happening when there is little personal value to the signatory. For example, an electronic ID that the signatory uses to interact with the Government, or to access their own personal finances, may be treated differently to a password that the signatory uses solely to sign documents on behalf of an employer.

48. Whilst this is undoubtedly true, the electronic process is at least as secure, and in the view of most members of the Working Group more secure, than the traditional method in that gaining unauthorised access to a private key is harder than forging a handwritten signature.

49. QES provide legal certainty under eIDAS because they are given legal equivalence to handwritten signatures, in terms of the presumption of legitimacy. This, however, is only one aspect of the function performed by a signature. Users also want to ensure that the signature provides reliable evidence that the contracting party agreed to be bound by certain terms. One of the elements of reliability is the ability to predict the weight to be given to any particular piece of evidence by the court in the event of a dispute. Since there is currently no case law in this jurisdiction relating to the use of QES, there is less certainty in how the court will approach a QES than there is for a handwritten signature. The latter benefits from established case law over a lengthy period of time. Potential users are therefore perhaps uncertain of the evidence that the court will require when considering a QES, and how the court will approach technical data such as digital certificates. One of the attractive features of a QES is the certificate by the QTSP or certificate provider confirming that the signature is "valid" or similar words. But such assurances are often qualified by a number of pre-requisites contained in the terms and conditions attaching to the certificate and which may appear in a typical relying party agreement. It is therefore important to acknowledge these limitations which may reduce the reliance which might otherwise be associated with the QES.

50. Any hesitation to adopt electronic execution based on this concern is both understandable, and somewhat inevitable, given the relative novelty of the technology and its legal treatment. It does, however, need to be considered in context: such limitations as there are in relation to the reliability of QES remain lesser those associated with handwritten signatures. Ever since the use of seals in Medieval times gave way to increasing use of handwritten signatures in the Industrial

age, evolution of society has led to different methods of executing documents. Electronic signatures are simply a 21st century manifestation of this change.

Lack of agreed processes

51. Although the signing process for simple eSignatures is still evolving, a settled practice has started to emerge. This has taken time, and has not yet extended to more advanced forms of signature. The further that the use of eSignatures moves away from traditional or established signing procedures, the longer the market will take to adopt a settled approach to their use. This lack of an established model may discourage some parties from the use of electronic signatures, particularly less sophisticated users.

52. There is yet further uncertainty when it comes to the interaction between QES and additional formalities such as witnessing. Although eIDAS provides that a QES is equivalent to a handwritten signature, it does not obviate the need for a witness where that is required under national law. Therefore, within the UK, if an individual were to execute a deed using QES, an in person witness and attestation would still be required. It is not yet apparent how this could be achieved: presumably either a "QES with a witness" process would need to be developed, or the law changed to remove the requirement for a witness where a QES is used.[51]

53. Whilst substantive reform of the law itself is in this respect outside the scope of the Working Group, it is our strong recommendation that such reform be considered by the Law Commission at the earliest opportunity. This is seen by the whole Group as a priority.

c. Requirements and Formalities

54. As stated above, certain documents have specific formality requirements. A formality is a procedure that a party must follow to give legal effect to a transaction, whether that transaction is an agreement between parties or a unilateral document. There are a number of these, usually enshrined in primary legislation. These are explained further below in two tables. The table in Appendix 3 addresses the electronic execution requirements relating to four document types: simple contracts, deeds, real estate contracts and smart contracts. The table in Appendix 4 addresses formality requirements for certain common types of transaction such as guarantees and powers of attorney.

---

[51] See below, under sub-heading "Recommendations for further analysis, development and reform".

55. Where there is no legal requirement formally to contract in writing, parties may agree (for certainty and evidential reasons) to enter into a signed and dated contract that records the agreement between them, so that there is then no question as to the legal validity of the contract form. The parties can agree their own signing approach.

d. Current technological capabilities

56. Different technologies target different use cases across the marketplace. Whilst most focus on remote use only, some provide for multiple scenarios within a single signing event (e.g. with one party present in person who needs to hand sign, another in a remote location who will sign cryptographically and another using an app who may be witnessing/advising and/or signing using their mobile). There is a broad spectrum of possibilities, including simultaneous wet ink and digital signing.

57. Electronic signing has progressed dramatically since the early days of handwritten eSignatures which used image capture analysis ("static signatures"), and even since the development of more sophisticated biometric signatures, which measure behavioural variances from known sample norms in a similar way to bank cheque verification. These forensically identifiable biometric signatures can also be combined with supplementary credentials such as social networking IDs (a Facebook login) or bank verification. Their high accuracy, customer understanding and convenience compared with paper mean that biometric signatures are used by millions daily and are relied upon by many large financial, commercial and governmental organisations in many countries, especially Europe.

58. Cryptographic techniques and the market-changing impact of platform promotion has, however, transformed the range of methods available, and such cryptographic techniques (often for simple signatures) have now gained a greater share of the mass market. All innovative market participants have invested heavily either to keep up or to gain competitive advantage in this race. A plethora of technologies exist and it is important for users to differentiate between different signature types, and to have the ability to prove the authenticity of, and connections between the signature, document and signature enablement providers.

59. Each technique carries a different profile of legal admissibility and evidential weight. For relying organisations (who intend to use eSignatures with customers) to assess suitability to meet a use case requirement, business processes may be analysed for match and categorised according to key requirements such as:
    - legal signature level, which defines the legal validity of the eSignatures,
    - use case, i.e. the specific context in which the eSignature is executed,
    - eSignature technology alternatives,

- user experience, i.e. how the user interacts with the business application to execute the signature, convenience versus security trade-offs, etc.,
- document model,
- deployment method.

60. As legal areas are covered elsewhere in this report, technology and process matters are covered below.

Use Case Categories

61. The most popular use cases and their requirements are:
    a. **In person,** including in branches shops or notary offices. This may use pen displays or signature pads, together with tablets and smart phones
    b. **Mobile** uses requiring offline integration of mobile tablets and smart phones to complete PDF forms and other documentation on the go. Scans of identity documents such as driving licence or passport, or capture of photographic images and biometric details, can also be used.
    c. **Remote** signing by external users on their own devices, typically via a web browser after clicking a link to trigger a transaction. This may be signing by completed PDF document or there may be a series of tasks still to be completed prior to signing, all of which may be done within one or more online sessions.
    d. **Internal** within organisations, where users may use single Sign-on (SSO) authentication from multiple application types and Public Key Infrastructure (PKI) integration. PKI is also useful for other signing types.[52]

eSignature Technologies

62. Selecting the most fitting signing technology for each use can be challenging. For simplicity, these may be grouped by:
    - basic (e.g. drawn image)
    - biometric handwritten signature
    - HTML5 web-based (click/type/draw/facsimile signing)
    - certificate-based

63. These methods may be used singly or in combination. It is important to remember that eSigning is about more than simply signing digital documents; it is about optimizing the whole process for the benefit of all parties. The process may vary by virtue of differences in national laws, even for the same type of transaction, as with financial services customer onboarding across different countries. The EU addresses such issues by publishing and updating regulations in this area.

---

[52] For an explanation of PKI, see Appendix 7B.

64. In 2014, Article 26 of the eIDAS Regulation set out requirements for advanced electronic signatures (AES). As set out above, an AES requires the following:
    a. it is uniquely linked to the signatory;
    b. it is capable of identifying the signatory;
    c. it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
    d. it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

65. The most common form of AES are digital signatures based on PKI, which satisfy all the above requirements.[53]

66. There are many different types of Certificate that can be used in various process elements e.g. for websites (SSL), Sealing, Timestamping, Encrypting, Identity tokens, etc. According to differing uses, the regulating Certificate Authority inspects and audits certificate issuers in respect of the intended (and permitted) use. Stronger forms of certificate use are associated with a person's identity, which enables the signing of documents using them. The intent is to generate a secure and unbreakable 'Chain of Trust' from issuing party down through users to third parties who may act on the completed documents.

67. Further assurances of signatory identity may be needed. Article 3 (12) of the eIDAS Regulation contains an option to create Qualified Electronic Signatures (QES), which are legally equivalent to handwritten wet-ink signatures across the EU. A QES is created by a Qualified Electronic Signature Creation Device (QSCD) which is based on a Qualified Certificate (QC) for electronic signatures, that is in turn issued by a Qualified Trust Service Provider (QTSP) and meets the requirements laid down in Annex I of eIDAS.

68. The remainder of this section addresses four areas of eSignature technology:
    (1) Processes for establishing eSigning certificates
    (2) An example QES process
    (3) User identification technology and signing types
    (4) Biometric signature processes

(1) Processes for establishing eSigning certificates

69. The eIDAS legislation has simplified the QES process by enabling the establishment of "remote signature" environments, where a QTSP manages the eSignature creation environment on behalf of the signatory. This means that users do not need to manage the eSignature creation device within their own environment, allowing a user to receive the required qualified eSigning certificates at any point throughout the business process (after an appropriate identification of the recipient). Increasingly,

[53] See Appendix 7B for a fuller overview of PKI.

this can be handled through API calls to eSigning platforms on a white label basis, where the platform appearance to a user is seamless, as if the entire user journey is experienced as if it were processed on a single, as opposed to multiple, systems.

70. Required elements include:[54]
    - Hardware – handwritten signature capture devices (such as dedicated eSigning pads/tablets, or general purpose computing devices including smartphones); Hardware Security Module (portable or server based); Biometric ID capture (Face, Signature, Finger/Palm, etc.), etc.
    - Software – residing both on user devices and on organisational or platform provider Server/Cloud (on-premises or cloud, or stand-alone) infrastructure, where the software controls most aspects of the perceived experience beyond digital performance.
    - QTSP Registration process ('Qualified' = 'Regulated') for the entity and process elements including for Signing Certificate Issuing to Individuals (natural person) and/or Seals (for Organisations).

71. The digital certificate in a QES is encrypted by a secure signature creation device, e.g. smart card or Hardware Security Module (HSM).[55] HSMs are the cryptographic device of choice to manage the generation of qualified signatures, and they securely generate and store the related Qualified Certificates and cryptographic keys. In recent years, HSMs have been available as part of a SaaS eSignature platform offering, which dispenses with the need for the user to carry a device, and for organisations to manage them.

72. A "virtual smartcard" HSM facility sited within a cloud (SaaS or on-premises) or network provides flexible anywhere-anytime access and signatories have sole control of their private key. As the OIX eSignatures (Oct 2021) Report notes:

    "Whilst the technology and cryptography of a QTSP's service may be far too complicated for many to comprehend, for the user the process of signing a document is now very straight-forward. With cloud-based software, QTSPs use HSMs to hold keys on behalf of their users, as opposed to storing the keys on physical hardware tokens. A signatory who uses a QTSP offering this service, uses the HSM to securely hold the signing keys, so there is a much lower risk of them being lost or stolen. Signatories can securely sign documents using their smart phone, tablet or another electronic device, which they are much less likely to lose or forget and means that the physical tokens aren't required to be re-issued making for a better experience for all involved and a more sustainable model. The use of HSMs is likely to be an

---

54 Note that this list is not exhaustive, and each of those elements listed below has several variants.

55 A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. A hardware security module contains one or more secure cryptoprocessor chips.

important factor in galvanising the market as is the ability of QTSPs in being able to verify the identity of the signatories remotely." [56]

(2) An example QES Process

73. The following example shows how QES could be used for a bank customer remotely to sign a credit application form on their online banking platform:
    a. The customer confirms identity by using their unique log-in, then reviews their credit details which may be added to an online form to sign. Alternatively, they may need other means of identification such as a KYC-AML compliant video-based onboarding for a new customer.
    b. For signing, an existing customer needs to enrol to use their QC, which – if not yet available – may be created directly during the signing process within the same front-end interface, or a disposable QC managed on a remote eSigning platform (RES).
    c. The customer then needs to perform two-factor authentication (e.g. mTAN or token based on existing 2FA by means available in the online banking platform) to proceed with the signing.
    d. Ask the customer to sign the request form to receive a QC online using OTP authentication on the phone number previously registered.
    e. Ask the customer to sign the document that requires a QES online using eSigning software:
        - Authenticate the customer's use of his/her personal QC managed in RES for executing a QES using OTP on the previously registered phone number.
    f. Replicate this step on every signature field that requires a QES.

74. A banking environment such as this has the advantages of the availability of complete customer data (required by the Anti-Money Laundering Directive) and 2FA mechanisms (already implemented for regular access to banking portals in compliance with PSD2).

75. In more detail, this signing process requires:
    - the crypto-server HSM certified according to eIDAS PP EN 419 221-5 "Cryptographic Module for Trust Services", which is equipped with
    - a 'signature activation' module certified according to eIDAS Protection Profile EN 419 241-2 "QSCD for Server Signing" to enable fast, scalable & flexible registration (certificate creation) and signing,
    - the signatory (e.g. bank customer) to be registered and identified,
    - his/her signing keys to have a Qualified Certificate (QC) attached,
    - the signatory to authorize a signature or operation (via the signature processing module), and

[56] https://openidentityexchange.org/networks/87/item.html?id=501.

- the signing key stored in the HSM being activated.

76. The signature module and integrated HSM ensure that the signatory has the sole control of authorizing a signing process, initiating a transaction or an operation. All communication to the HSM goes through the signature module for authorization first, and then activation of the signing keys.

77. For the customer, the process outlined above simply involves a regular video session and the use of an OTP on their mobile phones, which customers are accustomed to in their online banking software.

(3) User identification technology and signing types

78. One of the highest risks of potential fraud arises where the true identity of the signatory is insufficiently assessed and verified at the point of a transaction. So whilst a process may have been correctly executed in technical terms, if it is completed by an individual passing with fraudulent identity, the entire process will be compromised. Knowing exactly who one is dealing with, therefore, becomes increasingly important, especially in remote and self-service use cases. The table below summarises common forms of user identification by signing types:

Types	**SES**			**AES**	**AES with QC**	**QES**
Methods	Hard copy signed-Scanned and emailed	Signing Platform	Signing Platform-Use of 2FA	Signing Platform-Uniquely identifying the individual		
Uniquely linked to an individual				✓	✓	✓
User verified to defined standard (eIDAS)					✓	✓
User issued with electronic signing mechanism						✓

Source: OIX – Explaining eSignatures

79. With the highest level of security and proof defined in eIDAS, a QES satisfies not only the formality of "legal written form" but also has the characteristic of "non-repudiation".[57]

80. Electronic signatures are only as secure as the business processes and technology used to create them. Parties to high-value or important transactions may wish to have better quality electronic signatures: for example, signatures which are more securely linked to their owner in order to provide the level of assurance needed, and to ensure trust in the underlying system, such as AES or QES.

81. There are many ways a QTSP can verify user identity. Traditional processes relied on a face-to-face check of the user's ID document (usually a passport, driving licence or identification card) alongside a signed personal statement and other secondary documentation (proof of address).

82. eIDAS distinguishes between a signature produced by a natural person (individual citizen) and a seal produced by or on behalf of a legal person (organisation), although both use the same cryptographic process. When an individual applies for a QC on behalf of an organisation, additional information verifying the organisation's identity, address, and the individual's affiliation with that organisation will also be required.

(4) Biometric Signatures processes

83. A biometric signing process uses similar back-end technology to that used for fully cryptographic signing, but employs a different front end that permits the use of a handwritten stylus. For example, in an agent-assisted or self-service in-branch transaction, the customer identification by remote access login in the example given above[58] may be replaced by automated real-time signature recognition using stylus speed, acceleration, X-Y co-ordinates, rhythm, etc. to enable forensically discoverable signature evidence that can then be combined with an issued certificate.

84. Handwritten biometric signatures constitute a special case because they conform to two types of legal interpretation, that of a handwritten signature in electronic form and that of data in electronic form. Most of the legal treatment of eSignatures to date has tended to focus on eSignatures as 'data in electronic form' rather than as handwritten eSignatures, despite the fact that the (biometric eSigning) Solution allows for the creation of a handwritten signature in electronic form.

---

57 A quality, achieved through cryptographic methods, which prevents the signatory from denying that they signed the document: this is the technological analogy to reversing the burden of legal proof.

58 At [58].

85. Both contractual parties meet face to face,[59] which means that the organization that runs the Point of Sale/Service branch or shop environment has full control over the eSigning experience. While it is possible that customers may sign on their own device (e.g. smartphone), the standard scenario is that they read and sign contracts on a device that is set up for the use case, meaning that it has the proper size comfortably to read and sign documents, and has all necessary software pre-installed.

86. During this process, the customer signs with their own handwritten signature using a digital stylus, meaning the basic user experience is unchanged: all it takes to interact with the user is a device that can display documents and capture a handwritten signature.

87. The set-up can capture a QES (or other form of signature) and may be implemented through the following steps:
    a. Obtain the customer's consent to process his/her biometric signature using software for biometric eSignatures;
    b. Customer signs a request form to receive a QC - using the biometric eSignatures software;
    c. Identify the customer - using face-to-face identification and storing the identification assets for audit purposes (the latter may only be required by non-financial organizations as not under AML rules);
    d. Enrol the customer for qualified eSigning:
        i. Issue a (time-limited) QC that is managed on the provider's Remote eSigning platform (RES) using an API;
        ii. Create a biometric signature verification profile to enable biometric authentication for executing a QES using the customer's QC using the biometric signatures collected in step a and b;[60]
    e. Ask the customer to sign the document that requires a QES - using the biometric eSignatures software:
    f. Authenticate the just-captured biometric eSignature vs. the previously created signature verification profile (see step d(ii)) to execute a QES using the customer's personal QC managed in RES using a Biometric Server.
    g. Replicate this step on every signature field that requires a QES - using the Biometric Server;
    h. Delete the signature verification profile after expiration of the QES certificate:
        i. After 60 minutes with time-limited certificates;

---

[59] Remote biometric signature use is also possible, although is dependent on the availability of a stylus and a compatible (e.g. touch-sensitive, modern specification) device with which to sign on.

[60] Although, if future re-use of a signature to identify the signatory is not needed, and QES formality is not considered a requirement, creating a re-useable profile may not be necessary.

ii. After three years with standard certificates (note: this may only be possible in bank branches, as other scenarios require additional authentication when using standard certificates).

88. In such a case, for the customer to sign with a QES, the process outlined above only involves one additional handwritten signature for the certificate request form, compared with a regular advanced eSignature. The user experience is therefore similar to that for signatures on paper. [61]

89. This is just one example of a possible process; there are a great many variations on this that would be equally valid and effective.

Current video witnessing processes and capabilities

90. For some time, businesses have used CCTV records to help prove the identity of in-branch signatories in addition to documentary evidence. A greater number of QTSPs are now using video conferencing, necessitated by pandemic restrictions, although they are still dependent on appointment booking and agent availability to conduct the process. (It should also be noted that some QTSPs have gone a step further again and are able to meet the eIDAS requirements to create a QES via an automated end-to-end remote customer journey, without any need for video conferencing.)

91. There is also an obligation on the QTSP to ensure that the claimed identity of the user is a real person and is the same person as the one creating the account. Therefore, in addition to the information captured to fulfil regulatory requirements (as per Appendix 3), a “liveness check” using liveness detection software will also be required.

92. The entire process is facilitated differently depending on the QTSP in question, but must always be conducted in accordance with Article 24 of eIDAS. Once the user identity has been verified and the liveness check has been carried out, the QTSP can issue the QC to the user.[62]

93. Witnessing may be of an individual’s identity, and/or document completion, and/or of a signing. Often it is all three, and a person’s identity may also be captured and/or validated, and the signing process monitored, where the linkages between the documents, deposited signatures and identity may all be recorded via video using web cams (or similar). A Notary’s function is to validate all of this and conduct other checks (necessary as they have unlimited personal liability), but the process currently

---

61 Once registered, each new signing (in person or remote) will be similar to a paper process with only the document inspection and a handwritten signature. The difference is that the handwritten signature can authenticate a remote signatory, or that an in person signing can instantly identify the signatory.

62 ETSI Technical Specification 119 461 (July 2021) facilitates the meeting of European standards for identity proofing processes. This document aims to specify policy and security requirements for a ‘trust service component’, providing identity proofing of trust service subjects.

usually operates in person and is both relatively expensive and necessitates often inconvenient travel. This means that the convenience and cost advantage of remote witnessing is often preferred. Although personal appearance has been a fundamental characteristic of notarial practice for centuries, the Notary profession in England and Wales is trialling an electronic signature platform and testing other types of technology which, in the absence within the UK of digital identity cards, may enable them to process documents and carry out the necessary checks online. Quite often, Notaries are limited to the use of personal appearance and/or wet signatures because of the requirements of the jurisdictions in which their certificates will be used.

94. In a remote session, whilst physical documentation cannot be inspected in the same manner as a physical inspection of a passport (e.g. under UV light for unique verification features), technology is available which minimises the effect of such differences and adds to the overall documented record by means of video and audio recordings of an entire process (since it is not limited to the signing). It can also add new functionality such as:
    - instant automated cross-checks against databases of credit agencies, criminal records, etc.)
    - automated document validation (against known original document types, e.g. passports, driving licences, national ID cards, utility bills, government documentation, etc. for over 300 countries)

95. In addition, such processes are also able to provide the following benefits:
    - the giving of advice, consultative interactions and verbal agreements can be clearly captured and evidenced alongside digitally signed documents (this may be over one or multiple meetings).
    - signatory intent captured in video format provides clearer evidence of proof of understanding and agreement than solely relying on that which can be captured in documentary format (whilst there will of course need to be precautions built into the process to minimise coercion and similar unwanted behaviours).
    - every signed document will automatically generate audit trail records, capable of providing full details of each signatory, witness or meeting participant; their IP address, time, date and device; and a photo or video of the signatory captured as a minimum at the point of signature. Other details are also able to be captured, should the parties so wish.
    - advanced features such as person's liveness checks, 3D facial scan/model, rotation of passport/card documentation (and capture by webcam), RFID verification where allowed (e.g. passport chip information verification), automated voice, facial and movement analysis for stress indicators (that a live agent would act upon). There are more advanced features currently in development.
    - linkages with an entire customer record based in a provider CRM/customer management system may be embedded in the meeting metadata, enabling easier search and discovery in future if needed.

96. These are all appended to the transaction record. Different approaches mean that there may sometimes be multiple systems in use which need to be synchronised manually post-facto: there will be others where all artefacts are automatically captured and stored in an integrated seamless manner.

97. Best practice would dictate that all artefacts are bound together, encrypted, shared and stored in a tamper-proof manner. There is no common standard for how to achieve this and a lot of market development activity is currently ongoing this area. For example, storage may be achieved using secure repositories based on a traditional centralised data model, or may be securely split up and stored in Distributed Ledgers.

98. It should also be noted that with regard to use of real-time biometric data for identity purposes, the biggest issue is the correct linking of a biometric profile to the real person. This may best be done in person once at the beginning of the process, if some of the more powerful remote methods of identity verification are not available.

99. Whichever method is used, the goals of properly authenticating and proving intent and understanding with the highest evidential weight will be judged by businesses as a balance appropriate to the risks of the transaction. It is natural, therefore, that there will be many different solutions reflecting the diversity of the international electronic document execution landscape.

User experience by eSignature type

100. The user experience (how the user interacts with the business application to execute the signature) is key to the adoption rate of eSignature systems. Typical user experience options are:
    - Handwritten signatures (such as those on paper), captured mainly either on the same device on which the document is displayed/edited or on a peripheral device (e.g. sign pad) attached to a PC or display screen, or in some cases on a smartphone;
    - Signatures using a password-protected personal device (e.g. a smart card or USB token) with a personal certificate and/or company sealing certificate;
    - Click2sign signatures with or without an upfront identification or authentication step (e.g. two-factor SMS or email, facial recognition, etc.).

101. Each of these user experience options can be executed via an SES, AES or even QES when combined with Trust Services from a QTSP.

Types	Simple E-Signing (SES)			AES	AES with QC	QES
Methods & Validity	Mercury (scan/ email)*	eSigning Platform	eSigning Platform using 2FA	eSigning Platform uniquely identifying the individual		
Legal Equivalent to Wet Ink Signature						✓
E&W Simple Contracts	✓	✓	✓	○	○	○
E&W Deeds **	△	△	△	○	○	○✓
NI Deeds ***	✗	✗	✗			?
Scotland					Achieves Self Proving Status	

Key

✓ Suggested most appropriate option

○ Valid with greater assurance; may involve additional steps or expense. Deeds depends on use case***

△ Valid if witnessed correctly (some challenges practically)

✗ Cannot be used

? Not currently clear

* Hard Copy Signed – Scanned and emailed

** Deeds have different formalities required across different uses and also differ between individual signers versus legal entity signers (e.g. company Director signing). For regular signing where QES is permitted, users may prefer the convenience of cloud-enabled QES methods. Correct witnessing remains a practical challenge.

*** Northern Ireland has uncertainty due to 1584 Goddard's Case: whilst it is common practice for NI law deeds to be signed with wet ink as the safest execution mode, eSignatures also have some utilisation. The use of QES is untested in court.

Based on a format consistent with OIX eSignatures Report 2021.

102. User experience is also significantly influenced by how the signatory is guided through the transaction process. Two models have been proven useful:
    - Auto-stepping and workflow rules within a document, which define what a user has to do in order to eliminate expensive process failures such as missing signatures, data entries, or attachments;
    - Integrated video chat support that allows both contracting parties to meet and discuss contracts simultaneously simply via a web-meeting on any device. User authentication may be included through video or synchronous scan and share processes to comply with AML/KYC rules.

103. In addition to the legalistic or regulatory compliance aspects, there are many available methods to increase convenience and quality within eSigning processes:
    - Sequencing of multiple signatories' order of signing.[63]
    - Embedded markers (tags) and metadata about documents that can help consumers understand what they are signing and what fields they have to fill out, or a dynamic auto-display of only the relevant fields, based on user inputs.
    - The use of auto-check tools that identify common mistakes in documents in a timely manner to eliminate human error.
    - The addition of automated tailored notifications for participants, and dashboard status monitoring for organisations issuing multiple documents.

Other considerations

104. Some documents will require long term storage and it may be years (or half a lifetime on a pension or house purchase matter) before a dispute arises, so parties might not be confident that they can rely on signed digital documents. If the document is stored and the signatures are to be verifiable long after first created, in particular after the signing certificate has expired, the original validation data may no longer be available, or there may be uncertainty as to what validation data was used when the document was first verified. In addition, the cryptographic protection afforded by the signature may not be guaranteed after the certificate has expired. The ISO standard PAdES Long-Term Validation profile addresses this issue technically, but further work may be needed better to explain the issues involved to both users of eSigning platforms and courts. See Appendix 7 for more information.

105. With some platforms it is also possible to combine technologies in a mixed signing context, whilst still retaining compliance with eIDAS. For example, it is possible within a signing event for one party to sign biometrically in person (perhaps in the presence of a witness/sales consultant), another party to sign cryptographically using remote signing QES process, and a third to use a seal for organisational signing.

---

63 See, for example, the significance of signing order for LPA (above, under heading "Special contracts").

106. Increasingly eSignatures will be just one element of a fully automated remote or AI-assisted digital sales and service process. Some platforms offer a variety of collaboration and sharing tools that allow the operator to interact with the customer, exchange and capture documentation, as well as screen sharing, file sharing, document sharing and co-browsing, identity capture and verification (via documents, biometrics, intimate knowledge, etc.), certificate issuing for one-time or future identity authentication (tokens, biometrics, multi-factor authentication), and video recording, culminating in transaction sealing, sharing and archiving, all as part of a near seamless process.

Best Practice guidelines

a. Principles of best practice

107. It is clear from the Group's work so far that, under current legal and technological conditions, there is a broad range of options available to anyone wanting to use an electronic signature to execute a document. Whilst those options differ from one another sometimes quite substantially in terms of the security and reliability provided by each, those differences are reflected in the levels of knowledge, time and overall resource investment required for each type of signature.

108. These best practice principles identified by the Group are therefore intended to enable parties to use electronic signatures in a way which best suits their specific requirements. They are structured here so as to encourage wider adoption of the use of what is currently available, and so to facilitate the balancing of security and reliability benefits with the particular risks and resource constraints relating to particular transactions or arrangements.

109. Those principles, set out in full below, can be distilled into five high-level points:
    a. Agree as early as possible that a document is to be executed electronically and the procedure for doing so. Determine the optimal form of electronic signature for the transaction, and in particular which eIDAS category (Qualified, Advanced or Simple) is required. This should be a matter of user choice (depending on nature of parties/risk level/value/personal circumstances) and larger users should establish policies in relation to this.
    b. Where a signing platform is to be used, choose one that provides at least a minimum set of security/safety/functionality with a strong audit trail that demonstrates an intention to sign by the signatories. Such platforms should at the very least include the ability for signing parties to download/retain executed documents. In particular storage (so-called 'shelf life' of documents and their audit trail details) should be clearly identified by the signing platform to enable informed choice by signatories.
    c. Consider whether additional evidence to record the identity of the signatory and the fact that the signatory is approving the document and has the intention to be bound is necessary and/or appropriate, for example simultaneous video recording.
    d. Where possible, provide multiple options to vulnerable customers or counterparties so that these groups can adopt a method of signing that suits their needs.

e. Intention to authenticate should be easier to demonstrate for those with secure digital identities, but the latter should not be essential.

b. Is Electronic Execution Appropriate?

110. Before using an electronic signature (or deciding which type of electronic signature to use), it is important to consider whether the circumstances of the transaction (including the parties to it) have any features that affect the ability to use an electronic signature. Answering the following questions will help parties to identify this:

111. *Might a party want to enforce the agreement outside of England and Wales (for example, because the counterparty's assets are located there)?*

If so, parties may wish to seek local legal advice as to whether the relevant jurisdiction will recognise the validity of an electronically signed document (or a document electronically signed in the manner contemplated). Practice (and indeed regulation) differs widely. Whether the other jurisdiction is located within, or without, the EU is also likely to make a significant difference.

112. *Is any party incorporated outside of England and Wales?*

If so, that party may execute a document governed by English law using an electronic signature provided the signatory has the requisite authority. Authority is determined by the relevant local law. The authority of a signatory under local law may be dependent on their signing in a certain way or following certain formalities which may affect their ability to sign electronically.

a. For example, under local law, a signatory may only be authorised to execute a document if it is notarised or apostilled, which may not be possible with an electronic signature.
b. Parties may therefore wish to obtain local law advice confirming that any non-English signatories have authority to sign electronically. This should be a straightforward question to answer, as it does not require local legal advisers to consider the validity of an electronic signature in their jurisdiction.

113. *Is any party subject to corporate restrictions (for example in its constitutional documents) on its ability to sign electronically?*

Parties should check that any corporate signatories have the necessary corporate capacity and authority to execute documents electronically. Companies incorporated in England and Wales do not require specific authority to sign electronically, and will therefore possess the requisite capacity unless there is a specific prohibition in their constitution. Each entity will need to consider this (and a counterparty should therefore investigate or ask) on a case-by-case basis.

114. *Is any corporate party subject to restrictive internal information security policies regarding the use of cloud-based platforms?*

Some corporate entities have strict information security policies in relation to document storage and the use of third-party cloud-based systems.[64] These should be considered, at least in relation to the choice of signing platform.

115. *Must the document be filed with a registry or authority that does not accept electronically signed documents, or that has specific requirements relating to electronic signatures?*

If the document needs to be filed with an authority or registry, parties should establish at the outset whether the relevant body will accept documents signed electronically, or whether it has specific requirements relating to electronically signed documents.[65] An example of one that does not (although this is subject to review as at the date of this report) is the Office of the Public Guardian, which will not accept Lasting Powers of Attorney if that document is executed electronically. If the document needs to be filed with an authority or registry outside of England and Wales, parties should consider taking local legal advice as to whether an electronic signature in the form proposed would be acceptable.

116. *Does the location of the document, place of execution, or place of formation of the contract have particular regulatory or tax implications?*

The question of where an electronic signature is applied, or where an electronic document is held or stored, is currently untested, and therefore very difficult to answer with any degree of certainty. Is it, for example, to be determined by the physical location of the signatory or of the server on which the document is stored? Parties may therefore wish to avoid using an electronic signature for the time being if the question of location is material to the transaction concerned.

117. *Does the document require signing formalities that cannot be satisfied using an electronic signature?*

For example, if a party wishes to execute by affixing its common seal, it will not be able to sign electronically unless it has created and adopted an electronic version of its seal. Parties should also consider whether the document must be notarised or apostilled, or is subject to any other signing formality which would render an electronic signature ineffective.

118. *Does any party have a particular vulnerability?*

This will not usually be a concern in relation to a commercial contract entered into between two or more businesses, although it may be the case, for example, that one or more of the parties (or their authorised signatories) has a disability that needs to

---

64 Most web-based electronic signing platforms hold data in the 'Cloud'.

65 E.g., HM Land Registry, Practice Guide 8: Execution of Deeds (2021) at [13].

be considered. Paragraph 130 and following of this Interim Report contains further guidance for the use of electronic signatures where individuals, in particular vulnerable individuals, execute documents electronically.

c. How to choose the best form of electronic signature

119. As already established, the term "electronic signature" covers a broad range of technologies, all intended to link an identifiable person to information held in electronic form. The strength of that link varies between different technological solutions.

120. Above, under the heading "Statement of current technological capabilities", this Report considers both how different technologies can help provide evidence of identity and intention to authenticate when documents are executed electronically, and the security and reliability of those technologies.

121. As outlined above, some forms of electronic signature incorporate an intrinsic means of enhancing their own evidential weight. For others, it is possible to add best practice processes to achieve the same objective.

122. The decision as to which form of electronic signature is suitable for any given document will depend principally on the evidential weight appropriate for the transaction in question. This, in turn, will depend on two main factors:

    a. What is the value of the transaction relative to the financial means of each party?

       If the value of a transaction relative to the financial means of one or more of the parties is high, greater evidence that the document has been properly signed is likely to be appropriate. Conversely, parties may be prepared to adopt a less rigorous approach to an electronic signature in a transaction that has a relatively low value.

    b. What is the significance of the transaction to each party?

       Irrespective of its financial value, a transaction may hold particular strategic or personal significance for one or more of the parties. For example, it might be a contract for the supply of essential goods or services that are unique or not readily available elsewhere, or a patient signing to give consent to changes in personal care arrangements. Where this is the case, a signature with greater evidential weight is likely to be appropriate.

123. Appendices 5 and 6 provides detailed guidance as to the risk profile of different forms of electronic signature and the steps that can be taken to mitigate the relevant risks. Appendix 5 addresses issues arising from commercial transactions and Appendix 6 is focussed on individuals as parties to a transaction, particularly vulnerable individuals.

124. Not every signatory to a document must sign in the same way: some may wish to sign electronically and others using the traditional "wet-ink" method. Some parties may have a policy of using a specific electronic signing platform, whilst others may be prohibited from using a cloud-based platform. Although this is not a problem in principle, it can add complications, so it is helpful to be clear on which parties are signing using which method in advance, and to agree an appropriate signing process that is acceptable to both. Equally, if amendments to the final form may be required (or to put it differently, are not to be discouraged by the mechanism of execution) a platform that permits minor amendments should be adopted. A stark "accept and sign" only option may cause unnecessary practical difficulties, particularly where a lack of amendment capability may cause reluctance in wider adoption.

125. When using a web-based electronic signing platform, it is important to clarify on whose account the signing will take place. This may belong (for example) to one of the parties, or to a party's legal adviser. The person or organisation responsible for running the signing process should be prepared to provide the (other) parties with information regarding the security of the platform and the safeguards that it provides to verify the identity of the signing parties.

126. Alternatively, parties may wish to sign using their own preferred means of electronic execution before sharing the signed document with other parties by email or other agreed file exchange method. In this case, it is important for there to be transparency in relation to both the form of electronic signature that parties intend to use and the evidence that will be made available to other parties.

d. Fours steps to follow for electronic execution

127. The four steps to follow when executing a document electronically are summarised below.

Step 1: Agree in advance that the document will be executed electronically and decide on which procedure will be used in order to do so

128. There is no general requirement in English law for a contract to contain an agreement between the parties to use electronic signatures but, for the sake of clarity and certainty, it is advisable for the parties to agree between themselves that electronic signatures will be used, and the practicalities of doing so, in advance.

129. It is best practice for one party (or, if relevant, its legal advisers) to communicate with the counterparty/counterparties (or, if relevant, their legal advisers), setting out how the signing will be conducted as early in the transaction as possible. This is particularly important where the parties are unfamiliar with the electronic signing process in question, or a combination of signing methods are proposed, because it provides the opportunity for any issues to be identified and resolved in advance of signing.

130. Ensuring that answers to the following questions are provided in advance will help to identify any potentially disruptive issues, thereby allowing them to be dealt with at an early stage, and contributing to a smooth signing process:
    i. What information relating to the signatories (and any witnesses) is required in advance of the signing (e.g., name, email address, mobile telephone number, identity documents)? Do any of the signatories have special needs or are subject to any incapacity which must be taken into account to allow remote and/or on online signing to take place?
    ii. Who will circulate the final agreed document(s), and how?
    iii. What technology will the signatories need to have access to at the time of signing (e.g., their mobile telephone, the internet and potentially any identification documents, if required for a verification process)?
    iv. What form(s) of electronic signature are acceptable (e.g., inserting an image of a signature, signing using a touch screen and/or stylus, using an electronic signing platform)?
    v. Will any party be executing the document(s) other than by using an electronic signature (e.g., in “wet-ink” or using a company seal)?
    vi. Are there any particular signing requirements (e.g., authentication processes, confirmations required from signatories, witnessing requirements) and, if so, how will they be met? Will the signers need to be within a certain geographical location at the time of signing to meet legal requirements? Are any of the signatories acting in a representative capacity (e.g. director, executor or attorney) and have they provided evidence of their authority to act, if required? If any party is unrepresented, is there a need for them to take legal advice in advance to ensure they understand what they are signing? In case of cross-border documents, are they in language which all signatories can understand?
    vii. Who will date, release, exchange, deliver and/or compile the signed document(s)?
    viii. What will constitute an “original” of the document(s)?
    ix. Who will receive an original (or copy) of the signed document(s)?
    x. What (if any) evidence of the signing process will be provided to the parties after signing (e.g., a certificate of completion or an audit trail)?
    xi. Who will be responsible for any filings or registrations that might be required?

131. If cloud-based technology is being used, it is important to ensure that all parties are aware of this in advance. The choice of platform will depend upon a number of different party- and transaction-specific factors.

132. If data, particularly personal data (e.g., email addresses, telephone numbers, IP addresses), will be recorded and/or shared with others, it is also important to ensure that all parties are aware of this in advance.

Step 2: Circulate signing instructions that are as clear as possible

133. Shortly before signing, it is best practice for the individual or organisation co-ordinating the signing process to send clear signing instructions to all parties (or, if relevant, their legal advisers). If a web-based electronic signature platform is to be used, the document(s) and accompanying signing instructions may be sent directly from the platform.

134. The signing instructions should be consistent with the communication referred to in Step 1 above, acting as a reminder and providing further detailed practical guidance on the process. Some parties may be unfamiliar with the chosen signing process, and it is important that the instructions include clear, step-by-step guidance on the requisite steps, including:
    i. How any data is being collected or shared;
    ii. How to access the document(s) (including details of any authentication requirements);
    iii. How to sign and, if applicable, how to witness that signature[66] using the chosen form(s) of electronic signature;
    iv. How the signed documents are to be returned,[67] dated and released;
    v. The process for providing any additional confirmations that are required from the signatory or a witness, such as authority to date and release the documents; and
    vi. Contact details for the person co-ordinating the signing process.

Step 3: Circulate the relevant document(s) after signing is complete

135. It is best practice for each party to receive (or be given access to) a complete signed and dated document. Unless agreed otherwise, no third party (other than the parties' legal advisers, where relevant) or witness should have access to the final executed document. Some platforms provide storage as part of their eSigning service, but these provisions are not universal or indeed compulsory. Whether a party wishes to download, file or even print the executed document should be something that should

---

66 If an electronic signature is required to be witnessed, it is best practice to include a reminder, to both the signatory whose signature is required to be witnessed and the witness, that the physical presence of the witness is required at the time of signing.

67 With a web-based electronic signature platform, the signed document will be available for download from the platform.

be provided or available as a matter of course. That is not currently the situation, in the experience of some members of the Working Group.

136. If a web-based electronic signature platform is used, the certificate of completion and audit trail should be reviewed (or at least be made available) for consistency with the agreed signing process. That review should ensure that all parties are provided with a copy of the certificate of completion and audit trail. This provides evidence of the signing process and should be maintained (along with the final executed document) by the parties for their records. Storage of the executed version may be available by some platforms as part of their commercial service, although any "shelf life" concerns need to be considered.

Step 4: Handle information or data collected as part of the signing process appropriately

137. Any information or data collected as part of the signing process will need to be handled in accordance with any relevant information security standards, internal policies and legislation.

e. Identity, Security and Reliability

138. According to statute, certain documents (e.g., deeds) are only legally valid if they are "in writing", "under hand" or "signed".

139. Many other agreements (e.g., so-called "simple" commercial contracts) do not need to be committed to writing, or signed, for them to be binding. Parties may, however, choose to enter into written and signed contracts to provide evidence as to the terms agreed and the fact that they were agreed.

140. A signature is only useful as evidence if it provides a reliable link between the authorised signatory and the agreed terms. The stronger the evidence of that link, the more robust the signature. If the authenticity of a signature later comes to be contested (for example, in legal proceedings) it may be necessary to prove that the document in question was signed by the parties to it (or, where appropriate, their authorised signatory).

141. Where the authenticity of a handwritten signature is in doubt, it can be established using handwriting analysis. It is, however, also possible to authenticate handwritten signatures electronically, whether these have been deposited on paper with wet ink or whether they are made with a stylus (or finger) on a digitally recording device with a touch sensitive surface.

142. Using forensic analysis techniques, a wet-ink signature can be closely inspected by a specialist to determine factors such as stroke angle, pressure and image. Some

'traditional' specialists are now using electronic methods to inspect wet-ink signatures and present their results to the courts.

143. These electronic methods have often been retro-fitted from established biometric handwriting analysis techniques that have evolved over many years. These are much more powerful than inspecting the limited data points derivable from ink on paper layers, as they contain a full record of the manner in which the entire signature has been formed.

144. It is possible for such technology to show that, whilst a forged image of an electronic handwritten biometric signature looks superficially similar to a genuine one, some factors in its construction such as speed, rhythm, stroke angle, and a highly sensitive pressure profile, mean that the signatory in question is not the genuine originator.

145. Moreover, many banks and financial institutions in Europe use biometric handwritten signing to validate in real-time a signatory's identity using automated software. In the small number of cases where a sufficient match is not recorded, an alert is triggered to prompt additional proof of identity to be requested, and the process is automatically referred to supervisory staff.

f. Recent developments: HMLR, the e-APP

HMLR

146. HM Land Registry (HMLR) will, for the time being, accept (for the purposes of registration) certain deeds that have been electronically signed, but only if this has been done in accordance with the requirements set out in the HMLR Requirements that are set out in Practice Guide 8 – Execution of Deeds. These requirements are set out at Appendix 3 to this Interim Report under "Real Estate contracts". Importantly, all parties must have conveyancers acting for them. Non-conveyancers acting in person cannot do this.

147. HMLR will however accept so-called "mixed signing", which is when one party wishes to use a wet-ink signature and another electronic signatures. There are different requirements for different forms, and these are set out in a table at https://www.gov.uk/government/publications/signatures-accepted-by-hm-land-registry/accepted-signatures. A new Practice Guide incorporating this table is expected to be published by HMLR in early 2022, at about the date of publication of this Interim Report.

148. The deeds that can be executed in this way are:
    1. A deed that effects one of the dispositions referred to in section 27(2) and (3) of the Land Registration Act 2002.

2. A discharge or release in form DS1 or form DS3.
3. Equivalent deeds in respect of unregistered land.
4. An assent of registered or unregistered land.
5. A power of attorney other than a Lasting Power of Attorney (which are administered by the Office of the Public Guardian).

149. HMLR will also accept a deed of substituted security in respect of registered land, incorporating a discharge or release and a grant of a new charge, that has been electronically signed in this way, even though that discharge or release has not been done in form DS1 or form DS3. This is only provided there is nothing to prevent the deed from being regarded as sufficient proof of satisfaction of the charge (rule 114(4) of the Land Registration Rules 2003).

150. Documents in electronic form can be regarded as a deed if certain conditions are met, this provision being included in statute, namely Section 91 Land Registration Act 2002 (LRA 2002). However, that statute does not envisage the electronic signatures on the documents to which it applies being witnessed, which is perhaps not surprising, given the statute is 20 years old. HMLR is therefore piloting accepting for registration electronic documents that have been signed using a QES which will not require the presence of a witness. This is because the additional assurance offered by QES is considered by HMLR to compensate for the lack of a witness. If a conveyancer wishes to rely on section 91 of the LRA 2002, the HMLR policy will be that any party required to sign must do so with a QES.

151. Section 91 of the LRA 2002 does not disapply the formal statutory or common law requirements relating to deeds and documents; rather it deems compliance with those provisions. This means that a signature does not need to be witnessed. When the section applies, the electronic document is therefore to be treated as being in writing, as being signed by each individual and sealed by each corporation who has attached an electronic signature to it, and, where appropriate, as being a deed.

152. Section 91 LRA 2002 lays down requirements for making an electronic document, whether that document does the work of a formal deed, such as a transfer, a charge or a lease (which must be witnessed) or of a document that does not need witnessing, such as a contract. The section can be applied to any document in electronic form which effects the disposition of a registered estate or charge.

153. The Working Group had the benefit of a presentation from the personnel involved at HMLR on this subject. HMLR is currently trialling this through the acceptance of QES under a pilot scheme. This scheme involves a small number of conveyancers and through specified forms of transfers and charges. The draft practice on QES is under development and will follow, informed by the results from the pilot.

154. The Working Group considers that the approach of HMLR to the use of QES matches its own views as to the extra assurance provided by this level of eSignature.

Further, it also seems to align with the views of the Group that witnessing of deeds is no longer strictly necessary and ought to be reviewed at the earliest opportunity.

The Electronic Apostille or e-APP

155. Also, on 22 December 2021 the Hague Conference on Private International Law[68] (HCCH) issued Notification No.5 of 2021 of a new implementation of the electronic Apostille, or e-APP for short. This was to the effect that the UK was now permitted to issue e-APPs on all eligible public documents, as part of an initial pilot scheme. These would be issued by the Foreign, Commonwealth and Development Office as the Competent Authority.[69]

156. The Apostille is an important part of confirming the status, signature and seal of a Public Official and is recognised by more than 100 countries who are party to the Hague Convention 1961. Because the Apostille had always been issued in paper form only, it has prevented Notaries from being able to issue their certificates in electronic form. The advent of the e-apostille (e-APP for short) has added a tremendous boost to the initiative to enable the use and circulation of electronic Notarial acts. The pilot scheme in the UK will enable and encourage use of the e-APP among Public Officials in the UK, and will now be accepted in the relevant overseas jurisdictions that are also signatories to the Convention.

157. This demonstrates the increasingly widespread use of electronic versions of what were traditionally physical safeguards.

g. Vulnerable Individuals

158. In responding to the Law Commission's Consultation Paper on Electronic Execution of Documents, many consultees were concerned that consumers would be more likely to enter into agreements in haste or error if electronic signatures were used.[70] There was also concern that older or vulnerable individuals either may not have access to the required devices, not possess the required familiarity with technology to sign documents electronically, or not to be comfortable in doing so. This emphasises the need for best practice guidance in relation to vulnerable individuals who execute documents electronically.

---

68 This is an intergovernmental organisation in the area of private international law that administers several international conventions, protocols and soft law instruments www.hcch.net/en/home

69 https://www.gov.uk/verify-apostille

70 Law Commission, *Electronic Execution of Documents (Consultation Paper No. 237, 2018)*

Vulnerability

159. Vulnerability is multi-dimensional. Its nature and extent depend on the context or complexity of the decision someone is asked to make (and therefore on the document someone is being asked to sign). It is important to remember and recognise that many individuals do not wish to be categorised or described as vulnerable.

160. These guidelines refer to two categories of vulnerability:
    - **'Market specific vulnerability':** this derives from the complexity of the decision with which someone is faced and the type of documentation necessary to give effect to that decision.
    - **'Person specific vulnerability'**: this derives from a party's personal characteristics, such as a disability or poor mental health.

Market Specific Vulnerability

161. Any individual may become vulnerable because of one or more of the following complex and overlapping factors:[71]
    - **Health:** Health conditions or illnesses that affect an individual's ability to carry out day to day tasks
    - **Life Events:** Life events such as bereavement, job loss or relationship breakdown (the proportion of adults experiencing a negative life event was estimated to be three in ten (29%) in October 2020)[72]
    - **Resilience:** Low ability to withstand financial or emotional shocks
    - **Capability:** Examples include a lesser degree of knowledge of financial matters or low confidence in managing money (financial capability) and/or low capability in literacy or digital skills (digital capability).

Person Specific Vulnerability

162. Examples of characteristics that indicate vulnerability include:

    - Visual Impairment.

      Those suffering from a visual impairment are more likely to encounter difficulties in reading the document they are required to sign.

    - Physical Impairment

      Those suffering from certain physical impairments are more likely to encounter difficulties in signing the document they wish to execute.

---

71 Financial Conduct Authority, *FG21/1 Guidance for Firms on the Fair Treatment of Vulnerable Customers* (2021)

72 Financial Conduct Authority, *Financial Lives 2020 Survey: The Impact of Coronavirus*

- Mental Health.

  People suffering from poor mental health can sometimes experience difficulties with certain types of communication. This can mean they are unable to engage with processes that do not have a preferred method available to them. People with anxiety, for example, might avoid interaction with individuals and prefer to deal with matters by letter or email.

  Some of these characteristics can overlap, and one or more can be displayed. Individuals with any of these characteristics are likely to face additional challenges in executing documents, either conventionally or electronically.

163. Technology may increase accessibility for individuals with physical or visual impairments because many platforms include features which can assist with reading, reviewing and signing documentation. Using a technology platform to help with this process instead of relying, for example, on a third party for assistance, could provide additional protection for the signatory, particularly in cases in which undue influence or coercion may be present.

h. Best Practice Guidance - Vulnerable Individuals

164. The following best practice guidelines relate to the use of electronic execution with vulnerable individuals. They should be read in conjunction with Appendix 6.
    i. Where possible, parties should provide multiple options so that signatories can adapt a method of signing that suits their specific needs.
    ii. Parties should consider building into their processes the ability to guide parties through the signing process, for example by adding notes or explanatory wording throughout.
    iii. Parties should develop means of understanding the types of signatory that they interact with, or are likely to interact with. The needs of such signatories should be taken into account when building any customer onboarding processes or implementing policies in relation to the signing of documents.
    iv. If signatories are required to use a specific technology platform, parties should consult with the provider about the full range of accessibility features available. This information should then be passed on to those signatories in a clear and accessible form. By way of example, any documentation should be visible in all formats and on tablets and mobiles of all sizes.
    v. All parties should have the ability to reject documentation in a straightforward and user-friendly way. It may also be appropriate to consider placing an expiry date on the document so that positive action does not have to be taken by the signatory in order to reject it.
    vi. All parties should ensure that they all receive a copy of the executed agreement and give due consideration to how an individual may wish to receive this copy.

This is particularly important when contracting with vulnerable individuals who may find it difficult to organise their affairs because of issues with their memory, health, or technical capability.

vii. Free resources are made available by charities such as AbilityNet[73] or the Royal National Institute for Blind People[74] to understand the specific needs of signatories with vulnerabilities.

viii. Consideration should be given to the Web Content Accessibility Guidelines (WCAG 2.1)[75] when building any website or online customer journey.

ix. Consideration should be given to the fact that individuals may not 'self-identify' as vulnerable. Even if they have not been previously defined as vulnerable, this could change because of their personal circumstances at any time.

---

73 AbilityNet, 'Free Resources' <https://abilitynet.org.uk/free-resources> accessed 7 October 2021

74 Royal National Institute for Blind People, 'Services for Businesses' https://www.rnib.org.uk/services-for-businesses, accessed 7 October 2021.

75 World Wide Web Consortium (W3C), 'Web Content Accessibility Guidelines (WCAG) 2.1' (5 June 2018) <https://www.w3.org/TR/WCAG21/> accessed 7 October 2021

Recommendations for further analysis, development and reform

a. Legal

165. In considering the practical and technical aspects of the electronic execution of documents, the Group has identified areas in which law reform might not only facilitate, but also benefit from, an increased use of electronic signatures. As outlined at the beginning, one of the Group's principal conclusions is that both legal reforms and technological advances will be far more effective if they are developed alongside one another.

166. For example, one of the questions that emerged from the Law Commission's Consultation Paper on Electronic Execution of Documents[76] was whether the continued requirement of physical witnessing and attestation for the execution of deeds was preventing the widespread use of electronic signatures for that purpose. The Law Commission Report which followed, containing an analysis of the responses to that Consultation Paper, concluded that the need for law reform to change or remove those requirements had not at that stage been made out. In part, this was because it was not clear how many of the obstacles to adopting electronic signatures were logistical and how many were legal, or whether available technologies were capable of fulfilling the same legal objectives as physical witnessing. This was the basis on which the Industry Working Group was formed.

167. Having considered the legal and technological possibilities in tandem, the Group has concluded that Qualified Electronic Signatures, particularly if underpinned by a regulated digital identities trust framework, such as that proposed by DCMS, are capable of fulfilling the same objectives as physical witnessing and attestation. Since the process of obtaining a QES involves the parties identifying themselves to the satisfaction of the Certificate Provider, this provides a means of linking the identity of the signatory to a signature. Given the complete electronic audit trail that signature platforms are now able to provide for each signature, there is also an argument to be made that a QES is likely to be *more* reliable than a signature witnessed in an unsupervised environment.[77]

---

[76] Electronic Execution of Documents (2018) Law Commission Consultation Paper No 237 (CP 237), https://www.lawcom.gov.uk/project/electronic-execution-of-documents/.

[77] See section "Current technological capabilities".

168. In its Report, the Law Commission used the following criteria to test any prospective reform of the formalities required for the execution of deeds:[78]
    a. Evidential: providing evidence that the maker entered into the transaction, and evidence of its terms
    b. Cautionary: trying to ensure that the maker does not enter into the transaction without realising what they are doing and protecting weaker parties to a transaction (for example, tenants, employees and consumers)
    c. Labelling: making it apparent to third parties what kind of a document it is and what its effect is to be.

169. The Group considered the extent to which the current requirements for the execution of deeds achieve, or materially contribute to the achievement of, these three objectives.

170. If, as the Law Commission recognises, the "labelling" function is now fulfilled by section 1(2)(a) of the Law of Property (Miscellaneous) Provisions Act 1989,[79] it is hard to see why this section does not also sufficiently fulfil the "cautionary" function (i.e. ensuring that people do not enter into transactions without realising what they are doing). If the requirements for writing to be used, and for that writing to be clear on its face that it is a deed, are sufficient to indicate the nature and effect of the document to a third party, they should indicate at least the same to the signatory. It is unlikely that a party will fail to appreciate that a signature on a formal document describing itself as a deed is intended to have legal consequences. It may therefore be that, given the way that technology is now available to be used in the way identified in this report, that the “cautionary” function is also either satisfied or no longer properly considered to be discrete.

171. With regard to the "evidential" and "protective" functions, it is important to appreciate that the role of the witness in attesting a signature is very limited. Whilst witnessing and attestation have the aim of reducing the risk of signatories being subject to duress, and of documents being forged or fraudulently executed, they play only a minor role in this regard:

    “It is also important to be realistic and practical about the level of protection a witness may provide. Undue influence and duress are more likely to take the form of a sustained campaign, which the witnessing requirement cannot protect against, rather than a one-off “gun to the head” scenario. Even in that extreme situation, the requirement for a coerced signature to be witnessed presents only a minimal impediment to the person holding the gun. Indeed, depending on the transaction, that person may act as the witness themselves. Similarly, in general, witnessing will not provide complete protection against fraud and forgery because there is no legal

---

78 *Electronic Execution of Documents*, Law Com No 386 (2019), para 2.11.

79 As recognised in *Electronic Execution of Documents, Consultation Paper*, Law Commission, CP No 237 (2018), paras 2.6 and 4.40

requirement that a witness must be independent. Nor is there a requirement that the witness must know or be able to identify the signatory."[80]

172. Currently, a witness need not be independent, need not read the document, need not know the signatory, need not take steps to identify the signatory, and does not even vouch for the identity of the signatory.[81] It is difficult to see therefore what extra protections can be provided by someone witnessing someone's signature if they do not necessarily provide any of these protections. A witness does not take on the role and responsibilities of a notary, nor is it reasonable to impose such obligations on a lay person in any event. Few people invited to witness a signature on a deed would understand that, by agreeing to do so, they were taking on significant legal responsibilities and, if they did understand, few would be prepared to take on the role. Even if a lay person were prepared to take on the role, the lack of any rigour or professional supervision would render the exercise of questionable value.

173. In practice a witness is unlikely to be a complete stranger to the transaction or to at least one of the parties to a deed but, in theory, the minimum that a witness does by attesting another's signature is to confirm that the witness saw someone, whom the witness may or may not be able to identify at a later date,[82] sign the document that the witness also signed by way of attestation. This method of witnessing provides a single document containing the terms of the deed on which the witness will hopefully recognise their signature. That document is also intended to trigger a recollection as to the identity of the party who actually executed the deed and the circumstances surrounding that execution.

174. Even were the witness not in fact to observe the execution of the deed despite attesting the signature, the signatory may be unable to challenge the validity of the deed on that basis if the deed appears on its face to have been validly executed.[83]

175. In these circumstances, the witnessing and attestation requirements for deeds do not, in our view, fulfil the functions identified by the Law Commission to any greater extent than would a process that were based on QES, combined with robust and secure digital identity provision. The evidence that witnessing and attestation offers will not in most cases be materially better than a requirement for writing alone, and securing a witness who will offer no protection to a signatory in need of protection is unlikely to be difficult. Significantly, in a comparative international context, the need for physical witnessing and attestation makes English law somewhat anomalous and may well soon come to discourage and impede its use. Few jurisdictions impose similar requirements to those under English law, and this jurisdictional discrepancy is set only to increase as more documents are executed electronically.

---

80 *Electronic Execution of Documents, Consultation Paper*, Law Commission, CP No 237 (2018), para 8.22.
81 *Electronic Execution of Documents*, Law Commission, Law Com No 386 (2019), para 5.15.
82 Subject to all the normal problems of recollection and identification, particularly with the passing of time.
83 *Shah v Shah* [2002] QB 35 and *Re Gleeds Retirement Benefits Scheme* [2015] Ch 212.

176. This is not to say that particular types of documents executed by specific categories of person should not attract bespoke protections. For example, paragraph 2(1)(e) of Schedule 1 to the Mental Capacity Act 2005 requires a certificate on a lasting power of attorney by a person of a prescribed description that, amongst other things, at the time of execution of the power the donor understood the purpose of the instrument and that no fraud or undue pressure was applied to the donor.[84] In a similar protective vein, the Consumer Credit Act 1974 includes a 14 day "cooling off" period after signature on certain transactions during which a consumer can withdraw from the transaction. Whatever protections might be required for specific parties or specific kinds of documents, however, they do not arise from the mere fact of that document being a deed.

177. Additionally, the Covid-19 pandemic has catapulted society ahead in terms of the realisation that physical presence is no longer strictly necessary. As a single example, the use of remote appearances of not only defendants but also counsel in certain instances in the criminal courts, is something that was technically possible prior to 2020 but not adopted. The Working Group has concluded that there is no reason why video witnessing of signatures is something that should not be widely adopted or legally permitted, although primary legislation will be required in order to facilitate this.

b. Technological

178. There are several technological developments, identified by the Group, that would significantly advance and expand the adoption of electronic execution methods:
    - The creation of a cross-border database of permissible regulatory and execution modes for all major countries worldwide. It would be particularly helpful for this database to have easy look-up capabilities at summary level, plus links to underlying sources/documentation. This could start with major trading partners and over time (and use) expand to an increased number of jurisdictions. Such a database might be maintained by BEIS or another government entity, a legal research publisher or a not-for-profit industry organisation offering subscription access.

---

[84] Because a lasting power of attorney must be a deed, in addition to the certificate by the prescribed person the signatures of the donor and the attorney must be witnessed and attested. In its consultation paper *Modernising Lasting Powers of Attorney* (July 2021, CP 485), the Ministry of Justice reports that the dual requirement of witnessing and a certificate can cause confusion and expresses scepticism as to the benefit of witnessing and attestation independently of the certification requirement (para 70ff). The Ministry of Justice's preferred approach is to look for "objective evidence-based approaches to verifying that the parties executed the LPA" (para 101).

- The formulation of protections against misuse of biometric data (further than GDPR, its rights of redress and actions post-breach) in order to reduce the risk of lasting impacts for compromised persons.
- Increased use of tokens for federated identity, so that only those elements of identity that a user chooses to share with any entity and for specified purposes, will be shared at any one time, thereby maintaining user control. To this end, we should explore linkages with European Digital Identity (eID), including their Wallets technical framework (EDIW) once available (2022).
- The use of Distributed Ledger Technology for storage of finalised transactions and recognition records in the case of legal dispute.
- Integrated platforms (combining video, document creation, eSignatures, identity capture and validation) and their position within legal frameworks, especially for formalities requiring witnessing.
- The use of standards-based activities for everything from wet signatures to QES cryptographic approaches, including how a federated platform might use those standards for sharing via APIs, thereby encouraging further innovation without the barrier of legal non-acceptance.
- Increased collaboration and co-operation between groups working in the same space (e.g. Biometrics Institute,[85] OIX,[86] DCMS, Law Commission, UKAS,[87] etc.).

c. Other Initiatives

179. A more widespread use and acceptance of QES is likely to increase users' confidence in the execution of documents by electronic signature. The provision of accessible, user-friendly and non-commercial guidance that makes the legislative requirements for QES clearer and provides potential users with advice on the services available could be one way of achieving this. The Open Identity Exchange is a useful example of the type of resource that could be effective in this context.[88]

180. The success of document execution by means of electronic signature depends in no small way on the ability of signatories to create a robust and trustworthy digital identity. The Department for Culture, Media and Sport's ongoing work on establishing a Digital Identity and Attributes Trust Framework is a valuable example of how this could be done. It aims to build a "trust framework", with a view to

---

85 https://www.biometricsinstitute.org/

86 See above, fn 12.

87 See above, fn 40.

88 https://openidentityexchange.org/members/anon/new.html?destination=%2Findex.html. OIX describes itself as "a community for all those involved in the ID sector to connect and collaborate, developing the guidance needed for inter-operable, trusted identities Through our definition of, and education on Trust Frameworks, we create the rules, tools and confidence that will allow every individual a trusted, universally accepted, identity".

providing a "trust mark" to data-handling organisations that follow the rules of that framework. This allows data-handling organisations to show that they have been recognised as having robust processes, thereby enabling users to have confidence in trusting their digital identity to them.[89]

181. Ultimately, the setting of market standards for the use of electronic signatures is likely to have a significant effect in encouraging and facilitating that use. Currently, both HMLR's *Practice Guide on the execution of deeds*[90] and the *Ministry of Justice's Modernising Lasting Powers of Attorney (MLPA) project*[91] demonstrate what this could look like and how it might work.

182. The use of smart contracts is increasingly widespread. This means that both the formation and execution of a growing number of contracts will be automated and performed by computers. Such a process often necessitates the use of electronic signatures. In its *Advice to Government: Smart Contracts*,[92] the Law Commission has made it clear that electronic signatures are in principle a valid means of executing an automated agreement (subject to extrinsic formality requirements). In a similar vein, LawtechUK's *Smarter Contracts* project[93] sets out a series of smart contract use cases, with a view to providing concrete examples of how the process will work in practice in a variety of settings, from international trade documents to conveyancing. As automated agreements become more commonplace, and users become more familiar with them, the use of electronic signatures will inevitably increase.

183. It is important that as many Government documents as possible (such as Lasting Powers of Attorney and wills) can be executed electronically. Otherwise, there is a danger of piecemeal adoption of available technologies across different elements of society. A very ill person who wishes another trusted person (whether a relative or not) to assume conduct of their affairs could be said to require the speed and convenience of electronic execution more than most; it is contradictory that these cannot currently be signed electronically. Widespread adoption across the different categories and types of documents used in citizens' interaction with the authorities will encourage, and expand, the use of electronic signatures.

---

89 The framework is currently in alpha (prototype) format, so as to invite further feedback from private users, government and industry.

90 Practice Guide 8

91 https://sites.google.com/digital.justice.gov.uk/opgmlpa/home

92 Smart contracts | Law Commission 2021

93 https://lawtechuk.io/explore/smarter-contracts.

d. Accreditation/Kitemarking

184. The Group did not agree that this should be adopted or recommended. There was a wide range of very different views. Those in favour felt that it would give some external validation to the individual platforms, as well as potential credibility for smaller enterprises that might wish to attempt to break into the market. There are also examples of providers of computer services being entirely confident publicly of the performance of their systems, where the reality is less so. Those in opposition included those opposed in principle, as well as those who observed that providing the necessary access to code in order for this to be accomplished could undermine intellectual property rights. Some were of the view that the level of bureaucracy and oversight required would make such a system impracticable in any event.

185. Given this different range of views and lack of agreement, the Group cannot make a positive recommendation in this respect. The pros and cons are complex, and the potential for wider consultation means that all the Group can do at this Interim stage is to record this as an issue that has been widely debated within the membership. Whether those at a political level wish to conduct a consultation on this, or impose it, is a matter outside the scope of this Group.

Appendices

Appendix 1 – Group biographies

Catherine Goodman: Catherine Goodman has 20 years' legal experience, working as a corporate solicitor, business law lecturer and professional support lawyer. In her current role at Paul Hastings, as Lead Practice Innovation & Knowledge Counsel for Europe and Asia, Catherine runs legal tech projects for all practice groups, optimising legal processes with innovative technology solutions.

Simon James: Simon James is a solicitor and a partner in the Litigation and Dispute Resolution Group of Clifford Chance LLP in London.

John Jolliffe: John Jolliffe is the Adobe program lead for International Identity at Adobe, where he promotes the benefits of strong identity-backed electronic and digital signatures to customers, partners and governments across the world, and is responsible for building the network of trust service providers and identity providers who make their identity solutions available in Adobe Sign.

Chris Jones: Chris Jones is the Founder/MD of Icon UK, a consulting-led Software Integrator specialising in helping organisations implement solutions to digitize, complete and automate documents electronically. These drive productivity, identity assurance, compliance and growth – assisting customers' new services and delivery methods. His previous roles include CEO of a number of software services providers, benchmarking and consulting companies following roles with global outsourcer Perot Systems, Easams (GEC) and IBM, each helping customers digitally transform their business processes.

Simon Law: Simon Law is a Director and Head of Legal Practice for DC Law and JS Law both companies are part of the Simplify Group. Simon has over 20 years extensive experience working in the legal profession having worked for large and small firms. Simon is also the current chairperson of the Society of Licensed Conveyancers (the professional body for Licensed Conveyancers) having held the position previously from 2012 – 2018.

Michael Lightowler LL.B, FANZCN: Michael Lightowler retired from full time practice as a solicitor specialising in company and commercial law in 2010. He qualified as a Notary Public in 1990 and continued to practice from his office, based in Essex. He is a member of the Council of The Notaries Society and a former President. He also sits on the Board which advises regulators on policy and practical issues. He has developed a keen interest in steering the Notarial profession towards adopting digital methods of working, about which he has written a number of articles and given several presentations both in the UK

and overseas. For some years he has been working with government, stakeholders and industry in developing and testing digital tools, the aim of which has been to enable the profession to offer electronic services alongside the more traditional methods.

Eoin O'Reilly: Eoin O'Reilly is Director of Legal for Product at Monzo Bank. He is a Fintech lawyer and former Head of Legal & Compliance at SME lender MarketFinance.

Charlotte Ponder: Charlotte Ponder is the Legal Director for Countrywide Tax & Trust Corporation Ltd. She oversees the day-to-day operations supporting advisers offering estate planning services to their customers. She is heavily involved in the continued development of drafting and case management software, Countrywide Legacy. She regularly speaks at industry events and presented at the Law Society's Elderly Customer Conference in 2019. In December 2019 she became a Trustee for Age UK Coventry and Warwickshire and was elected Vice Chair of the charity in April 2021.

Jonathon Read: Jonathon Read has a variety of interests, including the provision of consulting and advisory services in the fields of law and business. He founded and chaired a mutually-owned financial services company after working in investment banking for many years. He combines his business interests with non-executive board positions, academic appointments, charitable work and has previously held elected office. He is called to the Bar of England & Wales.

Neil Singer: Neil Singer is a tech-focused property professional, member of the Royal Institution of Chartered Surveyors. Founder of Singer Vielle (investment agency) and the clicktopurchase online legal execution platform (blockchain powered). He has worked within the commercial property industry for over 35 years, moving into technology in 2006.

Quintus Travis: Quintus Travis has extensive experience of developing new technologies. He co-founded an optics company that Microsoft acquired in 2007 and spent 8 years in Redmond with Microsoft's Applied Sciences, an applied research and development team dedicated to creating the next generation of computer interaction technologies. Quintus holds an Economics degree from Cambridge and an MBA with distinction from Harvard Business School.

Elizabeth Wall: Elizabeth Wall is Head of Know-How for the Global Corporate practice at Allen & Overy and has extensive experience of mergers, acquisitions and other corporate finance transactions. She chaired the Company Law Committee of the Law Society of England and Wales from 2015 to 2019 and remains an active committee member. Elizabeth is an expert in the law and market practice relating to electronic signatures, and in 2016 chaired the joint Law Society and City of London Law Society working group that produced guidance on execution of a document using an electronic signature.

Appendix 2 – Glossary

AES	Advanced Electronic Signature
AgID	Agenda per l'Italia Digitale
AML	Anti-money laundering
API	Application Programming Interface
AI	Artificial Intelligence
CA	Certificate Authority
CCA 1974	Consumer Credit Act 1974
CP	Certificate Provider
CRL	Certificate Revocation List
CRM	Customer relationship management
BEIS	Department for Business, Energy & Industrial Strategy
DCMS	Department for Digital, Culture, Media & Sport
DLT	Distributed Ledger Technology
EDIW	Education for an interdependent world
eIDAS	Electronic Identification, Authentication, and Trust Services
eID	European Digital Identity
EU	European Union
GDPR	General Data Protection Regulation
HCCM	Hague Conference on Private International Law
HMLR/HM Land Registry	Her Majesty's Land Registry
HSM	Hardware Security Module
HTML	Hypertext Markup Language
ICO	Information Commissioner's Office
ID	Identity document
IP	Internet Protocol
ISO	International Organization for Standardization
IWG	Industry Working Group
JPEG	Joint Photographic Experts Group
KYC	Know Your Client

LPA	Lasting Powers of Attorney
LPMPA 1989	Law of Property (Miscellaneous Provisions) Act 1989
LRA 2002	Land Registration Act 2002
MLPA	Modernising Lasting Powers of Attorney
mTAN	Mobile transaction authentication number
OCSP	Online certificate status profile
OIX	Open Identity Exchange
OPG	Office of the Public Guardian
OTP	One Time Password
PAdES	PDF Advanced Electronic Signatures
PC	Personal Computer
PDF	Portable Document Format
PIN	Personal identification number
PKI	Public Key Infrastructure
PP	Protection Profile
PSD2	Payment Services Directive Two
QC	Qualified Certificate
QES	Qualified Electronic Signature
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trust Service Provider
RES	Remote eSigning Platform
RFID	Radio-Frequency Identification
SaaS	Software as a Service
SES	Standard electronic signature
SME	Small and Medium-Sized Enterprises
SMS	Short Message Service
SSL	Secure Sockets Layer
SSO	SingleSign-on
SWIFT	Society for Worldwide Interbank Financial Telecommunications
UK	United Kingdom

UKAS	United Kingdom Accreditation Service
USB	Universal Serial Bus
UV	Ultraviolet
VRI	Validation-related Information
WCAG	Web Content Accessibility Guidelines
2Fa	Two-factor authentication
3D	Three-dimensional

Appendix 3 – Table of electronic execution requirements for common document types

Document Type	Electronic Execution Requirements
Simple contracts	An electronic signature is capable in law of being used to execute a simple contract, provided that • by signing the contract, the signatory intends to authenticate the document and • any formalities relating to execution of that document are satisfied. Currently, any form of eSignature can be used for eSigning simple contracts, including: • a simple signature • a stylus-based signature • a digital signature (so an AES or QES), • a scanned manuscript signature, • the typing of a name, for example, at the end of an email, and • clicking on a website button. All satisfy the objective test of authenticating intention set out in the 2001 Law Commission Advice on Electronic Commerce. Under Article 25(1) of UK eIDAS, an electronic signature cannot be denied legal effect (either in terms of legal validity or admissibility as evidence) solely because of its electronic nature. Both UK eIDAS (Article 3(10)) and the Electronic Communications Act 2000 (section 7(2)), define an electronic signature broadly to include any data in electronic form which is attached to or logically associated with other electronic data and which is used by the signatory to sign.

Document Type	Electronic Execution Requirements
Deeds	An electronic signature is capable in law of being used to execute a simple contract, provided that • by signing the contract, the signatory intends to authenticate the document and • any formalities relating to execution of that document are satisfied. In terms of formalities, deeds must be: • Signed • Attested by a witness: Point 8 in Law Commission Executive Summary (above) states that the witness must be physically present in the same location as the signor if this requirement is to be met. A temporary amendment to the Wills Act 1837 was introduced to permit virtual witnessing of wills only (wills being a type of deed). The temporary amendment to the Wills Act 1837 permitting virtual witnessing of wills is due to expire on 1 February 2024.[94] • Delivered: i.e. the maker of the deed intends it to become effective and binding. There is a presumption of delivery on execution in the case of corporations but not individuals. Currently, many forms of eSignature can be used for eSigning deeds, including: • a digital signature (so an AES or QES), • a scanned manuscript signature, • the typing of a name, for example, at the end of an email, and • clicking on a website button. All satisfy the objective test of authenticating intention set out in the 2001 Law Commission Advice on Electronic Commerce.

[94] The statutory instrument was laid before Parliament on 11 January 2022, to come into force on 1 February 2022.

Document Type	Electronic Execution Requirements
Real Estate contracts	Real estate contracts, including deeds, can be eSigned, so the formalities above apply. *Additional* requirements for deeds purporting to transfer an interest in land are however set out in HMLR Practice Guide 8, section 13: 1. All the parties agree to the use of electronic signatures and a platform in relation to the deed. 2. All the parties have conveyancers acting for them, except that only the lender in the case of a mortgage, discharge or release, the personal representatives in the case of an assent and the donor in the case of a power of attorney need have conveyancers acting for them. If any party is unrepresented (other than in the situations just outlined), including a party who is not signing themselves, electronic signatures cannot be used by any of the parties involved. Where a deed is to be signed electronically by a party's attorney, and the deed is one other than the power of attorney itself, a conveyancer must be acting in respect of the execution, but it does not matter for the purposes of these requirements whether the conveyancer was instructed by the party or by the attorney. 3. A conveyancer is responsible for setting up and controlling the signing process through the platform. The signing and dating process is as follows. **STEP 1** – The conveyancer controlling the signing process: • uploads the final agreed copy of the deed (including any plans) to the platform • populates the platform with the name, email address and mobile phone number of the signatories and the witnesses. Where the platform allows, the details for a witness can be populated later, either by the signatory entering the details for their witness or the conveyancer doing so, provided this is done before STEP 5 • highlights the fields that need completing within the deed and indicates by whom they are to be completed, setting out the order (so the witness is after the signatory whose signing they are witnessing). **STEP 2** – The platform emails the signatories to let them know the deed is ready to sign.

Document Type	Electronic Execution Requirements
	STEP 3 – To access the deed on the platform via the email they have received, the signatories are required to input an OTP sent to them by text message by the platform. The OTP must contain a minimum of six numbers. **STEP 4** – The signatories enter the OTP and sign the deed in the physical presence of the witness, with the date and time being automatically recorded within the platform's audit trail. **STEP 5** – Once the signatory has signed the deed, the witness will receive an email from the platform inviting them to sign and add their details in the space provided in the attestation clause. The witness inputs an OTP sent to them by text message by the platform, signs and adds their address in the space provided, with the date and time being automatically recorded again. **STEP 6** – Once the signing process has been concluded, the conveyancer controlling the signing process or another conveyancer acting for one of the parties dates the deed within the platform with the date it took effect. (There will be a gap between this step and the previous one if, as will often be the case, the deed is signed by all the signatories and witnesses some time in advance of completion.) 5. The conveyancer who lodges the application does so by electronic means and includes with the application a PDF of the completed deed. However, where the application is for first registration, a print out of the PDF, certified to be a true copy of the original deed, can be lodged. 6. The conveyancer lodging the application (including an application for first registration) includes a certificate (not necessarily signed by them: see below) in the following form: "I certify that, to the best of my knowledge and belief, the requirements set out in practice guide 8 for the execution of deeds using electronic signatures have been satisfied." The certificate needs to be dated and signed by an individual conveyancer, their full name and firm must be added and the deed or deeds for which the certificate is given must be specified. This certificate will be read by HM Land Registry as referring to the requirements as they were on the relevant date. This means that if, for example, the requirements in respect of the signing process change

Document Type	Electronic Execution Requirements
	but the signing process has been completed before the date on which the requirements changed, the certificate will be read as referring to those particular requirements as they were before the change. The certificate can be given by any party's conveyancer who has satisfied themselves that the deed has been duly executed. In most cases involving transfers, the conveyancer controlling the signing process will be the seller's conveyancer and the conveyancer lodging the application will be the buyer's conveyancer. The certificate might then be signed by the seller's conveyancer and passed on to the buyer's conveyancer; alternatively, the buyer's conveyancer, having been satisfied on completion that the deed was duly executed, might sign the certificate, bearing in mind its qualified terms. A conveyancer is not precluded from giving the certificate because they have signed the deed themselves on behalf of a party, acting under a power of attorney. The registrar will rely on the conveyancer's certificate lodged with the application. Any audit report or certificate of completion issued by the platform must not be lodged with the application but should be retained. It may contain personal data and would be open to public inspection.
Special contracts	If a registry only accepts "wet ink" signatures, then the parties will not be able to execute documents electronically, regardless of the technical legal position. For instance, there are several "additional safeguards" required by the Office of the Public Guardian before e-execution can be considered in relation to Lasting Powers of Attorney (LPA): • For an LPA that names one attorney and one replacement attorney, there are nine signatures and six people needed to execute the document. These include a witness for the donor and attorneys and a certificate provider (CP). • There is also a specific signing order that is required. The donor signs first, followed by their witness. Then the CP signs. Then, finally, the attorneys sign followed by their witnesses. Failures to comply with this sequencing will result in the LPA being returned for re-execution

Document Type	Electronic Execution Requirements
	• An LPA must be executed (signed and witnessed) and registered on paper. This is so it meets the requirements of the Mental Capacity Act 2005. Although OPG introduced a digital tool in 2013 to help people fill in the LPA form, the final stages of the process must still be completed on paper. On this, however, see The Ministry of Justice's *Modernising Lasting Powers of Attorney (MLPA)* project,[95] aiming to bring the execution of LPAs into line with contemporary technological processes. This means that as at the date of this report, it is intended to change the current position, but that this has not yet occurred.
Smart Contracts	A smart legal contract is a legally binding contract in which some or all of the contractual obligations are defined in and/or performed automatically by a computer program. Smart contracts, including smart legal contracts, tend to follow a conditional logic with specific and objective inputs: if "X" occurs, then execute step "Y". There are essentially three forms a smart legal contract can take, depending on the role played by the code. These are: **Natural language contract with automated performance** A contract in which all of the terms are recorded in natural language, either orally or in writing, and only performed through the execution of a coded computer program. **Hybrid contract** A smart legal contract, some terms of which are defined in natural language and other terms of which are defined in the code of a computer program. Some or all of the contractual obligations are performed automatically by the code. In addition, the same contractual term(s) can be written in both natural language and in code.

95 https://sites.google.com/digital.justice.gov.uk/opgmlpa/home

Document Type	Electronic Execution Requirements
	Solely code contract A smart legal contract in which all of the contractual terms are defined in, and performed automatically by, the code of a computer program. Where a smart legal contract takes the form of a natural language agreement which is performed by code, the question of whether the contract has been "signed" can be answered in the traditional way. The court would consider whether the parties had indicated an intention to authenticate the natural language agreement by signing it by hand or electronically. In the case of a hybrid agreement, the signing of the natural language component of the agreement may be sufficient to authenticate the coded terms. Where parties sign a natural language document which refers to and explains the effect of the coded terms, the parties could be taken to have authenticated the coded terms. Where a smart legal contract consists solely of code, the potentially novel question arises as to how the parties can "sign" the code. In the context of code deployed on a DLT system, parties can sign a piece of code by applying their digital signature to the relevant coded transaction. In its 2021 Report, *Smart Legal Contracts: Advice to Government*, the Law Commission stated that "the private key and digital signature must be used in a manner which indicates the parties' intention to authenticate the document.[96] However, this does not change the conclusion that a digital signature is capable of fulfilling a requirement for a signature in principle".[97]

[96] *Golden Ocean Group Ltd v Salgaocar Mining Industries PVT Ltd* [2012] EWCA Civ 265, [2012] 1 WLR 3674 at [32] by Tomlinson LJ; UKJT Legal Statement at [160].

[97] Smart contracts | Law Commission, 2021.

Appendix 4 – Table of formalities for common types of transaction

Type of transaction	Formality requirement
Guarantee agreement	Writing, or evidenced by writing, and signed by the guarantor or a person authorised by the guarantor. (Statute of Frauds 1677, s4)
Transfers of registered securities under the Stock Transfer Act 1963	Made "under hand" (that is, in writing otherwise than by deed) in the form set out in Schedule 1 to the Stock Transfer Act 1963.
Contract for the sale of land	In writing and signed, incorporating all the terms which the parties have expressly agreed in one document or, where contracts are exchanged, in each document. (Law of Property (Miscellaneous Provisions) Act 1989 (LPMPA 1989), s2)
Regulated credit agreement under the Consumer Credit Act 1974	In writing in a prescribed form, including information such as the remedies available under the Act to the consumer. (Consumer Credit Act 1974 (CCA 1974), ss60-61, 88 and SIs)
A unilateral promise	Executed as a deed.
Lasting power of attorney	Executed as a deed, in a prescribed form. Includes prescribed information as to the purpose and effect of the instrument. Also includes a certificate by a third party who confirms that the grantor of the power understands the purpose and scope of the document and that no fraud or undue pressure is being used to induce them. (Mental Capacity Act 2005, s9 and sch 1, Lasting Powers of Attorney and Public Guardian Regs 2007, SI 2007 No 1253).

Appendix 5 Best Practice Guidance Table – Commercial Transactions

Method/type of Electronic Signature	Risk Profile	Best Practice
Qualified electronic signature (QES) (as defined in the eIDAS Regulation as it forms part of retained EU law)	An electronic signature is only classed as qualified if it meets the requirements set out in the eIDAS Regulation. The eIDAS Regulation provides a requisite standard for the signatory identification process and the security and reliability of the technology. This requires the use of a digital signature based on public key infrastructure (PKI) which will only be issued once the Qualified Trust Service Provider has verified the identity of the signatory using a process that meets the requirements of the eIDAS Regulation. QES are not commonly used in England and Wales for commercial transactions, largely because of the complexity of the process involved, and the fact that simple electronic signatures are valid under English law.	• Ensure that the parties agree to the use of a qualified electronic signature platform in advance. • Check that the proposed platform meets the requirements set out in the eIDAS Regulation for a "qualified electronic signature creation device" and that the electronic signature will be based on a "qualified certificate for electronic signatures". • Check that the individuals signing the agreement are citizens of jurisdictions that the relevant trust service provider can verify the identity of in accordance with the eIDAS Regulation (e.g., using electronic identification). • Ensure that the parties consent to using a cloud-based platform. • Check whether the platform meets the parties' information security standards. • Ensure that the parties are comfortable with the proposed identification procedure (e.g., participating in a video call) and are made aware of how their personal data will be handled. • Agree in advance what will comprise the "originals" of the documents. • Agree in advance whether any law firm(s) representing the parties will approve the documents on the platform before they are signed.

Method/type of Electronic Signature	Risk Profile	Best Practice
		• Agree in advance whether the signing platform will automatically date the document or if the individual or organisation co-ordinating the signing will do this at the appropriate time. • Use an electronic signature validation tool to ensure that the signatories' signing certificates are valid. • Obtain and save a copy of the validation, the full audit trail and completion certificate provided by the electronic signature platform in relation to the execution process. • Download and save a tamper-proof PDF of the final signed and dated document. • Parties should agree how data will be managed – e.g., documents to be uploaded just before signing and then deleted from the platform once every party has downloaded their electronic original.
Advanced electronic signature (AES) (as defined in the eIDAS Regulation as it forms part of retained EU law)	An electronic signature is only classed as advanced if it meets the requirements set out in the eIDAS Regulation. This requires the use of a digital signature based on public key infrastructure (PKI) which will only be issued once the identity of the signatory has been verified using a process that meets the requirements of the eIDAS Regulation.	• Ensure that the parties agree to the use of an advanced electronic signature platform in advance. • Check that the proposed platform meets the requirements set out in the eIDAS Regulation for an advanced electronic signature. • Check that the proposed identification process meets the requirements set out in the eIDAS Regulation. • Ensure that the parties consent to using a cloud-based platform.

Method/type of Electronic Signature	Risk Profile	Best Practice
	AES are not commonly used in England and Wales for commercial transactions, largely because simple electronic signatures are valid under English law.	• Check whether the platform meets the parties' information security standards. • Ensure that the parties are comfortable with the proposed identification procedure (e.g., providing their photo identification) and are made aware of how their personal data will be handled. • Agree in advance what will comprise the "originals" of the documents. • Agree in advance whether any law firm(s) representing the parties will approve the documents on the platform before they are signed. • Agree in advance whether the signing platform will automatically date the document or if the individual or organisation co-ordinating the signing will do this at the appropriate time. • Use an electronic signature validation tool to ensure that the signatories' signing certificates are valid. • Obtain and save a copy of the validation, the full audit trail and completion certificate provided by the electronic signature platform in relation to the execution process. • Download and save a tamper-proof PDF of the final signed and dated document. • Parties should agree how data will be managed – e.g., documents to be uploaded just before signing and then deleted from the platform once every party has downloaded their electronic original.

Method/type of Electronic Signature	Risk Profile	Best Practice
Web-based electronic signature platform using a simple electronic signature	Simple electronic signatures do not need to meet a particular standard, but most signing platforms contain several features that enable the creation of an audit record that provides clear evidence linking the signatory to the electronic signature. These vary from platform to platform but can include: recording the IP addresses of signatories; geolocation; verification of email accounts; and the use of one-time passcodes or PINs. Documents uploaded to the platform for signing are held in an encrypted state and then, once signed, a tamper-evident pdf is generated, offering higher security levels than email signing.	• Ensure that the parties agree to the use of an electronic signature platform in advance. • Ensure that the parties consent to using a cloud-based platform. • Check whether the platform meets the parties' information security standards. • Agree in advance what will comprise the "originals" of the documents. • Agree in advance whether any law firm(s) representing the parties will approve the documents on the platform before they are signed. • Use SMS authentication features built into the electronic signature platform for all signatories (and witnesses). SMS authentication involves sending documents to an individual's business email address and then requiring the person who accesses that email to input a unique, automatically generated PIN, sent to the signatory's mobile telephone. This limits the chance that a person other than the signatory will access and sign the document: whoever signed the document must have had access to the signatory's business email address and a mobile telephone personal to that signatory. This safeguard is recorded in the audit trail which then provides valuable evidence to dispute an allegation that a document was not signed by the person who purported to sign it. • Agree in advance whether the signing platform will automatically date the document or if the individual or

Method/type of Electronic Signature	Risk Profile	Best Practice
		organisation co-ordinating the signing will do this at the appropriate time. • Obtain and save a copy of the full audit trail and completion certificate provided by the electronic signature platform in relation to the execution process. This tracks and records when and where a document is signed, and includes IP addresses used to access the document, and any changes to the signing process or signatories once the process is underway. • The completion certificate and audit trail should be reviewed by the individual or organisation co-ordinating the signing for consistency with the agreed signing process. • Download and save a tamper-proof PDF of the final signed and dated document. • Parties should agree how data will be managed – e.g., documents to be uploaded just before signing and then deleted from the platform once every party has downloaded their electronic original.
Signing on screen using a touch screen or stylus	These methods have the benefit that the signatory readily understands the significance and use of the signing act. Signing using a stylus or finger on a touch screen may make a basic image of a signatory's mark/signature or may be biometric (if using appropriate software and device). As a basic image this is a	• Ensure that the parties agree to the use of this form of electronic signing in advance. It is also important to identify or decide whether the signature is: (a) a basic image drawn (i.e. X-Y co-ordinates of the stylus path shown and a little metadata recorded), i.e. non-biometric (b) a full biometric where multiple types of data are recorded via a digital stylus and/or screen at least a dozen times per

Method/type of Electronic Signature	Risk Profile	Best Practice
	SES, whereas a biometric signature may be SES, AES or QES – since the stylus/software may provide additional data and metadata that aids the evidential link to the signatory (more strongly than traditional forensic handwriting methods). Under the eIDAS Regulation, biometric signatures can provide a robust method for signatory identification with high reliability when using compliant technology. There are, however, differences between vendors, and professional advice may be needed to ensure that the hardware/software mix is correctly deployed with appropriate security protocols in place. This includes both specialist eSigning devices and general purpose equipment (e.g. smartphone or tablet). These are used more widely in Europe and are valid in the UK as described in this report.	second for each data vector and using at least 128 variable pressure levels, with rich metadata also recorded (c) a less sophisticated form of biometric signature, such as a finger drawn biometric signature on a less sensitive device without full biometric data recording. • Agree in advance what will comprise the “originals” of the documents – and what additional proofs may need to be captured, if any. Note that a basic image can easily be copied, whereas a full biometric signature cannot be identically copied by a user. • Adopt the same signing protocols as for a wet ink virtual signing, updated to reference the form of signature and the lack of a wet ink original. • Parties may wish to agree practical ways to evidence and record the fact that the signatory is approving the document. This could include: • Conduct (and record) the signing by video call. • Ensure that the signed document is returned from the authorised signatory’s email account, and that the authorised signatory confirms the signing and sending of the document by telephone. • Ensure that those receiving electronically signed documents conduct basic checks to ensure that there is nothing obviously suspect, for example that it does not come from an unknown email address.

Method/type of Electronic Signature	Risk Profile	Best Practice
		• Use a full Biometric Handwritten Signature, especially at a QES standard. Although the technology is sophisticated, user actions are simple. The signatory (and any witnesses) are more likely readily to understand the significance and use of the relevant signing actions. • It is important to pre-agree what eIDAS standard is going to be used in relation to a risk-weighted view of future needs for evidence.
Inserting a saved jpeg or pdf signature into a document	This method is not as robust or secure as most of the methods described above, or will at least require additional authentication or verification steps. The saved jpeg signature can easily be mis-used by others, either maliciously or with the implied approval of purported signatory (e.g. by a secretary, or another family member, with or without the originator's permission).	*This method is typically not best practice and should be avoided where possible, using other easily available methods.* • Ensure that the parties agree to the use of this form of electronic signing in advance. • Agree in advance what will comprise the "originals" of the documents. • Adopt the same signing protocols as for a wet ink virtual signing, updated to reference the form of signature and the lack of a wet ink original. • Parties may wish to agree practical ways to evidence and record the fact that the signatory is approving the document. This could include: • Use other identifying approaches, such as 2FA or mTAN SMS codes[98] sent to a pre-known device. • Conduct (and record) the signing by video call.

[98] See Appendix 7 for explanation.

Method/type of Electronic Signature	Risk Profile	Best Practice
		• Ensure that the signed document is returned from the authorised signatory's email account, and that the authorised signatory confirms the signing and sending of the document by telephone. • Ensure that those receiving electronically signed documents conduct basic checks to ensure that there is nothing obviously suspect, for example, that it does not come from an unknown email address. • You should also carefully consider whether the signature has been applied to the document by the authorised signatory. If it has not, then there is a heightened risk of the signature being invalid.[99] If you are put on notice that the signatory is not available to sign in wet ink when it has been agreed that the signing will occur by email, you should clarify how the pdf signature will be applied.
Typing a name into a document	The name typed in a signature can easily be guessed or mis-used by others. There is a higher risk of other parties forging a signature of the purported signatory (e.g. by a secretary, or another family member, with or without the originator's permission).	• Ensure that the parties agree to the use of this form of electronic signing in advance. • Agree in advance what will comprise the "originals" of the documents. Adopt the same signing protocols as for a wet ink virtual signing, updated to reference the form of signature and the lack of a wet ink original.

[99] Law Society, 'Q&A on How to Use Electronic Signatures and Complete Virtual Executions' (6 January 2021) <https://www.lawsociety.org.uk/en/topics/business-management/qa-on-how-to-use-electronic-signatures-and-complete-virtual-executions> accessed 7 October 2021.

Method/type of Electronic Signature	Risk Profile	Best Practice
	This method may be sufficient for lower value and simpler forms of signing, but requires additional authentication or verification steps to increase its evidential weight.	• Parties may wish to agree practical ways to evidence and record that the signatory is approving the document. This could include: • Use of other identifying approaches, such as 2FA or mTAN SMS codes[100] sent to a pre-known device. • Conducting (and recording) the signing by video call. • Ensuring that the signed document is returned from the authorised signatory's email account and that the authorised signatory also confirms the signing and sending of the document by telephone. • Ensuring that those receiving electronically signed documents conduct basic checks to ensure that there is nothing obviously suspect, for example, that it comes from an unknown email address. • Carefully considering whether the signature has been typed in the document by the authorised signatory (as opposed to another person). If it has not, then there is a heightened risk of the signature being invalid. If you are put on notice that the signatory is not available to sign when it has been agreed that the signing will occur by email, you should clarify how the typed signature will be applied.

[100] See Appendix 7, for explanation.

Appendix 6 Best Practice Guidance Table – Individuals

Method/type of Electronic Signature	Risk Profile	Best Practice
Qualified electronic signature (QES) (as defined in the eIDAS Regulation which forms part of retained EU law)	Setting up a Qualified Electronic Signature certificate for the first time will require each signatory to engage with a Qualified Trust Service Provider to set a signing certificate. This may impose unnecessary costs on customers with limited financial resources and introduce additional stress and confusion for persons unfamiliar with the role and purpose of the trust service provider. Identity documents may be checked by the 3rd party before a signatory can be set up. Vulnerable individuals may not be able to comply with standard AML requirements and this can represent a barrier to access. **Benefits:** The enhanced security features make it apparent to users that they are entering into a significant contract or arrangement.	Although this is one of the most secure forms of electronic signing, consideration should be given to whether it is necessary or appropriate to require this level of signing standard. (See above for best practice above on when to consider Qualified Electronic Signing) If the contract requires a high security standard, then consideration should be given to how the counterparty can be provided with a step-by-step guide on how to create the necessary signing certificate with the 3rd party trust service provider. Further points to consider are the costs to the counterparty of creating a signing certificate and whether they are proportionate to the value of the transaction. If it is known that the counterparty will be required to provide personal information or documents (e.g., copy of a passport) to the trust service provider, then this should be made clear in advance, so it does not cause any unnecessary stress or anxiety when engaging the 3rd party. A handwritten biometric signature may also be used with a certificate to provide a QES signature, combining a readily understood process with cryptographic approaches.

Method/type of Electronic Signature	Risk Profile	Best Practice
	Interaction with independent third parties may provide additional protections for the individual.	The location at which the public element of a PKI pair might be inspected or requested should be made available to the signing parties.
Using a web-based eSigning platform	The security features may rely on 'one-time passcodes' sent to a mobile phone device. Although this method is now common when using online banking and technology platforms, some individuals do not have access to a mobile phone or may have a shared device. An email address of each signatory and witness is usually required by the signing platform. Vulnerable individuals may not have access to email. Vulnerable individuals may be unable to arrange for an independent witness to be present. **Benefits:** Web-based platforms are broadly compatible with accessibility features and assistive technologies available on major operating systems. For example, magnification, voice command and text-to-speech conversion.	Confirm what technology or devices the signatories have access to before arranging for electronic signing. Before selecting an eSigning platform, consideration should be given to its accessibility features or its compatibility with features available on major operating systems. These details can be obtained, whether from published material or even the sales representative for the eSigning platform to be used, if there is any uncertainty about the features available. Where guidance is available on how to use the platform, this should be provided to parties, customers or counterparties. Most eSigning platforms will provide a copy of the executed agreement by email to each counterparty. Consider alternative methods of signing where the counterparty does not have access to an email account or has low technical capability. Be clear as to how the customer may cancel any agreement. Consider including a time limit to apply a signature, so that by not signing the customer can be considered to have 'opted out'.

Method/type of Electronic Signature	Risk Profile	Best Practice
	It may be possible to build in further review points or guidance as part of the signing process to provide further assistance for the user.	
Signing on screen using a stylus or Apple pen	Requires specialist technology which may be expensive or not widely available to all users. Requires physical movement of stylus or pen which cannot be assisted by accessibility features usually available on computers or personal devices (e.g., magnification or voice features). **Benefits:** It simulates the act of signing in wet-ink, so it may feel natural for those more comfortable with wet-ink signatures and will be easily understood to be an act of signing.	Signing 'on screen' with a stylus or pen is not accommodated on all devices. If a signatory's device allows for a mouse or touchscreen to be used, in place of a stylus, the signature impression may not appear the same as when signing in so-called "wet ink". This should be considered if the process involves a comparison of an electronic signature with a wet-ink signature held in records. Special purpose signing devices are recommended for accuracy and security, otherwise compatibility of software with a device and use of modern devices (tablet, smartphone, PC, etc.) should be checked with the vendor by the issuing organisation. This technology is commonly used where a customer is signing at a business premises, or a sales representative is completing a sale at the customer's home (i.e., the contract is being executed on a terminal or device used by a business). In these circumstances, consideration needs to be given on a transaction-specific basis of what (if any) further steps need to be built into the signing process to ensure that the customer is given the opportunity to read and understand the agreement. This will allow for confirmations and acknowledgements to be provided throughout the process.

Method/type of Electronic Signature	Risk Profile	Best Practice
Inserting a saved jpeg or pdf signature into a document	Persons with low technical ability may be unfamiliar with different document formats and how each is displayed in a document. May be used without the signatory's consent where persons have shared access to technology or persons in unstable domestic environments. **Benefits:** It may feel natural for those more comfortable with wet-ink signatures and relies on widely available technology.	Care should be taken with vulnerable individuals to ensure that this is not mis-used. Additional steps to verify the signatory's understanding may be advisable. Give clear instructions that image of the signature must only be used by the signatory or a person assisting the signatory to sign. Ask who else may have access to any device used by the individual. Provide alternative means of signing (such as typed signature or biometric signature) for those unable to capture or store images of their signature, and provide additional verification such as 2FA approaches. Consider confirming via telephone or email that the individual has executed the document via this means and that documentation is returned from an address known to belong to that individual. Signing can, for example, be recorded via video conference.
Typing a name into a document	Those with capacity issues or cognitive disability may not appreciate the significance of typing a name in lieu of a handwritten signature **Benefits:** Requires limited technical knowledge and relies on widely available technology.	Care should be taken with vulnerable individuals to ensure that this is not mis-used. Additional steps to verify the signatory's understanding may be advisable. Where a typed name is being used as a signature, ensure that the legal significance of typing a name is clearly explained. Some major operating systems may auto-populate blank data fields (particularly name fields). Consideration should be given to whether the signatory would understand that they are signing even

Method/type of Electronic Signature	Risk Profile	Best Practice
		if the typed field is auto filled by the signatory's own operating system on the device they are using. Consider confirming via telephone or email that the individual has executed the document via this means and that documentation is returned from an address known to belong to that individual. Signing could be recorded via video conference.

Appendix 7 – Further detail

1. This appendix contains further detail on the following topics:
   A. Qualified Certificate Requirements
   B. Public Key Infrastructure Overview
   C. The document model and long term archive

A - Qualified Certificate Requirements

2. Qualified Certificates for electronic signatures shall contain:
   (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a Qualified Certificate for electronic signature;
   (b) a set of data unambiguously representing the Qualified Trust Service Provider issuing the Qualified Certificates including at least, the Member State in which that provider is established and:

3. for a legal person: the name and, where applicable, registration number as stated in the official records,

4. for a natural person: the person's name;
   (c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;
   (d) electronic signature validation data that corresponds to the electronic signature creation data;
   (e) details of the beginning and end of the certificate's period of validity;
   (f) the certificate identity code, which must be unique for the Qualified Trust Service Provider;
   (g) the advanced electronic signature or advanced electronic seal of the issuing Qualified Trust Service Provider;
   (h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;
   (i) the location of the services that can be used to enquire about the validity status of the Qualified Certificate;
   (j) where the electronic signature creation data related to the electronic signature validation data is located in a Qualified Electronic Signature Creation Device, an appropriate indication of this, at least in a form suitable for automated processing. In the UK the ICO regulates organisations that issue certificates. Use of Trust Services, QTSPs, the UK Trusted List, Approval processes, Enforcement and more can be found on their website (https://ico.org.uk/for-organisations/guide-to-eidas/qualified-trust-services/).

B - Public Key Infrastructure (PKI) overview

5. A public key infrastructure (PKI) is a set of rules, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. In relation to eSigning, it is implemented differently by different vendors but all aim to meet the regulations demanded by their markets, across multiple jurisdictions.

6. The Open Identity Exchange (OIX) in Oct 2021 published an eSignature explanation document, including this useful description of PKI:[101]

   "Digital signatures rely upon advanced cryptography to produce results by using a secret value (key) that cannot easily be guessed or discovered by trying possible answers one at a time – it would just take too long. There are two kinds of cryptography available – symmetric (the same key encrypts and decrypts) and asymmetric (two different keys: one to encrypt and one to decrypt). Symmetric is faster and more efficient (it is used in online secure transactions indicated by the padlock symbol) but it is obviously very difficult to share securely. In asymmetric cryptography, one key is kept secure (i.e. private) and the other can be shared (i.e. public).

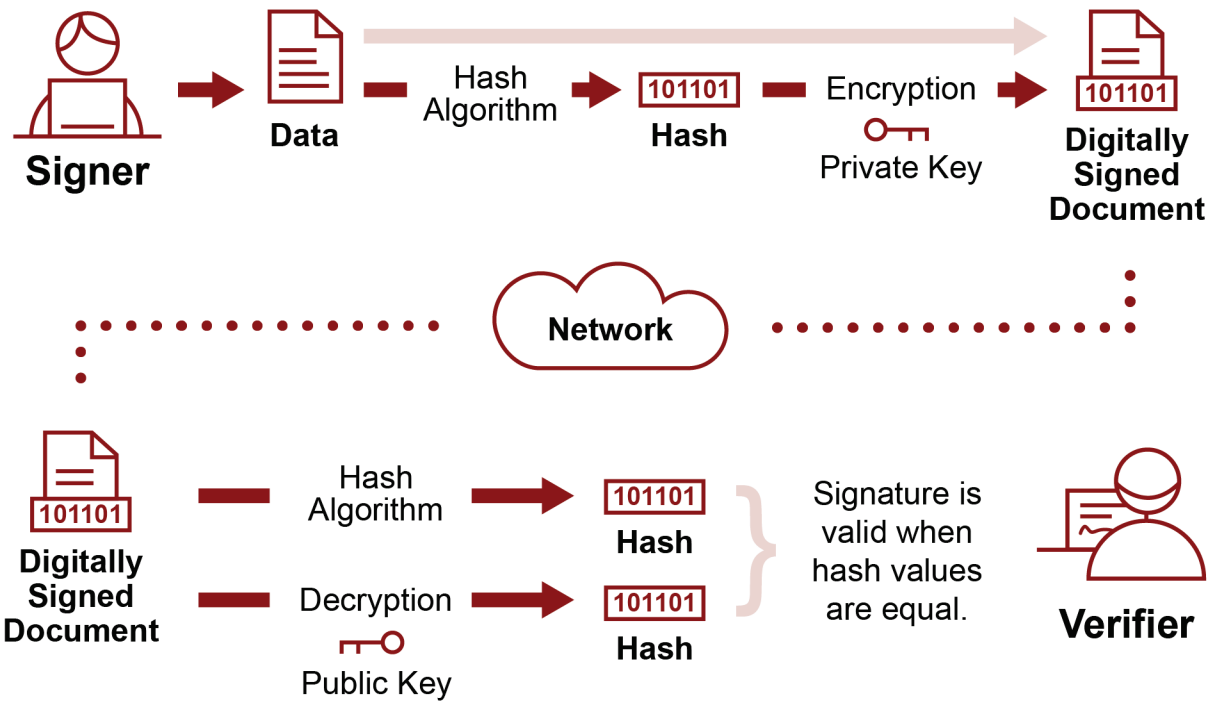
   If you are trying to keep information confidential and only want the recipient to be able to read it then imagine that they provide online 'padlocks', anyone can then use one of these padlocks safe in the knowledge that only the recipient has the key to unlock it. If you are using digital signatures then the analogy is reversed and you provide online keys, so that when you sign (or padlock) a document the recipient knows it was signed by you because they can only unlock it with one of your keys. Don't worry about the potential for confusion though as each of these online keys and padlocks come with a certificate that says who it belongs to and whether it is a key or a padlock – this certificate service is all provided by a Public Key Infrastructure made up of trustworthy Certificate Authorities ("CA").

   When a signatory electronically signs a document, it is chopped up into equally sized chunks that are repeatedly compressed (using a known hashing algorithm like SHA-256) until a single chunk is left – the hash or digest of the message, which along with the date and time is then encrypted using the signatory's private key, which must be securely kept by the signatory. The recipient then performs the same hashing function and also produces the hash of the message and if this matches the received hash (after it has been decrypted using the signatory's public key) then you can be confident that the message is from the signatory and has not be altered.

   As an example, Jane signs an agreement to sell a timeshare using her private key. The buyer receives the document. The buyer who receives the document also

[101] https://openidentityexchange.org/networks/87/item.html?id=501

receives a copy of Jane's public key. If the public key can't decrypt the signature (via the cipher from which the keys were created), it means the signature isn't Jane's, or has been changed since it was signed. The signature is then considered invalid.



As mentioned earlier, to protect the integrity of the signature, the process requires that the keys be created, managed and stored in a secure manner, and requires the services of a reliable CA. A CA can be the digital signature provider themselves or a trusted independent third party. PKI also enforces additional requirements, such as a digital certificate, end-user enrolment software, and tools for managing, renewing, and revoking keys and certificates."

C - The Document Model and Long Term Archive

Source: Namirial Digital Transaction Management White Paper. (Namirial is a QTSP that has also been accredited by AgID for Long-Term Archiving/Digital Preservation Services)

PDF[102] is typically chosen as it is an open document standard where digital signatures are well defined in the PAdES ISO standard. PAdES enables signed documents to be "self-contained", which - according to Gartner Research (Publication ID Number: G00159721) - is the best document format, so it includes the content to be signed, the signature, and the metadata to make it searchable. In addition, it should store the signature process evidence data, such as the signing date,

[102] Which stands for Portable Document Format, although many different files are now simply referred to as "PDFs"

geolocation, and so forth. Last, it should require only a reader that's freely and universally available to show the document in its original form.

PAdES Basic Profile (based on ISO 32000-1)

Digital signatures are well defined in PDF itself (Adobe PDF Reference PDF 32000-1:2008 12.8.3.3 PKCS#7 Signatures, as used in ISO 32000-1), meaning that every standard compliant viewing application, such as Adobe Acrobat Reader, correctly shows digitally signed PDFs without the need for any proprietary software. This includes the following data:

- Signature image (the visual representation of the signature);
- Document status when each digital signature was applied (the embedded signature history), even if you are not connected to the internet;
- The document's integrity, meaning whether the signed document is still original or whether it has been altered since the signature was applied;
- Date and time the document was signed—optional, via a trusted time stamp service;
- Geolocation where the document was signed (GPS data if provided);
- Identity of the certificate holder, which in cases where a sealing certificate is used (e.g. for biometric signatures) typically points to the issuer of the signed document.

PAdES Long-Term Validation (LTV Profile)

Validation of a PAdES signature requires data to validate this signature such as CA certificates, Certificate Revocation List (CRL) or online certificate status profile (OCSP) information, commonly provided by an online service (referred to as validation data). If the document is stored and the signatures are to be verifiable long after first created, in particular after the signing certificate has expired, the original validation data may no longer be available or there may be uncertainty as to what validation data was used when the document was first verified. Also, the cryptographic protection afforded by the signature may not be guaranteed after the certificate has expired.

The PAdES LTV profile addresses this issue and thus is equivalent to the PDF variant, being designed for long-term storage and activation, defined as a PDF/A in ISO 19005-1:2005. PAdES LTV uses an extension to ISO 32000-1 known as a document security store (DSS) to carry such validation data as necessary to validate a signature, optionally with validation-related information (VRI), which relates the validation data to a specific signature. Additionally, it uses another extension known as document time-stamp to extend the protection lifetime of the document. The document time-stamp also protects the DSS by binding it to the document to which it applies.

The protection lifetime can be further extended beyond the life of the last document timestamp applied by adding further DSS information to validate the previous document timestamp along with a new document time-stamp.[103]

[103] https://www.xyzmo.com/Downloads/Documents/en/Namirial_DTM_Solution.pdf

References

AbilityNet, 'Free Resources' <https://abilitynet.org.uk/free-resources> accessed 7 October 2021

Alzheimer's Society, *Dementia UK: Update* (2014)

Department for Work and Pensions, *Family Resources Survey 2016/17* (2018)

Financial Conduct Authority, 'Financial Lives Survey' (19 June 2018) <https://www.fca.org.uk/publications/research/financial-lives> accessed 7 October 2021

——, *FG21/1 Guidance for Firms on the Fair Treatment of Vulnerable Customers* (2021)

——, *Financial Lives 2020 Survey: The Impact of Coronavirus* (2021)

HM Land Registry, *Practice Guide 8: Execution of Deeds* (2021)

Law Commission, *Electronic Execution of Documents (Consultation Paper No. 237, 2018)*

——, *Electronic Execution of Documents (Law Com No. 386, 2019)*

Law Society, 'Q&A on How to Use Electronic Signatures and Complete Virtual Executions' (6 January 2021) <https://www.lawsociety.org.uk/en/topics/business-management/qa-on-how-to-use-electronic-signatures-and-complete-virtual-executions> accessed 7 October 2021

Lord Keen of Elie, 'Government Response to the Law Commission report Electronic Execution of Deeds (UIN HLWS135)' (3 March 2021) <https://questions-statements.parliament.uk/written-statements/detail/2020-03-03/HLWS135> accessed 7 October 2021

Namirial, 'Digital Transaction Management' <https://www.xyzmo.com/Downloads/Documents/en/Namirial_DTM_Solution.pdf> accessed 20 January 2022

National Health Service, 'Adult Psychiatric Morbidity in England - 2007: Results of a Household Survey' (27 January 2009) <https://digital.nhs.uk/data-and-information/publications/statistical/adult-psychiatric-morbidity-survey/adult-psychiatric-morbidity-in-england-2007-results-of-a-household-survey> accessed 7 October 2021

Office for National Statistics, 'National Population Projections: 2018-Based' (21 October 2019) <https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationprojections/bulletins/nationalpopulationprojections/2018based> accessed 7 October 2021

Open Identity Exchange (OIX), 'Explaining Electronic Signatures' (11 October 2021) <https://openidentityexchange.org/networks/87/item.html?id=501> accessed 20 January 2022

Royal National Institute for Blind People, 'Services for Businesses' <https://www.rnib.org.uk/services-for-businesses> accessed 7 October 2021

World Wide Web Consortium (W3C), 'Web Content Accessibility Guidelines (WCAG) 2.1' (5 June 2018) <https://www.w3.org/TR/WCAG21/> accessed 7 October

This publication is also available on our website at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at general.queries@justice.gov.uk