Industry
Working
Group

Electronic Execution of Documents

Industry Working Group Final Report

February 2023

Industry Working Group

Electronic Execution of Documents

Industry Working Group Final Report

February 2023

Contents

Executive Summary **3**

A. Introduction **8**

a. Background and formation 8

b. Terms of Reference 12

c. Interim Report conclusions and the outstanding Terms of Reference 13

d. Progress in field of electronic documents generally 14

e. Certification/Accreditation 18

f. Conclusions 19

B. Outstanding Terms of Reference **20**

a. Cross-border challenges 20

b. Protection from fraud 32

C. Best Practice as explained in the Interim Report **47**

a. Is Electronic Execution Appropriate? 48

b. How to choose the best form of electronic signature 50

c. Fours steps to follow for electronic execution 52

d. Identity, Security and Reliability 55

e. Vulnerable Individuals 56

f. Best Practice Guidance - Vulnerable Individuals 58

g. Other developments since the time of the Interim Report 59

D. The need for rapidity and progress in this field **63**

E. Certification/Accreditation **66**

F. Consultation **68**

The Consultation Questions 68

Conclusions 74

G. Recommendations **76**

Appendices 79

Appendix 1 – Group biographies 79

Appendix 2 – Glossary 81

Appendix 3 – Table of electronic execution requirements for common document types ... 84

Appendix 4 – Table of formalities for common types of transaction 91

Appendix 5 – Best Practice Guidance Table – Commercial Transactions 92

Appendix 6 – Best Practice Guidance Table – Individuals 102

Appendix 7 – Electronic Trade Documents Bill 107

Appendix 8 – The validity of electronic signatures on deeds in Northern Ireland 111

References 113

Executive Summary

i. The publication of this Final Report occurs alongside a number of significant transitional steps towards a more digitalised world. The growing demand for online interaction, coupled with ever increasing technological capabilities, mean that electronic execution is at once both more widely available and subject to greater scrutiny. This has led to, amongst other initiatives, the formation of the UK's own digital identity and attributes trust framework, the EU's digital identity wallet, the Government's publication of its Consultation on draft Digital Government (Disclosure of Information) (Identity Verification Services) Regulations 2023, the Electronic Trade Documents Bill starting its passage through its parliamentary stages and the publication of a major report on technological innovation and the future of Britain.[1] Against that backdrop, this Report completes the objective of the Industry Working Group to promote and facilitate the electronic execution of documents by matching appropriate solutions to the requirements of parties and to the problems they might face.

ii. The Interim Report, published in February 2022, dealt with six of the Group's eight Terms of Reference. This Report is concerned with the final two of those: issues arising from cross-border transactions and the risks of fraud. In so doing, it functions as a standalone document, referring to the Interim Report where necessary, and repeating the main conclusions of the earlier analysis, without reiterating that material in full. It also sets out the context and results of the Group's public consultation on certification/accreditation; a question that gave rise to mixed views both internally and externally.

Cross-border challenges

iii. Legal agreements underpinning cross-border transactions may in practice need to be drafted and executed in accordance with the law relevant to the parties and the governing law in order to minimise the risk that the transaction turns out to be invalid or not binding. The uncertainty around the interpretation of different jurisdictions' electronic execution laws, and the requirements and formalities surrounding electronic execution can give rise to challenges of increased costs, delay and uncertainty, all of which can hinder adoption of e-signing.[2]

---

1 A New National Purpose: Innovation Can Power the Future of Britain | Institute for Global Change

2 See paragraph 7 (Conflicts of law issues) of The Law Society Company Law Committee & The City of London Law Society Company Law & Financial Law Committees Note on Electronic Execution of Documents for a discussion of the circumstances in which the parties to a document to be signed using an electronic signature may wish to seek advice from counsel in another jurisdiction.

iv. In relation to a transaction involving parties (and performance) across multiple jurisdictions, questions arise as to the applicable law governing the transaction and, sometimes consequently, the enforceability of the relevant agreement.

v. One of the cleanest ways of dealing with these issues, which are otherwise somewhat inevitable, would be for significant trading states to adhere to some form of international norm or code. To this end, the Group recommends that the UK consider adopting the UNCITRAL Model Law on Electronic Signatures, at least in some form. Article 12 of the Model Law is particularly instructive on the point of cross-jurisdictional recognition, and UK movement on this point, given its significance as an international commercial hub, would send a strong signal, and perhaps act as an incentive, to other jurisdictions.

vi. As stated in the Interim Report, the best way of mitigating potential inconsistencies in definitions and requirements of electronic signatures is for parties to adopt eIDAS standards. In the UK, the eIDAS Regulation was implemented by the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 and section 7 of the Electronic Communications Act 2000. 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. The second section is concerned with Trust Services and electronic signatures. The EU in June 2022 published another version of eIDAS, which is known as eIDAS2 or eIDAS 2.0. It aims to update the original eIDAS and make it more uniformly acceptable, with a view to becoming more widely used across all member states, including being compulsory in some instances. eIDAS 2.0 is not yet adopted and this is expected to occur sometime in the middle of 2023.

vii. In a similar vein, consistency in technological reliability standards is crucial to smooth cross-border transacting. In order to reduce the risk of the same electronic signature being deemed reliable in one jurisdiction but not another, the formulation and widespread adoption of internationally aligned standards are again the obvious solutions, and Article 6 of the UNICTRAL Model provides a strong example.

viii. Robust and universally available digital identities would function effectively alongside such standards and the two would be mutually reinforcing. The work of the Department of Digital, Culture, Media and Sports (DCMS)[3] in developing a UK Digital Identity and Attributes Trust Framework is a very positive development in this regard. The Framework's objective is to ensure a standard for identity verification that can be applied across the whole UK economy. The EU Digital Wallet scheme is a similarly valuable step towards comity in digital identity recognition.

[3] As was at the time of drafting – now Department for Culture, Media and Sport. The UK Digital Identity and Attributes Trust Framework now sits in the Department for Science, Innovation and Technology (DSIT).

ix. Even once international norms and standards have been adopted by some states, there remains a problem of information asymmetry, so that it can be very challenging, and therefore costly, for parties to discover which standards have been adopted and by whom. The Group suggests, therefore, that some form of repository for this information be established, or that the function be assigned to a body already in existence, such as the Information Commissioner's Office (ICO). It would be very helpful were there to be some form of online "one stop shop" for information on international recognition, standards and requirements.

x. The signatures and seals of public officials for use in foreign countries are frequently verified by a Government Agency, Embassy or High Commission in a process known as legalisation. Those countries which are party to the Hague Convention 1961 on the abolition of legalisation requirements achieve verification instead through one competent authority (in the case of the UK the Foreign Commonwealth and Development Office "FCDO") issuing an "Apostille". For some years The Notaries Society has been working with the FCDO to make available to public officials in the UK an electronic version of the Apostille (known as the e-APP) In September 2022, the FCDO announced the official launch of the e-APP. The advent of the e-APP in the UK will, potentially and hopefully, encourage other countries to accept such documents and signatures.

Protection of electronic signatories to deeds from potential fraud

xi. The presence of an electronic signing platform in the deed authentication process has several significant advantages over its paper and wet ink signature counterpart. The provision of advice and guidance to signatories can be both carried out by that platform and recorded and stored as evidence that the provision occurred. Similarly, the signing process itself can be recorded and video and audio evidence of it stored for future reference, thereby providing a record that is both more accurate and longer lasting than the testimony of a human witness. Platforms can also be configured so as to ensure that all of the requisite steps are followed before the document can be submitted, thereby reducing, if not eliminating the possibility of defective execution.

xii. The circumstances in which such electronic signing is able to take place can also reduce the possibility of physical witness intimidation or duress because a signatory might well feel more comfortable taking their time to read and process the document and its implications in the absence of a physical witness. The platform can also record exactly what the signatory saw before signing took place, whilst also being able to restrict access to this data to particular individuals.

xiii. As an example of how this can work in practice, the home buying and selling sector has worked to develop a digital identity trust scheme (DITS), aligned to the UK Digital Identity and Attributes Trust Framework. The Home Buying & Selling Digital Identity Trust Scheme will allow participants in the Scheme to trust an identity proof provided by third party Identity Providers, who are subject to audited certification and

regulation. The Scheme details how an identity can be digitally proved following the Government's GPG45 standard, whilst meeting money laundering regulation (MLR) customer due diligence requirements. The Scheme will allow the digital identity of a home buyer/seller to be verified *once only* (rather than multiple times as currently) and then be shared by the consumer and used throughout the rest of the sales transaction, based on consent. This will streamline what has, traditionally, been a cumbersome process.

xiv. Also, in March 2021 HM Land Registry (HMLR) launched its first Digital Identity Standard. This provides a step-by-step list of requirements for conveyancers' use of digital services to verify their client's identity securely online. The new standard is optional. However, it offers a 'Safe Harbour' for those conveyancers who meet the requirements. HMLR would not seek recourse against conveyancers who comply with the standard in the event their client was not who they claimed to be. The Group regards both of these as models that could usefully be followed in other sectors.

xv. One subject upon which all members of the Group did not fully agree in all respects was that concerning certification of providers of platforms. It is widely accepted that trust in the platform providers and/or the services provided by the same – whether trust by the public or by commercial entities that wish to use e-signature services – is fundamental to wider adoption and use generally. There are two approaches to such a requirement, which are at opposite ends of the spectrum, and innumerable different points of view in between. One end of the spectrum is the entirely market-forces view, namely that only the best (or the adequate) will survive, and such survival is dependent upon trust from users which should be earned. This viewpoint eschews regulation as being both undesirable but also unworkable in practice, particularly in terms of requirements that are non-technical in nature. The other point of view is that some sort of approval or oversight mechanism is required so that some order can be imposed on what is currently a largely unregulated and unsupervised environment. The Group does not at this point find itself in a position where it can proffer a unanimous recommendation in this area.

xvi. In order, however, to ensure that the content of the Final Report by the Group reflected as wide a view as possible, the decision was taken to put certain questions out for public consultation. The consultation process was administered by the Ministry of Justice and the Secretariat to the IWG. A reasonable number of responses were received, including from major City firms, practitioners and industry specialists. The results of that consultation process are set out in the Report with a view to their forming the basis of future consideration by Government.

Recommendations for reform

xvii. The Report's main recommendations for reform, or work towards reform, are as follows:

- Enhanced certification through the role of the ICO and a review of the National Cyber Security Centre ("NCSC") Technical Assurance Principles initiative
- Self-certification involving ICO/DSIT or another government body working as a moderator that:
  (1) develops a set of signing platform 'basic performance standards';
  (2) publishes the standards on a 'dedicated/go-to' webpage that is easily locatable for prospective platform users;
  (3) invites signing platforms to confirm whether they meet the standards;
  (4) publishes a list of signing platforms that submit self-certifications on a go-to webpage;
  (5) confirms listings annually.
- Work towards uniformity of approach to e-signing and online identification by way of an international standard or mutual recognition
- Government consideration of wholesale adoption of e-signatures for all purposes, and investigation into modernising any area where wet ink signatures are mandated
- Review by the Law Commission of the law of deeds with a view to the abolition of at least some of their current requirements
- A review of the law of statutory declarations
- The establishment by Government, or a suitable Department, of a standing body similar to the Industry Working Group, comprising both legal, industry and academic membership that is able to focus solely on these issues and to keep abreast of developments as they occur.

A. Introduction

a. Background and formation

1. This Industry Working Group ("IWG") which produces this Final Report was established by the Government in the spring of 2021 following a public appointments competition. This followed the Government's acceptance of a Law Commission report *Electronic Execution of Documents* (2019),[4] in which the Law Commission had concluded that e-Signatures 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. That Law Commission report had, however, also recognised that uncertainties generally remained at that time regarding the mechanics of executing documents electronically, and that those uncertainties were having a potential impact upon the degree of confidence that both professional and individual users may have. This lack of confidence could have an impact on the increased use of electronic signatures. As the Report at that stage expressed it, there were potential doubts about the evidential weight or probative value that might be given to a signature if there were disputes about the identity of the signatory or about the contents of the document. The Law Commission recommended that a multi-disciplinary group of business, legal and technical experts should be convened in order to consider both 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.

3. As a result of this, the IWG was established in order to perform this role. The Government indicated that it considers the IWG to play a vital role in improving the confidence of both domestic commerce and international trade in the digital age. The Group was chaired initially by Mr Justice Birss, who was then appointed to the Court of Appeal and became Lord Justice Birss, together with Professor Sarah Green (Law Commissioner for Commercial and Common Law) and Mr Justice Fraser (the former Judge in Charge of the Technology and Construction Court, and now the Judicial Lead for Data). When Birss LJ became the Deputy Head of Civil Justice in 2021,

[4] https://www.lawcom.gov.uk/project/electronic-execution-of-documents/

Mr Justice Fraser took over the role of Judicial Chair and has continued to chair the IWG with Professor Green since then.

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

A short description of each of their expertise is at Annex A. The IWG also co-opted Richard Trevorah, the Technical Director of tScheme Ltd, the self-regulatory body for electronic trust service approval in the UK, and a description of his expertise also appears in Annex A. The IWG has met a number of times throughout 2021 and 2022, predominantly on a virtual basis, and also had the benefit of presentations from industry names not represented in the Group, and governmental departments. The publication of the Interim Report was achieved in February 2022. All members of the IWG act on a voluntary and unpaid basis. The Interim Report was published less than 12 months after formal inception of the group, which in the circumstances of voluntary participation and other employment/duties on the part of all of its members, was a shorter timescale than expected.

4. However, that timetable was only achieved in the following way. It was not possible to address all of the Terms of Reference in the timescale from the group's inception to the date that the Interim Report was delivered in draft to the Government in January 2022. Some of the Terms of Reference were therefore postponed to be dealt with in a Final Report. Further, one point in particular remained contentious between members of the group, namely certification/accreditation of e-Signature providers. The Chairs considered that this subject ought to be put to public consultation, and this took place in the summer of 2022. That consultation received responses from a wide area of interested parties, including the technology industry itself. A summary of the results is in Section F.

5. The Group continued its work throughout 2022 and into 2023 in parallel with other digital advances taking place generally across the public sector, for example the progress at the Land Registry for digital signing and the ongoing work towards digital identity. In January 2023 the Government published its Consultation on draft Digital Government (Disclosure of Information) (Identity Verification Services) Regulations

2023, with the aim of that draft legislation being to improve how data is shared and used across the public sector.[5] This is to make identity verification online easier and more reliable, and to help the Government ensure more people can use digital public services.

6. That proposal is for a new regulation under the Digital Economy Act 2017 ("DEA") "to strengthen the ability for departments to share necessary information to support identity verification and reuse".[6] In the Ministerial Foreword to the Consultation, Alex Burghart MP stated:

   "The proposed data-sharing legislation will ensure that more people than ever before will be able to prove their identity online and access government services, so that anybody who wants to use online services is able to. Furthermore, the government is committed to realising the benefits of digital identity technologies without creating ID cards."[7]

7. Digital identity is also a subject being progressed by the European Union ("EU"). In December 2022 the EU announced the companies awarded the contract for the development, consulting and support services for the EU digital identity wallet. The wallet is intended to provide universal and interoperable digital identity across the EU, along with electronic signatures and document validation across all sectors. It is also intended to provide full transparency of data use. It is proposed that the wallet will provide safe, secure and transparent digital identification, with benefits of ease of use and reduced costs for businesses, and will also enable more cross-border transactions. The wallet is to be offered to EU Member States and other stakeholders implementing the requirements of the framework for a European digital identity, according to the company announcement. The EU is preparing for the 2024 release of its digital ID wallet, which would enable all EU residents to store digital identity credentials such as national ID, driving licence and bank account details. This means that the legislation is intended to be passed in the spring of 2023, including the publication of industry standards and specifications. The aim of the EU Digital Wallet is to simplify daily life for EU citizens and businesses and is said by its proponents to be something that will create growth opportunities for public and private services across the EU.

8. The UK's own digital identity and attributes trust framework was published in its beta version (0.3) on 11 January 2023.[8] In the Ministerial Foreword to the publication, Julia Lopez MP the Minister of State for Media, Data, and Digital Infrastructure said:

---

5 See also R Oliphant, Latest trends in the UK e-signing market | THINK Digital Partners : THINK Digital Partners

6 Cabinet Office and Government Digital Service

7 https://www.gov.uk/government/consultations/draft-legislation-to-help-more-people-prove-their-identity-online/consultation-on-draft-legislation-to-support-identity-verification

8 https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version/uk-digital-identity-and-attributes-trust-framework-beta-version

> "Seeking out views from the public has been central to moving the trust framework to beta phase. Research on public perceptions of digital identities and attributes conducted by *BritainThinks* provided important insights about what people need to trust and adopt digital identities. Users were clear that they wanted digital identities to be easy to use, safe, reliable, and offer control over personal data, with clarity over providers' business models. We have taken all of these into account when updating the trust framework… We have previously committed to encouraging the recognition of trusted digital identities across borders. During the alpha phase, we have assessed how trust framework rules compare to frameworks being developed in other countries. We will continue working with international partners to better understand how to achieve the ambition of international interoperability in a way which best aligns with UK democratic values and principles."[9]

9. There is therefore no doubt that this is a rapidly moving area. The basic principle of an e-Signature is to match or better the physical demonstration of the acceptance or acknowledgement of terms in a document, that traditionally would have been shown by using a wet signature, but in digital form. When the Government decided in 2020 to accept the Law Commission recommendation to set up a working group, such matching, at least on a large scale, was still a relatively novel development in most sectors, but the Covid-19 pandemic earlier that year had shown that traditional wet signatures, which by definition would require physically attendance, were not always (or even regularly) possible. Since 2020, it can be confidently suggested that human behaviour has changed dramatically. Even in February 2020, the digital economy was worth over £400 million per day to the UK economy;[10] more recently, the Office of National Statistics reported that 25% of all retail sales for Q3 of 2022 were online.[11] Paragraph 16 of our Interim Report referred to the "astonishing speed" with which modern technology moves. That speed is, if anything, accelerating.

10. The importance of e-Signatures is similarly elevated, in the view of the Group as a whole. Given this central importance, all the relevant features of authentication, safety, robustness and the overall confidence that society has in their validity and security must not only be addressed, but their importance sufficiently recognised. The Group has been highly productive and enjoyed co-operative working relations internally, even when individuals have disagreed on the only contentious point, namely certification/accreditation. In particular, the mix of legal, business and technology works extremely well and is recommended as a model for such groups going forwards. However, it believes collectively that further work in this particular area must now be passed to a non-voluntary body, which will be better able to recommend, innovate and react to this fast-changing area of society, allowing

---

9 https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version/uk-digital-identity-and-attributes-trust-framework-beta-version

10 https://www.gov.uk/government/news/digital-sector-worth-more-than-400-million-a-day-to-uk-economy

11 https://www.ons.gov.uk/businessindustryandtrade/retailindustry/timeseries/j4mc/drsi

individual members to devote more time to this important task. This is the only way that the UK can achieve and maintain the status of a global leader in the digital world.

b. Terms of Reference

11. The original Terms of Reference were as follows. The Industry Working Group was asked to:
    (1) consider how different technologies can help provide evidence of identity and intention to authenticate when documents are executed electronically;
    (2) consider the security and reliability of different technologies used to execute documents electronically;
    (3) 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;
    (4) produce best practice guidance for the use of electronic signatures where individuals, in particular vulnerable individuals, execute documents electronically;
    (5) consider challenges arising from the use of electronic signatures in cross-border transactions and how to address them;
    (6) consider potential solutions to the practical and technical obstacles to video witnessing of electronic signatures on deeds and attestation;
    (7) consider how these potential solutions can protect signatories to deeds from potential fraud; and
    (8) make recommendations to Government and to others on proposals in areas where the group consider reforms should be made.

12. The Terms of Reference that were addressed in the Interim Report were (1), (2), (3), (4) and (6) and (8). Those terms that remained outstanding following publication of the Interim Report were therefore those numbered (5) and (7), with room to add to the list of recommendations under (8).

13. These outstanding terms are therefore addressed in this Final Report. Additionally, due to the difference of views within the Group itself concerning certification/ accreditation, this was one of the matters put out by the Joint Chairs for public consultation. That consultation was commenced on 22 July 2022, and the deadline was extended from its original one of 9 September 2022 by 14 days only in order to incorporate additional responses. The questions that were posed for consultation were as follows, with agreement or disagreement sought by consultees together with comment generally. The questions were:
    (1) eSignature platforms should self-certify against a set of principles formulated, maintained and publicised by an industry or governmental body (such as the Information Commissioner's Office, LawTechUK or the National Cyber Security Centre). Do you agree? What (sort of) body is best placed to do this?

(2) Such certification should be based on an evaluation of the way in which the relevant software performs and functions. The underlying code is not a relevant subject for external evaluation. Do you agree?
(3) Self-certification should cover both (a) the functionality of the service(s) offered by the platform (in establishing whether those services meet the requirements for an advanced or qualified electronic signature) and (b) the security of the platform. Do you agree? Are there other areas against which e-signing platforms could usefully self-certify?
(4) Self-certification against these benchmark principles should be a process performed on an annual basis. Do you agree?
(5) Self-certification should not be mandatory but should instead be a choice made by platforms on the basis of market considerations. Do you agree?
(6) A failure to adhere to self-certified standards should be addressed through a complaints and investigation procedure, resulting, where appropriate, in enforcement orders, publicity orders and/or fines. Do you agree?

14. There was broad agreement for most of these proposals from the majority of consultees, but also significant disagreement from some industry consultees, and also from some members of the Group. This subject is addressed in more detail in Sections E and F of the Final Report. It is the one area of the Group's work where consensus could not be achieved. There are respectable arguments both for and against certification, accreditation and self-certification, and the overall conclusion of any particular member of the group or consultee is dependent upon the different weight given to the individual features or arguments, together with the view of some in the industry that it is for the platform providers to achieve confidence in the market and without that, such platforms would either not be used or would fail. The Chairs take the view that such an approach fails to take account of individual consequences of those affected by any such failures (were they to occur) and that prevention is better than cure, but recognise that prevention is not always possible and over-regulation of any sector can be detrimental.

15. All that the Group can do in these circumstances is to present the different possible approaches, outline the considerations that arise in respect of each approach, and leave any future decision to the Executive.

c. Interim Report conclusions and the outstanding Terms of Reference

16. Parts of the Interim Report have been reproduced in this Final Report in order that it can conveniently be read and considered as a stand-alone Report. However, for full consideration of the Interim Report and the other Terms of Reference addressed in it

in detail, recourse should be had to that earlier document. Its contents are not reproduced verbatim in this Final Report.

17. The Group's recommendations on the outstanding Terms of Reference that are addressed herein have been collated with its earlier ones, so that the recommendations in this Final Report at Section G are comprehensive, and there should be no need for a reader to consult separately the recommendations in the Interim Report.

18. There are isolated further explanations of some limited detailed areas of the Interim Report (for example one technical legal point concerning the law of Northern Ireland, which is slightly different to the law of England and Wales in one particular respect). These further explanations are provided to assist those who responded specifically to the Interim Report on these discrete areas. In so far as this Final Report addresses the law, that is the law of England and Wales (as it was in the Interim Report).

d. Progress in field of electronic documents generally

19. The Covid-19 pandemic demonstrated that as well as the natural evolution and gradual adoption of technology, which occurs naturally over time, driven by technological advancement, entrepreneurship and usually business need, there are occasions when there is adoption of technology due to sudden increased societal need. The inability of a person, for example, during the lockdown period, to be legally permitted to have a will physically witnessed in the way required, and legal innovation in order to permit that to be done (at a time of higher mortality), is an example of existing technologies being redeployed or adopted in certain areas at a speed that could not have been contemplated in the different circumstances of 2019.

20. However, as well as the wider societal acceptance of the use of technology in this way, there is an obvious realisation that the law needs to keep pace with technology. On 11 October 2022 the Electronic Trade Documents Bill ("ETD Bill") was introduced by the Department for Digital, Culture, Media and Sport ("DCMS"), having been drafted by the Law Commission of England an Wales. A call for evidence on the Bill was published at the end of 2022.[12] The ETD Bill relates to trade documents, such as bills of exchange, promissory notes and bills of lading (amongst others) which currently require physical possession in order to perform their legal function in facilitating international trade. The ETD Bill seeks to remove the legal blocker that currently prevents electronic versions of these documents from being possessed,

[12] 2 December 2022 Special Bill Public Committee, https://committees.parliament.uk/call-for-evidence/3001/

thereby granting them the same legal status, and allowing them to perform the same legal function, as physical paper documents.

21. The Bill sets out specific "gateway criteria" in order for a document in electronic form to qualify as an electronic trade document. These criteria are designed to replicate the salient features of paper trade documents, such as exclusive control and divestibility or transfer to others. This would achieve the policy objective of enabling certain trade documents in electronic form to be used in the same way as their paper counterparts.

22. Whilst, for most purposes, electronic documents are already perfectly acceptable alternatives to their paper counterparts, the ETD Bill deals with a very specific type of document. Possession is the operative concept in the Bill because the types of trade documents the Bill is concerned with rely on possession to achieve their commercial and legal functions. Until the advent of distributed ledger technology, it was very difficult, if not impossible, to replicate the salient characteristics of paper (and therefore possessable) documents in electronic form. The Bill functions so as to apply traditional concepts of "possession" to electronic trade documents. The Bill has adopted a "technology neutral" approach to the proposed legislation, an approach which the Group has strived to match. There are undoubtedly commercial advantages for whichever platforms emerge from business competition as the market leaders, but whatever approach is adopted now can only survive in the view of the Group if it is technology neutral. Otherwise, there is a risk that specifying requirements would soon lead to redundancy of those requirements, which would then be rendered obsolete in short order. It would be very difficult for anyone now, whether industry specialist or Parliamentary counsel, to predict what technological advances might occur in the future, even in the next 12 to 18 months. Developing industry standards is a far more efficient way of "regulating" – or more accurately ensuring – such an issue. The general industry reality ought to be recognised.

23. Technological innovations, which allow an "electronic document" to replicate the features of paper, challenge existing legal principles which have grown up and been refined over hundreds of years, before such innovations existed. A trader in Victorian times trading internationally would have known very clearly the value to him of a bill of lading, which would be physically transferred to him, and which he would therefore come to possess, as part of his or his company's acquisition of the cargoes to which such bills related. The physical possession of that piece of paper would be very important because it was what enabled him to trade that cargo in the numerous exchanges where such transactions took place and, ultimately, to secure delivery of the cargo. There is in principle no reason why in the 21st century such status could not be granted to electronic trade documents, and every reason why it should. But law reform is required to do so and the passage of the Bill is necessary to achieve that.

24. Equally, e-Signatures are merely the electronic manifestation of what has been used for hundreds of years. A mediaeval nobleman, wearing a unique signet ring, would impress it into hot wax to seal a document; the Victorian trader would sign documents using a quill pen, having more important documents witnessed to avoid future disputes. A 21st century consumer, buying a car on finance, may do so without ever having sat in that car, having viewed it virtually in the showroom or even at home. It is only logical, as the Group observed in the Interim Report, that the finance agreement for the transaction be signed electronically.

25. However, in order that this can be achieved in a wide range of scenarios, both for individuals and in commerce, there are two main areas that have to be assured. First, security and proof, namely that such an e-Signature is at least as reliable (if not more so) than the older paper and wet ink equivalent. Secondly, that society in general ascribes the same effect to both approaches to demonstrating assent, and can utilise the benefits of e-Signatures with confidence. These are mutually reinforcing. The more robust and reliable the technology or platform is, the more everyone will take comfort from using these methods of execution.

26. Finally, as outlined above, given future developments in the technology field are, or are likely to be, of a type that cannot be predicted, the current approach to adopting both of these principles has to be technology neutral. This is consistent with the approach of other organisations to electronic signatures, for example that adopted by the UN Commission on International Trade Law[13] and also by DCMS/DSIT in all of its work in the digital field.

27. This therefore brought the Group to consider what could safely be described as the one area of controversy between its members, and this is the subject of certification or accreditation.

28. In the Interim Report the Group recommended that the three types of signature recognised by the EU under the eIDAS Regulation[14] be used. This Regulation was passed within the auspices of Directive 1999/93/EC on a Community framework for electronic signatures ('Electronic Signatures Directive') which established a legal framework for electronic signatures and associated certification services.[15] That framework had been updated by the eIDAS Regulation[16] which aimed to create a uniform regime for electronic identification and trust services throughout the EU. In the UK, the eIDAS Regulation was implemented by the Electronic Identification and

---

13 UNCITRAL Model Law on Electronic Signatures (2001) United Nations Commission On International Trade Law

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

15 The Directive was implemented in the UK by the Electronic Communications Act 2000 and the Electronic Signatures Regulation 2002 (SI 2002 No. 318)

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

Trust Services for Electronic Transactions Regulations 2016 and section 7 of the Electronic Communications Act 2000. 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. The second section is concerned with Trust Services and electronic signatures.

29. 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, namely (1) Simple (2) Advanced Electronic Signature ("AES") and (3) Qualified Electronic Signature ("QES").

30. The EU in June 2022 published another version of eIDAS, which is known as eIDAS2 or eIDAS 2.0. It aims to update the original eIDAS and make it more uniformly acceptable, with a view to its becoming more widely used across all member states, including being compulsory in some instances. The five core trust services to which it relates are e-Signature, e-Seal, electronic time stamps, electronic registered delivery services and certificates for website authentication. The EU Commission considered that slow application rates under eIDAS and other shortcomings in the Regulation had become apparent, as it was expressed, "due to technological developments that offer new types of electronic identity solutions, such as electronic ledgers. User expectations have also changed, with smartphones providing smooth, mobile online transactions. Users expect seamless possibilities to share various data attributes online, with a high level of control and security safeguards embedded in the system".[17] However, eIDAS 2.0 is not yet adopted and is expected to occur sometime in the middle of 2023, in parallel with developments working towards the EU Digital Identity Wallet.

31. 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). QTSPs are regulated in the United Kingdom 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).[18]

32. 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, and the Group has not identified any publication within or emanating

---

17 https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf

18 Appointed in September 2021 to accredit certifying bodies using ISO 17065:2012.

from the EU, including from the Commission, that suggests that will change under eIDAS 2.0.

33. To be a QES, a signature must first fulfil the requirements of an AES.[19] 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 described in the Interim Report at [69] to [72].

34. 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.[20] Given the requirement for regulation of QTSPs by UK eIDAS by the ICO, and for the requirement for accreditation of conformity assessment bodies by UKAS, the Group naturally turned to consider the desirability or otherwise of certification or accreditation of providers of e-signatures in the UK generally.

35. It ought also to be noted for completeness that neither AES nor QES is currently widely used to execute documents governed by English law. An increasing number of requests to use digital signatures (AES and QES in Europe, and digital signatures in the US) have however been observed by the Group in 2022 and 2023.

e. Certification/Accreditation

36. This important subject is dealt with in detail in Section E. The subject generally was put out to public consultation to obtain the largest possible range of views, and other bodies were also expressly invited to provide their input, in particular DCMS itself.

37. The general weight of the overall input on this subject was that some sort of accreditation be adopted. However, there was some isolated but strong opposition to this, predominantly from areas within the industry itself and from existing e-Signature platform providers. There were three broad areas of concern. These were that

---

19 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 of a signature that:

(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.

The requirements for all forms of signature under EIDAS are set out in detail in the Interim Report.

20 See Enisa, *Security guidelines on the appropriate use of qualified electronic signatures*, Annex D.1.

regulation can be expensive, cumbersome and inefficient, and would delay innovation; that there was no suitable body in existence that ought to be required to resolve a problem that did not currently exist; and finally, concerns relating to the integrity or safety of intellectual property in the underlying code used by existing providers.

38. The counter-arguments to each of these are set out in Section E.

39. The Final Report does not therefore present a positive recommendation one way or another on this point, although it was the view of the majority of the group members that some form of accreditation be adopted. All that the Final Report does in these circumstances is to outline the different points that arise and have been considered in respect of each approach, and leave decisions of policy and future development to the Executive.

f. Conclusions

40. It is clear that the demand for electronic execution facilities continues to increase. At the same time, the technological capacity to meet each aspect of that demand is also increasing. The next step, and one which this Report aims to facilitate, is to ensure that those potential solutions are properly matched with the requirements and problems that they can best address, and that users are confident participants in the whole process.

41. The Interim Report focussed mainly on the rudiments and day to day practicalities of this matching process. This Final Report addresses two concerns that are broader in their effects and yet more specific in their focus: how to optimise the advantages of electronic execution of documents in a cross-border context, and how best to mitigate the risks of fraud.

B. Outstanding Terms of Reference

42. The two main areas in which the Terms of Reference remained to be addressed by the Group concerned specific challenges in the use of electronic signatures in cross-border transactions,[21] and how potential solutions to the use of electronic signatures generally (both domestically as in solely within the UK, and also internationally) could protect signatories to deeds from potential fraud,[22] together with associated recommendations.

43. These will be considered sequentially.

a. Cross-border challenges

44. Legal agreements underpinning cross-border transactions may in practice need to be drafted and executed in accordance with the law relevant to the parties and the governing law in order to minimise the risk that the transaction turns out to be invalid or not binding. The uncertainty around the interpretation of different jurisdictions' electronic execution laws, and the requirements and formalities surrounding electronic execution, can give rise to challenges of increased costs, delay and uncertainty, all of which can hinder adoption of e-signing. Even within the United Kingdom, differences can apply as between, say, the law applicable within England and Wales and that of Scotland.[23]

45. The Law Commission Report on Electronic Execution of Documents states:

> "Given the increasingly cross-border nature of business, it is not appropriate to consider the domestic landscape in isolation. In international transactions, parties will want to ensure that their documents are executed in such a way as to enable their recognition, registration or enforcement in other jurisdictions. These issues will also arise when a document executed in this country needs to be notarised and used in

---

21 Term of Reference (5) considering challenges arising from the use of electronic signatures in cross-border transactions and how to address them

22 Term of Reference (7) considering how these potential solutions can protect signatories to deeds from potential fraud

23 See paragraph 7 (Conflicts of law issues) of The Law Society Company Law Committee & The City of London Law Society Company Law & Financial Law Committees Note on Electronic Execution of Documents for a discussion of the circumstances in which the parties to a document to be signed using an electronic signature may wish to seek advice from counsel in another jurisdiction.

another jurisdiction outside a transactional context – for example, a marriage certificate or divorce decree." [24]

This approach as set out by the Law Commission is one that the Group both understands and fully endorses.[25] The challenges presented by such transactions are explored further below, with suggestions and recommendations as to how these may be addressed or overcome.

1. What confidence is there that a signatory e-signing in a particular jurisdiction is doing so validly?

46. Establishing whether electronic execution of a document is valid and/or enforceable in a particular jurisdiction, on a cross-border transaction, may necessitate local law opinions, which can be time consuming and costly. The question is whether, under the laws of the relevant jurisdiction, the signatory has authority to sign electronically, and if so in what form. As the Law Society Company Law Committee & The City of London Law Society Company Law & Financial Law Committees point out in their Note on Electronic Execution of Documents:

"Article 9(1) of the EU's e-commerce directive 2000/31 (the E-commerce Directive), regulating matters within the EU, states:

"Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means."

There are various exceptions to these general obligations. First, the E-commerce Directive does not apply to certain activities, including gambling, taxation and telecommunications (Article 1(5)). Secondly, Article 9(2) permits member states to lay down that the general obligations in Article 9(1) do not apply to all or certain types of contracts falling into the following categories:

- contracts that create or transfer rights in real estate, except for rental rights;
- contracts requiring by law the involvement of courts, public authorities or professions exercising public authority;
- contracts of suretyship granted and on collateral securities furnished by persons acting for purposes outside their trade, business or profession;
- contracts governed by family law or by the law of succession.

The Brexit related Trade and Co-operation Agreement regulating matters between the EU and the UK and signed on 31 December 2020 (the TCA) also contains provisions related to electronic execution of contracts. Broadly, it provides that each

---

[24] Para 2.38, Commission, *Electronic Execution of Documents (Law Com No. 386, 2019)*

[25] See also CLLS-and-Law-Society-E-signatures-paper-October-2022.pdf (citysolicitors.org.uk)

of the UK and the EU must ensure that contracts can be electronically executed and that its law does not create any obstacles to the use of electronic contracts, subject to certain possible exemptions. The list of exemptions is similar to, but not exactly the same as, the provisions relating to electronic signatures in the E-commerce Directive.[26]

Respondents to the Law Commission consultation noted that the process and cost of obtaining local advice on this point is a significant deterrent to adopting e-signatures for cross-border contracting.[27]

47. This is a role sometimes undertaken by Notaries in the originating country (particularly in Europe) who may be required to certify not only the identity, capacity, understanding and authority (where the signature is made in a representative capacity) of the signatory, but also its binding effect (whether electronic or otherwise). A challenge for Governments everywhere is to seek to clarify (and amend if necessary) the law in order to confirm to all who need to know that an electronic signature is valid and binding. As to the type of e-signature, it would be helpful if Governments were to encourage the adoption of, and agree, an international standard of electronic signature which would be recognised in all participating jurisdictions as has been done in the case of the EU (910/2014) and also by UNCITRAL who have created a model law on electronic signatures.[28] Were the UK to adopt the UNCITRAL Model Law on Electronic Signatures, this would be a highly constructive step, both in terms of its substance and its signal to other jurisdictions. Article 12 is particularly pertinent to this point:

Article 12. Recognition of foreign certificates and electronic signatures

1. In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had:

   (a) To the geographic location where the certificate is issued, or the electronic signature created or used; or (b) To the geographic location of the place of business of the issuer or signatory.

2. A certificate issued outside [the enacting State] shall have the same legal effect in [the enacting State] as a certificate issued in [the enacting State] if it offers a substantially equivalent level of reliability.

3. An electronic signature created or used outside [the enacting State] shall have the same legal effect in [the enacting State] as an electronic signature created or used in [the enacting State] if it offers a substantially equivalent level of reliability.

4. In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph 2 or 3,

---

26 CLLS-and-Law-Society-E-signatures-paper-October-2022.pdf (citysolicitors.org.uk) at [3.3]

27 Paras 2.42, 2.43 Commission, Electronic Execution of Documents (Law Com No. 386, 2019)

28 https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures

regard shall be had to recognised international standards and to any other relevant factors.

5. Where, notwithstanding paragraphs 2, 3 and 4, parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law

2. Enforcement risk

48. The challenge that arises upon enforcement concerns e-signing a contract governed by English law that a signatory may wish to enforce elsewhere, outside the jurisdiction:

"There is … a risk that an English law governed agreement of one of these types that has been electronically executed may not be enforced by the courts of a member state if that member state has taken advantage of any of the exceptions to these general obligations (in relation to the E-commerce Directive, member states are required to notify the Commission where this is the case). Parties entering into such types of contract may therefore wish to take local law advice to check whether or not local law supports the signature of such contracts by electronic means."[29]

49. If English law transaction documents require a party to pursue legal action in a foreign jurisdiction, local legal advice may be required in order to consider whether the use of electronic signatures on the underlying transaction documents would impact on the outcome of those proceedings. If an English legal judgment needs to be enforced in another country (e.g. where a transaction concerns assets held overseas and enforcement is required in order to deal with those assets), there are a number of international conventions already in place governing its mutual recognition and enforcement. It seems unlikely to the Group that the operation of such conventions would necessarily be affected by virtue of the signatures to the underlying contract or contracts being electronic only. However, given the potential issues around the cross-border enforcement, counterparties may need to give additional thought to their enforcement strategy for such contracts. The method of signing (electronic or wet-ink) should align with that strategy, with local law advice obtained for the relevant jurisdictions. Particular consideration is required in any cross-border transactions where a claim may arise under the exclusive jurisdiction of a foreign court, for example rights relating to real property or public registers (e.g., patents and trademarks). Once more, such uncertainty could be significantly reduced by adopting the UNCITRAL Model, and particularly its principle of non-discrimination between domestic and foreign electronic signatures.[30]

---

29 CLLS-and-Law-Society-E-signatures-paper-October-2022.pdf (citysolicitors.org.uk) at [7.5]

30 01-89959-p1.dg.qxd (un.org) at [27].

3. Place of incorporation vs governing law of a transaction

50. Notaries and others tasked with ensuring that documents executed abroad are valid in that they comply with local requirements there are well aware that the legal formalities in the specific jurisdiction of execution must have been observed. Equally, documents that are to be used in a foreign jurisdiction must comply with the law of the place of signing, and if this is to be in England and Wales, the requisite requirements of English law must be complied with too. This may require amendments to be made to certain documents that have been drafted abroad for execution here, for example to demonstrate they have been executed as a Deed. This applies whatever kind of signature is made, whether electronic or wet ink.

51. This could be described as a challenge to the use of electronic signatures (whether for use domestically or cross-border). The desirability of abolishing deeds in their entirety has been discussed within the Group generally, as has reforming their requirements, although these are wider issues for potential future law reform and outside the Terms of Reference of the Group. Certainly, it is the view of the Group that different or higher standards of execution within the UK (such as, for example, the requirement of a deed for some company documents) can inhibit cross-border acceptance.

4. Lack of certainty as to how courts will evaluate e-signatures, and no international standard on evidential value

52. The Group noted that, outside of the EU, there is uncertainty around the law and also how different platforms meet local requirements. This uncertainty is what led to the original Law Commission Report.

53. One option for resolving this (or at least encouraging greater certainty) is the consideration of certifications of platform providers, which could create base/minimum standards for effective e-signing, in order to promote trust in and encourage the use of e-signatures, and to assist in addressing some of the challenges outlined, as well as potentially moving towards or encouraging the establishment of an international standard. Self-certification has a high potential to assist with this challenge, which extends beyond cross-border transactions.

54. As to the subject of evaluation of the evidential weight of an e-signature, this is likely to include not only whether the signature complies with local legal requirements (for example whether the document in question was executed as a deed and signed in the presence of a witness) but also whether the electronic signature was made by the relevant signatory with the intention of being bound, and was capable of being linked to the identity of the signing party. Whilst there are platforms which will “validate” certain electronic signatures (such as a QES) the terms and conditions attaching to such a validation will often exclude or limit responsibility where the signature was

made by someone else, to whom perhaps the signing party had disclosed its private key, username or password.

55. In terms of cross-border transactions and international standards, Paragraph 3 of Article 6 "Compliance with a requirement for a signature" of the UNCITRAL Model Law on Electronic Signatures sets out a number of conditions which need to apply in order that a signature may be treated as reliable. These standards were first drafted in 2001. UNCITRAL has been very active in the area of electronic commerce having created a model law on e-signatures. It is currently working on draft provisions on the use and cross border recognition of Identity Management and Trust Services.[31]

56. These dovetail with the work being undertaken in the UK such as that by DCMS on Digital Identity.[32] Although Digital Identity is outside the scope of the Group's work, and one can of course (and currently can only) execute an e-signature in the UK without a Government- approved Digital Identity, in some circumstances they can be seen as raising such closely related issues that the overlap is considerable. The unique feature of Digital Identity in the UK, compared to other countries including those presently in the EU, is that identity cards are not compulsory in the UK and never have been. Indeed, there has been a historical objection within the UK to such documents, with the compulsory requirement for such identity documents often being equated to infringement of civil liberties. A citizen can be required to produce their driving licence, as a statutory condition to driving a motor vehicle on a public road is that the relevant licence is held. Sometimes driving licences are used as a means of demonstrating identity and age in other circumstances, for example when purchasing alcohol. However, there is no requirement upon every adult member of the population to have a driver's licence and many do not do so. The average number of adults over a 5 year period of 2014 to 2019 in the UK who did was 74%.[33]

57. Possession of a Government-approved digital identity (if or when such is available) would make proof of identity, and therefore one of main challenges relating to evidential weight, namely whether the signature was capable of being linked to the identity of the signing party, more straightforward. However, other steps are available to achieve the same end, such as third-party authentication by another means (an app or message to a pre-approved secure location such as an email address) or biometrics.[34]

58. When dealing with the evidential value placed on documents and signatures by Courts in foreign jurisdictions, emphasis should be placed on establishing an international norm through organisations such as UNCITRAL. When adopting new

---

31 https://uncitral.un.org/en/working_groups/4/electronic_commerce

32 This now sits in the newly formed Department for Science, Innovation and Technology (DSIT).

33 https://www.ethnicity-facts-figures.service.gov.uk/culture-and-community/transport/driving-licences/latest

34 Also, see *https://www.electoralcommission.org.uk/i-am-a/voter/voter-id?gclsrc=aw.ds:* from 4th May 2023, photo ID will be required to vote in certain elections.

standards relating to electronic signatures in England regard should be had to any existing standards which may emerge internationally, such as UNCITRAL, eIDAS (within the EU, intended soon to become eIDAS 2.0 in 2023), and UETA and ESIGN Act standards in the US.

5. Inconsistent definitions of/requirements for e-signatures in different jurisdictions

59. Although UK eIDAS Regulations allow the legal effect of EU eIDAS qualified trust services to continue to be recognised and used in the UK, no reciprocal agreement currently exists. This means UK eIDAS Regulation qualified trust services are not automatically recognised and accepted as equivalent in the EU.[35] QTSP mutual recognition between EU-UK (for QES) is therefore needed, along with more bi-lateral recognition agreements (based on similar methods and certifications).

60. Mutual recognition (as in the case with notaries) would be mutually beneficial, but in the interim users are currently more likely to be best advised to utilise a QES issued by a QTSP based within the EU. This would reduce the likelihood of rejection due to any differences in UK eIDAS, that likelihood potentially becoming greater later in 2023 and into 2024 with the introduction of eIDAS 2.0.

61. The UK & Singapore Digital Economy Agreement has agreed, amongst other things, "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."

    This agreement is something that would be, at least partially, fulfilled by the Electronic Trade Documents Bill,[36] and Singapore, as a significant geographical hub for international trade, has many bi-lateral free trade agreements ("FTAs"), including with the United States, China, Costa Rica, India, Japan, Jordan, New Zealand, Republic of Korea, Panama, Peru, Sri Lanka, the European Union, United Kingdom and Turkey.[37]

62. Trade has been described at a Government level in Singapore as "fundamental to our economic survival" as it has "no natural resources, but….one precious natural endowment and that is our geographical location." PSA Singapore is the largest container trans-shipment port in the world, and has been described as "a unique interchange in the world, connecting East and West, Europe, Middle East, India, China. The port is central to the growth of the maritime industry, responsible for 160,000 jobs in Singapore today."[38]

---

35 https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/

36 Appendix 7.

37 https://www.trade.gov/country-commercial-guides/singapore-trade-agreements

38 Minister of Health Ong Ye Kung Ministerial Statement, 6 July 2021

63. To engage in significant volumes of international trade, through transactions which are increasingly conducted on a wholly electronic basis, the UK must be at least equal with the other international participants in terms both of its technological advancement in electronic formation of such relations, and its legal recognition of those advancements.

64. Mutually recognised worldwide standards for the different types of electronic signature, and a mutually recognised method of linking the electronic signature to the identity of the signer remain, to the regret of the Group currently, something of a distant prospect. However significant progress is being made in many areas, including the EU's latest eID drafts, the UNCITRAL model, as already outlined, and work by groups such as the Open Identity Exchange (OIX).[39] Once such standards are agreed, the issues of user and regulator comfort and adoption of electronic signatures remain open.

65. Paragraphs 2.55-2.57 of the Law Commission Report state that some consultees called for a more consistent approach on execution formalities across the UK and other jurisdictions, along with cross-border initiatives aimed at streamlining these processes, and others suggested that robust technologies (that were able to validate both identity and intention to authenticate) should be enough to satisfy the requirements of any jurisdiction.

66. On a practical level, there can be problems in electronic signing (whether within one single jurisdiction or cross border) where more than one electronic signing platform is used. This is because conflicts can adversely affect (and also therefore corrupt) digital signatures which have already been attached to a document. As an example of one solution to this, it is the current intention of notaries in England and Wales that they choose and adopt one signing platform for all parties. By doing this, they can not only exercise some control over how the document is circulated (and in what order) and signed, but avoid the possibility of a signing platform used by another party affecting the workflow.

67. Given the worldwide adoption of what have effectively become market leaders (if not monopolies) in some software applications, such as word-processing and document creation, over time it may be that the problems of different platforms for the same international transactions diminish or even disappear. Similar difficulties in a different technological field arose in the 19th century with the difference between narrow-gauge[40] and broad-gauge[41] railways. A Royal Commission was required to resolve that difference, which resulted in the Regulation of Gauge of Railways Act 1846.[42] Such an investigation and legislative intervention on platform differences and

---

39 https://openidentityexchange.org

40 Now more commonly referred to as standard-gauge

41 As favoured by Isambard Kingdom Brunel on the Great Western Railway (“GWR”)

42 Which adopted narrow-gauge for all future railways but permitted GWR to continue with broad-gauge

software is not only unlikely, but would also be unnecessary, as the pace of both technological innovation and market competition is such that both these things will lead, essentially, to the survival of the fittest.

6. Lack of assurance that e-signing solutions/platforms meet different global requirements, with no equivalent to ISO standards used for information security

68. The current EU implementing regulations for eIDAS deal with technical standards and the regulation for QES refers to the ISO/IEC standards (International Organisation for Standardization/International Electrotechnical Commission). These bodies establish the general concepts and principles of IT security and specify the general model of assessment to be used as the basis for evaluation of security properties of IT products.

69. Furthermore, the European Committee for Standardisation (CEN) has developed, under the EC's standardisation mandate M/460, standards for qualified electronic signature and seals creation devices where data is held in an entirely but not necessarily exclusively user-managed environment (e.g. published standard EN 419 211). For further information, and a list of standards, readers should refer to eIDAS[43] itself, but with the awareness that eIDAS 2.0 is planned.

70. Although these and associated ISO standards are acknowledged and often accepted by the technology providers, they are not currently internationally used in all countries beyond the EU and the UK. Such standards are often recognised as a best practice default starting point that numerous nations take account of when developing their own legislation and standards references. It should also be noted that this is a moving target as technologies develop and even within the EU there is ongoing work to align all related member state requirements, including the pending arrival of eIDAS 2.0 to encourage wider adoption and greater confidence in use.

71. In addition, ENFSI (European Network for Forensic Science Institutes) has published standards and maintains a Best Practice Manual for the Forensic Examination of Handwriting (in wet ink and electronic signature forms), including guidance for tools to help examine handwritten signatures and present findings to Courts and other interested parties.

72. The lack of an international and universal technical standard is undoubtedly hindering, for the moment, more widespread international adoption generally. It is outside the scope of this Report to consider the role in which the UK could potentially take the lead in terms of an initiative in driving a single international standard.

---

43 https://ec.europa.eu/futurium/en/system/files/ged/celex_32016d0650_en_txt.pdf

However, it is certainly an objective that would, in the view of the Group, be valuable to pursue.

7. Financial institutions: reluctance to e-sign, imposing additional requirements (such as requirement of wet ink in addition to e-signatures, or forcing a hybrid signing where some e-sign and some wet ink sign)

73. It is not clear why some financial institutions in the UK continue to insist on wet ink signings in certain transaction. As banking and finance are important industries for the UK, the Group considers that the adoption of electronic signatures by financial institutions to be of particular relevance in assessing the challenges to the use of electronic signatures in cross-border transactions.

74. There appears to be some reluctance from certain institutions to utilise e-signing for financial transactions. The need remains for education and reinforcement of the positive attributes of e-signing. No data is available for any increase in confidence amongst financial institution users from the publication of the Interim Report of the IWG in February 2022, but there was some noticeable and beneficial public and press comment following on from that. There is also some anecdotal evidence from members of the Group that, in practice, there is an increase in the incidence of financial institutions creating AES/QES-only signing policies.

75. Some institutions now appear to have dispensed with a “signature” at all for some transactions, even those that would have been subject to the requirement of a formal signature historically. For example, telephone banking uses passwords and answers to memorable questions; other institutions such as private pension providers send a series of emails which require authentication; others use authentication apps which provide a six-digit code valid for short periods (typically 60 or 90 seconds); some still rely on codes sent by SMS to pre-approved mobile telephone numbers.

76. There appears to be some evidence of an increasing acceptance by some European financial institutions of e-signatures where they have been authenticated by a public official.

8. How to identify countries outside of the EU that have adopted e-signing standards that trend towards an international standard? How can the ICO help in this regard?

77. As part of the group’s recommendation that the ICO expand their role to include more involvement in regulation (and potentially also self-certification as explained below per recommendation 1), consideration was given to what more could be accomplished by the ICO in order to assist.

78. For e-Signing in the UK, the ICO (or similar) could potentially act as a reference source of information (sometimes in the vernacular described as the 'go-to' source)

that has been subject to some level of fact checking once submitted by any vendor interested in demonstrating the level of provision of their e-signing platform.

79. For e-Signing in multiple jurisdictions (and certainly those outside the EU), users can presently only be advised to make the relevant jurisdiction checks and/or seek informed advice. Such a recommendation should also appear on a central resource (which could be the ICO site or similar), in keeping with the reference source suggestion above. In addition to this, the ICO might also publish links to other international or governmental organisations who keep similar lists in other jurisdictions (for example, each member state of the EU will have a designated register for QTSPs) or provide guidance on the different international standards (or links to where that guidance could potentially be found). The site could also include and publish reference source pages (such as EU's eIDAS and eID pages, legal reference sites, foreign government e-Signing guidance pages, and similar sources of information for those engaged in cross-border transactions).

80. It is questionable whether such information and guidance could dispense entirely with the need to obtain locally-sourced legal opinions on the use of electronic signatures, but this would of course depend upon the type and size of the transactions. Over time, as e-signing processes and laws align internationally and become more widely accepted, it may do so. It may also reduce the risk to an acceptable level for some parties and transactions. Including the relevant links centrally, so that the information can be sourced directly by a potential user (but by accessing a particular nation's own sources) would be more suitable and save either the ICO, or a comparable institution, from the highly challenging task of sourcing and maintaining such information itself.

81. There are a variety of disparate resources available separately already to those seeking clarification or general information about the acceptability, validity and formality requirements of e-signatures. Some of these are maintained by law firms and some are subscription-based products. Whilst there is no such universally recognised compilation, most e-signing platforms have summary guides covering such information.

82. Here, for convenience, is a link to a list of countries that have adopted the UNCITRAL model law on electronic signatures: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures/status

9. What is the relevance of the location of the platform servers executing the document?

83. For some providers and services, the user is able to select the location of the services holding the platform.[44] Providers should be encouraged to promote a list of

[44] One example being Amazon Web Services

locations available, and it may be that clarity on this is required. There are potential data protection, tax and other implications, depending upon the transactions being undertaken and the laws of the relevant overseas jurisdiction.

84. The Group recommends that some guidance be drawn up on the extent (if any) to which the location of platform servers is relevant in legal terms. There are complex legal issues that arise in relation to the physical location of servers and in which jurisdiction they are to be found, and this is a subject that requires further consideration and is outside the remit of the Group. The Law Commission, however, is currently engaged on a project examining these issues, and expects to produce its Final Report in 2024.[45]

85. If a signing platform automatically saves a copy of a document, attention needs to be paid as to the location of the server storing the *saved* document in case relevant GDPR[46] provisions are breached or privacy notices and policies need to be adjusted.

10. Recent developments in the UK Government's digital agenda to assist in using electronic signatures in cross border transactions

86. The signatures and seals of public officials for use in foreign countries are frequently verified by a Government Agency, Embassy or High Commission in a process known as legalisation. For this purpose, the world can be divided into three main categories:
(1) Those countries requiring no such verification – principally between Commonwealth and some former Commonwealth countries;
(2) Those countries which are party to the Hague Convention 1961 on the abolition of legalisation requirements. There are over 100 member countries where verification is achieved through one competent authority (in the case of the UK the Foreign Commonwealth and Development Office "FCDO") issuing an "Apostille";
(3) The rest of the world which require not only a form of Apostille but also legalisation through the Embassy or High Commission in the issuing State.

87. Until recently, the FCDO only issued the Apostille on paper. The service has now been extended to include the electronic Apostille (or e-APP). This means that for over 100 countries where it was not previously possible to prepare or sign documents in electronic form, it has now become possible. This event has far reaching consequences for cross border documents signed within the UK.

88. For some years The Notaries Society has been working with the FCDO to make available to public officials in the UK an electronic version of the Apostille (shortly known as the e-APP) and which has for a long time been promoted among its members by The Hague Conference on Private International Law. In December

---

45 Law Commission of England and Wales, "Digital Assets: Which Law, Which Court?" Law Commission to review how private international law applies to digital assets and other emerging technology - Law Commission

46 General Data Protection Regulation implemented in the UK by the Data Protection Act 2018

2021, the FCDO announced its intention to begin a pilot project with a view to implementing the e-APP. Working closely with the FCDO and their technical advisers, the Notaries Society participated in the trial and in September 2022, the FCDO announced the official launch of the e-APP.

89. Although member countries agree that the use of an electronic apostille (as opposed to a paper one) is not a valid ground of objection to acceptance of a document, there are still some States which are parties to the Hague Convention whose internal laws have not yet accepted electronic documents or signatures, or whose laws require that certain signatures are not generated remotely. This is, of course, one of the advantages of an electronic signature platform. This problem has at its heart the difficulty of identifying people online, which is being widely addressed both by Governments, industry and the professions.

90. The advent of the e-APP in the UK will, potentially, encourage other countries to accept such documents and signatures.

91. When dealing with cross-border documents, one of the primary checks which any public official should make is to establish that the document will be accepted in the receiving State in electronic form. This is reinforced by the guidance given by the FCDO on its website where it advises users on relevant checks.[47]

92. One practice which the Group were told has arisen as a practical step is to prepare a duplicate set of documents in electronic form to accompany the paper version. Both would then be sent to the recipient jurisdiction with a request to confirm whether the electronic version will be acceptable in place of the paper version. This is one way in which the acceptability of electronic signatures in other jurisdictions can be tested; however, it is cumbersome, has the potential for delay, and is somewhat contrary to the ethos of what is hoped to be achieved, namely speedy transmission of documents that are signed electronically.

93. In summary, one of the main challenges attached to the use of e-signatures in cross-border transactions is in persuading more countries to join the e-Apostille convention, reforming the laws to accept electronic documents and signatures and to set internationally agreed standards. Eventually that wider adoption will occur, but until it does, all that can be done is persuasion and encouragement.

b. Protection from fraud

94. The second outstanding area from the Terms of Reference is how potential solutions to the use of electronic signatures generally (both domestically, as in solely within the

47 https://www.get-document-legalised.service.gov.uk/select-service

UK, and also internationally) could protect signatories to deeds from potential fraud. Deeds are what is called a specialty, with their own particular formation requirements as well as an extended (and hence far longer) limitation period for causes of action arising from them under the Limitation Acts.

95. The Group consider that a higher proportion of signatories of deeds (rather than what are called simple contracts) are likely to have advice prior to or upon execution. This is because of the type of transactions that are performed by deed rather than simple contracts. Some consumers may only sign a deed once in their life, if at all. Some may never do so. Equally, many sophisticated businesses may execute deeds as a matter of course. The different stages are broadly as follows.

The advice stage

96. Those setting up deeds for signature on electronic platforms have a range of options open to them when doing so to increase confidence and ease for all parties. The first stage will be the advice process. The giving of advice, consultative interactions, and verbal agreements can be captured by electronic platforms and retained alongside any documents later signed digitally to provide further reassurance to the parties and their representatives that the proper processes have been followed. Retaining documentation surrounding the advice process leading up to signing of the deed itself may help to establish intention and understanding, should this ever be in doubt.

The signing occasion or “ceremony”

97. Electronic signing platforms can document and record exactly what is said and done during the occasion when a deed is executed by the parties, sometimes called the signing ceremony. Using an electronic signing platform can potentially therefore provide greater assurance than mere physical presence to demonstrate and record the processes followed to sign a deed, and the steps taken in advance of doing so. Using technology to record and preserve the evidence surrounding execution of a deed can provide a much more accurate and longer lasting record than the recollection of an individual or witness present at the time it is signed. Recollections, and ex post facto evidential demonstration of what occurred, were the purpose historically of requiring witnesses to such documents; in the event of disputes, the witnesses would give evidence to a court or tribunal about the validity of the signature that they had witnessed. Electronic data can achieve the same purpose far more easily, securely and permanently.

98. Use of an electronic signing platform can also ensure that the same robust process is followed every time a deed is signed. All parties can be directed to follow a required process which can be established to include checks and safeguards, rather than relying on those present for the signing to recall how to proceed and what steps to take next. Individuals may unintentionally omit parts of the process when they are not

prompted as to the correct steps to take whilst in the process of signing a deed. One example of this is Lasting Powers of Attorney or LPAs. These can be created using an online tool[48] but even then the forms must be printed off and signed in a particular order, and then submitted physically for registration to the Office of the Public Guardian. If the signatures have not been completed in a particular order, the form will be refused, returned, and the LPA will not be registered. Members of society wishing to execute a LPA may attempt to do this themselves, and there is no reason that they should not do so, but in circumstances where those needing one may be infirm, the delay if there is a mistake can be considerable and cause significant difficulties.

99. Using an e-signing platform means it should be possible to design the required process and stages to sign a deed so that requisite steps cannot be bypassed. Mistakes or failures in correct sequences can then be identified immediately and therefore can be almost instantly corrected. Pictures or videos can be used to highlight or explain a point of procedure if a party to the document prefers a visual aid instead of a textual explanation. Using an electronic platform, all parties can be required to acknowledge that they have followed the necessary procedures validly to sign and witness a deed, in addition to signing and witnessing the document itself. This can provide clearer evidence of understanding and agreement than solely relying on documentary proof.

100. Signing a deed in this way can reduce the risk of a person being subject to coercion or duress, or at least make it easier to expose duress when it has occurred, as during the process an electronic signing platform can record what the signatory has seen in the deed itself before proceeding to sign the document. Depending upon the sophistication of the platform, the behaviour of the signer can be tracked to show the amount of time taken to review, read and sign each page of a deed. This approach can provide greater assurance as to the specific steps a signatory had taken in signing the document and the time taken to absorb the provisions within, therefore establishing a significant audit trail of the activities undertaken by the parties in the act of signing and witnessing a deed. Steps taken by a witness in adding their signature to the deed may no longer be just implied but can be documented and incorporated into the digital audit trail created surrounding the document. This can be further extended to the review and acknowledgement of each page of a deed.

101. An e-signing platform has (or should have) no inherent bias and can therefore provide additional independence for individuals in the process of signing a deed. Such an individual may feel less pressured when reviewing and acknowledging the terms of a deed in advance of signing where they are not physically supervised by an individual present throughout the execution process. E-signing potentially allows for more time to be used in reviewing the provisions of the deed in advance of signing. The subconscious pressure that might be experienced by, say, a signatory attending

48 https://www.gov.uk/power-of-attorney/make-lasting-power

at an adviser's business premises in order to sign a document could be almost entirely avoided, together with a record being kept electronically of exactly how long that signatory had taken to read the document (or even each page of that document).

102. It is possible to use video or voice recording of the signing process further to confirm the identity of the parties present and their state of mind when signing the deed or acting as a witness to a signature. A photo or video can be taken – and stored electronically - of each signatory, witness, or attendee, to assist with the confirmation of identity of the parties. The IP addresses of devices used to sign the deed can be recorded to observe where parties are located and the type of device used to sign the document can also be recorded and evidenced later if needed. This may have the added advantage of allowing others to confirm that a witness was present in the same location as party to the deed, at the time it was signed and therefore witnessed.[49] Video recording can also be used and retained to record the established processes taken to sign a deed by all parties, so that in the event of a dispute there is evidence to confirm that this was validly done.

103. Overall, it is the view of the Group that the use of technology can allow for better record keeping, and the collection and preservation of evidence of the signing process to a level significantly more cogent than that available using traditional methods for signature. An audit trail will be available for every deed signed using an electronic platform.

Time limits and rejection

104. Use of an e-signature platform to sign a deed means a time limit can be placed on the signing, meaning inaction will lead to a party failing to execute a deed as opposed to being required to take positive action. This in turn limits the coercion or duress placed on the potential parties to a deed and allows rejection by simply failing to sign it in the prescribed time limit. This is not possible with physical execution.

105. Signatories can be given an express power to reject the deed by confirming via the e-signature platform that they do not wish to proceed to sign the document. Some platforms may allow the signatory to assign the signature of the deed to someone else, therefore removing the burden on themselves or permitting them the opportunity to discuss their intentions in relation to the deed with another individual or representative.

[49] This can be a significant element of the audit process, although it is not infallible because IP addresses can be spoofed and because the use of Virtual Private Networks (VPNs) can distort the trail.

Options to amend or comment on deeds

106. This is one area in which the field of electronic signatures falls behind that of traditional execution, whether for deeds or otherwise, although is to some extent dependent upon the nature of the platform. Some more basic platforms simply do not enable a signatory to amend terms. The more sophisticated ones do. Electronic signing platforms *can* allow a party to the deed to review and comment on it first before proceeding to sign the document itself, and for deeds this should be set as an absolute minimum of functionality. Parties can also be given powers to amend and edit the deed, although it is not expected that this power would be exercised in all cases. Where appropriate for such amendments and edits to be made, however, the platform must enable this to be done, and for any proposed amendments to be shared with the counterparties for approval prior to execution. Again, the Group consider that this should be set as an absolute minimum of functionality, at least for significant transactions.

Accessibility

107. Electronic signature platforms are also able to ensure that deeds are accessible and legible when displayed on a range of devices (large or small screens, mobile devices or tablets). This can ensure that the parties to the deed have been able to review the document fully and easily in advance of signing, taking into account their specific requirements or additional needs. Allowing a deed to be displayed differently for individual parties to a document in accordance with their needs means they can each be clear about the content of the document which they are being asked to review, sign and execute.

Access to information

108. Deeds signed via electronic signing platforms allow for security of data to be maintained by permitting access to the platform only to the parties intended to review and sign the deed. The content of the deed can be restricted to the parties to the document and any others authorised to read or review it, with permissions set by the party setting up the deed on the platform for signature. This preserves confidentiality, and is likely to be of an enhanced level compared to a more traditional paper document. It can be agreed in advance between the parties how finalised copies of the deed are to be circulated and stored by the electronic platform. This allows deeds to remain private to the required parties only and prevents the risk of physical paper copies of deeds falling into the wrong hands, being wrongly copied or being lost. As a result, parties are less vulnerable to misuse by others.

Identity in Electronic Execution of Deeds

109. The identity of the parties to a deed is of significant consequence when considering the implications arising from potential fraud. If a process is technically executed but is in fact carried out by an individual assuming the identity of another, the entire process is compromised. This applies as much to electronic documents as to physically executed ones, and can be considered independently of the benefits of a so-called “electronic identity” such as that being currently considered by DSIT.

110. Legally, the transfer of real property can only be achieved by deed. Identity and its verification have become more significant issues since the Covid-19 pandemic restricted physical interactions, and this is particularly true in relation to the sale and purchase of property. The following frameworks are currently being developed in response to the changing landscape.

The UK Digital Identity and Attributes Trust Framework

111. As outlined above, DSIT is currently developing a UK Digital Identity and Attributes Trust Framework. The Framework’s objective is to ensure a standard for identity verification that can be applied across the whole UK economy. Working under this Framework, sectors across the economy are able to develop an appropriate Scheme that will meet their own sector-specific needs if required or if they wish to do so.

112. The home buying and selling sector has worked to develop a digital identity trust scheme (DITS), aligned to the UK Digital Identity and Attributes Trust Framework that is being developed by DSIT. The Scheme will allow the digital identity of a home buyer/seller to be verified *once only* (rather than multiple times as currently) and then be shared by the consumer and used throughout the rest of the sales transaction, based on consent. This will streamline what can, traditionally, be a cumbersome process.

113. The Scheme, by following GPG45 guidelines, is working to align with DSIT policy objectives and certifying identity providers’ (IDSP) adherence to the standard, allows IDSPs to support many methods of identity verification in order to provide certainty for all service providers, whilst ensuring inclusivity for consumers. The Scheme is working to ensure inclusivity, especially for digitally excluded people or those considered to be ‘thin file’, a phrase which is generally used for those who, for example, lack an existing digital footprint or credit file.

114. The Home Buying & Selling Digital Identity Trust Scheme (the Scheme) will allow participants in the Scheme to trust an identity proof provided by third party Identity Providers, who are subject to audited certification and regulation. The Scheme details how an identity can be digitally proven following the Government’s GPG45 standard, whilst meeting money laundering regulation (MLR) customer due diligence requirements.

The Money Laundering Regulations or MLR

115. The 2019 amendment to the Money Laundering Regulations specifically recognises the role of third parties in identity verification ("IDV") and provides guidance on the conditions required to meet the obligations of the Service Provider ("SP"). The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 prescribe the following:

    "(19) For the purposes of this regulation, information may be regarded as obtained from a reliable source which is independent of the person whose identity is being verified where—
    (a) it is obtained by means of an electronic identification process, including by using electronic identification means or by using a trust service (within the meanings of those terms in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23rd July 2014 on electronic identification and trust services for electronic transactions in the internal market (11)); and
    (b) that process is secure from fraud and misuse and capable of providing an appropriate Level of Confidence that the person claiming a particular identity is in fact the person with that identity."

116. The DSIT UK National Digital Identity and Attributes Framework is intended to meet the requirement in (a) above and this Scheme, by being compliant with the DSIT Framework, will meet this requirement. In addition, the Scheme will meet the requirement in (b) above by:
    (1) Specifying the specific GPG 45 level, LOC Medium or Higher, which meets the requirement of (b).
    (2) The Scheme will require an initial Politically Exposed Person (PEP) check and require IDSPs to undertake additional mitigation to ensure the person being checked is either the PEP or a different person (many PEP positives are false positives and require mitigation to prove the case). This ensures that individual risk will be addressed.

Land Registry's Digital Identity Standard

117. In March 2021 HM Land Registry (HMLR) launched its first Digital Identity Standard. This provides a step-by-step list of requirements for conveyancers' use of digital services to verify their client's identity securely online. The new standard is optional. However, it offers a 'Safe Harbour' for those conveyancers who meet the requirements. HMLR would not seek recourse against conveyancers who comply with the standard in the event their client was not who they claimed to be.

118. HMLR has stated that it believes that there is scope for an alternative higher standard of identity check – one that uses biometric and cryptographic technology, is defined, and gives clarity and certainty to the conveyancer that they have discharged their duty on identity verification in connection with land registration applications.

119. The enhanced level of check is defined by reference to a set of requirements, collectively known as the HM Land Registry digital identity standard. The standard is founded on the principles within the Government's Good Practice Guide GPG45. The requirements involve biometric and cryptographic checking of identity and verification that the individual or individuals signing of behalf of corporations are the owner of the property or are authorised on behalf of the owner of the property.

120. The standard, when followed, constitutes what is regarded by HM Land Registry as a discharge of the duty to verify the identity of a party to a registrable transaction.

121. A conveyancer who adopts this approach will have fulfilled their obligation to take reasonable steps in relation to the requirement to verify their client's identity and will reach the "Safe Harbour". This means that if a conveyancer carries out the steps described in the standard, HM Land Registry will not pursue any recourse claim against the conveyancer resulting from the registration of a fraudulent transaction on the grounds that identity checks were inadequate.

122. Schedule 8 to the Land Registration Act 2002 ("the Act") provides for compensation to be paid to a person who can show that they have suffered loss as a result of a mistake in the register on an indemnity basis. This includes where a fraudulent transaction is registered. Under paragraph 10 of Schedule 8 to the Act, HM Land Registry has a statutory right to recover from conveyancers compensation paid by it in certain circumstances. This includes cases where compensation has been paid as a result of fraud.

123. A conveyancer who carries out the requirements to achieve the standard must remain vigilant during the remaining course of the transaction. If, at any time prior to the completion of the transaction, the conveyancer has (1) reasonable doubt about the checks they have conducted, or (2) has reason to believe the characteristics of the transaction itself indicate the parties they represent may not be genuine, then they should make further enquiries and seek further evidence, as appropriate, to ensure those doubts are removed. They must make a record of the results of those further checks and enquiries. Where there is reasonable doubt and it is not positively resolved, the standard will not be achieved.

124. It is acknowledged that it may not always be possible to conduct all the steps set out in the standard in every transaction. Where it is not practicable to carry out these enhanced checks, or resolve any doubts around the checks, the conveyancer will not reach the standard. In these circumstances, the conveyancer may remain at some risk of HM Land Registry seeking recourse if it turns out the transaction was indeed fraudulent, and the conveyancer has been either negligent or fraudulent in relation to the checking of identity.

125. Electronic signing platforms can add to the documented record of a transaction by carrying out automated checks on credit agency databases, electoral rolls and so on.

It is also possible for electronic platforms to validate documents automatically such as passports and driving licences themselves, or to be linked with other systems that will carry out this function.

Recommendations for Reform

126. The Group is aware that some of the aims and outcomes identified here are aspirational. It is also aware that law reform recommendations are largely the province of the Law Commission under statute, and it therefore merely proposes these steps for further consideration by Government.

1. Regulation and certification

127. There is a desire to provide the end-user with as much confidence as possible in e-signing platforms by introducing a set of minimum standards to bolster the integrity of the e-signing experience and process. To move towards achieving this, the group recommends:
(1) exploring an enhanced role that could be fulfilled by the ICO; and
(2) reviewing the National Cyber Security Centre ("NCSC") Technical Assurance Principles initiative.

128. As regards (1), the role of the ICO could be expanded to (a) be more active in this area by publicly supporting guidance being given on best practice – and possibly providing more recognition of eIDAS/eID and related kitemarks; and (b) provide a self-certification service for e-signing platform providers. It might be that Government is not persuaded that such a wider ambit could be "bolted on" to the existing role of the ICO.

129. The Group is entirely neutral about the precise identity of the relevant body, but notes that the AI Standards Hub has recently been set up by the Alan Turing Institute, BSI, NPL and the Government, and might well be an ideal body to take on this function.[50]

130. Self-certification could involve ICO/DSIT or another government body working as a moderator that:
(1) develops a set of signing platform 'basic performance standards';
(2) publishes the standards on a 'dedicated/go-to' webpage that is easily locatable for prospective platform users;
(3) invites signing platforms to confirm whether they meet the standards;
(4) publishes a list of signing platforms that submit self-certifications on a go-to webpage;
(5) confirms listings annually.

131. As regards (2), the NCSC is developing a new approach, called "Principles Based Assurance', to help determine if a piece of technology is suitably secure for its

50 AI Standards Hub - The New Home of the AI Standards Community

intended use. The NCSC draws on its many years of experience in helping industry, and government departments will undoubtedly gain confidence in a variety of technologies and systems to set this new approach, which is centred on a set of principles. The NCSC states that "*Technology assurance helps people decide whether a technology is secure enough for their needs and supports the UK's digital growth ambitions in a safe and secure way*". The Group considers that the work of NCSC can be drawn on in order to form part of the exercise to encourage adoption of e-signature through effective and reassuring communications and frameworks.

132. A next phase proposal is to apply the principles identified by the NCSC's Head of Technical Assurance Group (first link below), by thinking through the structure of: Principle, Description, Threat, Protective Measures, as far as they apply to e-signature. The Technical Assurance principles and an explanation of them is publicly available.[51] The white paper on Principles Based Assurance is here: https://www.ncsc.gov.uk/collection/technology-assurance.

133. As the NCSC itself explains it, "the process of gaining confidence starts with a good set of principles that describe the key security requirements and ends with appropriate evidence they've been met. Ultimately, it's all about the evidence and how much of it you need…and that comes back to the risks and impacts."[52]

134. Confidence in both platforms and performance standards is, in the judgement of the Group, fundamental both to wider adoption and confidence generally in e-signatures and other electronic documentation such as ETDs.

2. Uniformity of approach to e-signing and online identification by way of an international standard or mutual recognition

135. International uniformity of approach may be optimistic and aspirational but if technologies can demonstrate robustly the critical elements of e-signing (namely proof of identity together with demonstration of intention to authenticate), and a set of minimum standards for e-signing platforms is established to facilitate this, then uniformity of approach would potentially become easier to achieve. The work of the EU in relation to eIDAS 2.0 reforms is an example of one group of countries that are seeking to achieve widespread adoption through reform. The degree to which the UK could or should closely follow those developments is a policy decision, but the Group cannot see any disadvantages in doing so.

51 https://www.ncsc.gov.uk/blog-post/principles-and-how-they-can-help-us-with-assurance

52 https://www.ncsc.gov.uk/blog-post/future-of-technology-assurance-in-the-uk

3. Government consideration of wholesale adoption of e-signatures for all purposes, and investigation into modernising any area where wet ink signatures are mandated

136. In the case of some Government issued documents (such as civil status certificates and DBS checks), this could be achieved by the documents themselves having a high-quality electronic signature or a system capable of verifying the documents online using a code or by the use of a QR code or similar.

137. Similar reforms are being considered by the Land Registry to streamline transactions concerning land.

138. It is difficult for the Government to seek to widen adoption of e-reforms such as e-signatures unless official documents dealing with all areas of life can be accomplished by using them. Exceptions are difficult to justify and although piecemeal reform is one option (for example the procedure adopted for formal execution of wills during the Covid-19 pandemic which allowed witnessing to be performed over a video link, a temporary measure which the Interim Report recommended be made permanent) in areas where specific formalities are required, it would be more beneficial if all Government departments adopted an entirely streamlined approach. One of the recommendations in the Interim Report was that the Government adopt e-signatures in all dealings with third parties.

4. The abolition of deeds

139. At common law, a deed was required to be written on paper, parchment or vellum, and then to be sealed (though not necessarily by the person whose deed it was or with that person's seal), and to be delivered as a deed (in order to display an intention to be immediately and unconditionally bound by the deed).

140. The term seal was historically usually applied to the impression left by the stamping of an engraved metal die or 'matrix' which has been pressed into a material such as wax, but it is also used to refer to the matrix itself. Often bearing their owner's portrait or coat of arms they were used to authenticate documents (such as charters, letters, writs) in much the same way as signatures are used today.[53] The National Archives holds a Digital Seals Register of over 2,500 seals from the 12th century onwards.[54]

141. "Sealing" would traditionally have involved the application of a wax disc, later replaced by paper, later replaced by the use of the cipher "LS".[55] Section 73 of the Law of Property Act 1925 added a requirement that the deed of an individual be signed as well as sealed. The Law of Property (Miscellaneous Provisions) Act 1989 removed any requirement as to the substance upon which a deed must be made and

---

53 https://www.nationalarchives.gov.uk/help-with-your-research/research-guides/seals/

54 https://discovery.nationalarchives.gov.uk/details/r/C13431170

55 *Locus sigilli*, literally "place of the seal"

imposed new requirements that a deed must be clear on its face that it is intended to be a deed and must be validly executed. For individuals, valid execution no longer involved the deed being sealed; instead, valid execution of a deed by an individual required the individual to sign the deed in the presence of a witness, who attested the signature.

142. For companies incorporated in England and Wales, valid execution of a deed could be achieved by affixing the company's common seal (with no requirement for signature, unless otherwise required by the Articles) or by the signature of two authorised representatives or of a director whose signature is attested by a witness. However, local authorities are treated differently in law from other corporate bodies such as limited companies. The legislation governing local authorities dates back to the Local Government Act 1972, and (unlike limited companies) it has not been updated to reflect technological change. At present, in line with HM Land Registry's (HMLR) Practice Guide 8, Chapter 7, HMLR will accept execution where a local authority also certifies that it is, under its constitution, able validly to execute a deed other than in accordance with their special arrangements. This requires a certificate to be lodged with the application, signed by an individual conveyancer employed by the relevant authority, which states that the deed has been duly and properly executed in accordance with the council's constitution. A number of authorities are now amending their constitution to authorise alternative methods of execution to allow for electronic signatures and seals.[56]

143. Members of the Group have discussed the need for any requirement for a signature to be witnessed and attested, and whether it serves any useful purpose in the 21st century. Some members have raised a question as to whether it should be abolished. There is a view that the formal execution requirements for deeds adds complexity and cost to their execution but without any, or any sufficient, resulting benefits, particularly with electronic execution of documents now an increasingly (if not dominant) form of execution.

144. The ideal solution would be to abolish any rule of law that requires an act to be done by way of a deed and, at the same time, to consider what, if any, replacement measures are appropriate for those transactions that can at the moment only be done by deed. For example, the ability to make unilaterally a binding act, which currently requires a deed poll, is a valuable feature in English law. If deeds were totally abolished, it would be necessary to consider means of achieving the same legal effect by another means, such as by writing and signature (wet ink or digital)

---

[56] The Law Society guidance document, "Note on the execution of a document using an electronic signature", (initially released in 2016), was updated in October 2022 to reflect changes in practice adopted by HMLR. Sections 8.2 and 8.7 of the guidance outline the constitutional requirements for e-signatures, (though it highlights as referenced above, that the position may be different in relation to corporations not formed under the Companies, i.e. Local Authorities). It is noted that this will depend upon both the wording of the Act of Parliament/Royal Charter creating it and the corporation's own constitutional documents.

with or without specific or general words that make it clear that the signatory intends the document to be binding on the signatory. As far as the protections afforded by the Limitation Acts are concerned, the parties could agree in the contract or agreement that the benefits provided by the Limitation Acts should nonetheless apply.

145. An alternative would be to retain the concept of deeds as a specialty but to abolish all formalities surrounding the execution of deeds with the exception of the requirements that a deed be in writing and signed (in wet ink or digitally) and that it must be clear on its face that it is intended to be a deed. The formalities that should be abolished include the requirement, generally referred to as the Mercury requirement, that a deed exist as a discrete physical entity at the moment of its signing. This term comes from the case of ***R (on the application of Mercury Tax Group and another) v HMRC*** [2008] EWHC 2721 (Mercury). The Law Society has issued a practice note giving guidance on good practice in light of the Mercury case and suggested different options for virtual signings/closings,[57] which was reviewed in May 2020 in the light of the Covid-19 pandemic and the lockdown imposed in March 2020.

146. The Group considers that it would still be useful for consideration to be given to all instances where a deed is currently required, and all parties (including local authorities) in order to determine whether any additional protections were required for particular transactions or particular parties (and, indeed, whether the requirement for writing was necessary), but it may be that this could be carried out as a longer-term exercise. In any event, this is squarely within the province of the Law Commission, and a ministerial reference on the matter has already been made to it.

5. Statutory Declarations

147. Statutory declarations are made under the Statutory Declarations Act 1835 and provide a solemn verification of a fact otherwise than in the context of legal proceedings. They are required to confirm certain facts or circumstances by various statutes or the practice of some Governmental bodies, such as the Land Registry.

148. A statutory declaration must be made in the form required by the Act before someone who is entitled to administer oaths (usually a solicitor or notary), on payment of the prescribed fee. Knowingly and wilfully making a false statutory declaration is a criminal offence under section 5(a) of the Perjury Act 1911, and carries a penalty of up to two years' imprisonment or a fine, or both. It is presumably the threat of this punishment, coupled with the need to execute the declaration before a professional, that is regarded as adding solemnity and seriousness, and thus reliability, to a statutory declaration beyond a mere written statement to the same effect. However, the form of the declaration does not refer to the risk of punishment if the declaration is false, nor is the person before whom the declaration is made obliged to explain this

[57] https://www.lawsociety.org.uk/topics/business-management/execution-of-a-document-using-and-electronic-signature

to the person making the declaration, or to check on the identity of the person making the declaration (although in practice most will do so, certainly in respect of identity).

149. There is no specific requirement in the Act that a statutory declaration be on paper or that the person making the declaration and the person before whom the declaration is made are physically present in the same place at the same time. The Group considers that there is no obvious reason why a statutory declaration could not be made electronically, but it is in practice a cumbersome process and, statutory declarations having customarily been made in person, there may be some doubt about an electronic statutory declaration's validity.

150. This risk has been addressed for certain statutory declarations required for insolvency proceedings. A Temporary Insolvency Practice Direction Supporting the Insolvency Practice Direction ("TIPD")[58] states the following:

"Where Schedule B1 to the [Insolvency] Act [1986] requires a person to provide a statutory declaration, a statutory declaration that is made otherwise than in-person before a person authorised to administer the oath may constitute a formal defect or irregularity".

151. The TIPD notes that it is open to the court to declare that a formal defect or irregularity shall not invalidate the relevant insolvency proceedings, unless the court considers that substantial injustice has been caused by the defect or irregularity. The TIPD goes on to say that a statutory declaration made by video conference, and stating that it was made in that way, should not *of itself* be regarded as causing substantial injustice. The Law Society has also published, with permission from Lexis Nexis, a guide to making and administering statutory declarations by video conference, referring expressly to the TIPD. This recommends video-conferencing and that the statutory declaration be scanned, printed and emailed between the parties.

152. The TIPD takes advantage of a particular provision in the Insolvency Rules to address the consequences of the risk that a statutory declaration may be invalid if it is made other than in person. This solution cannot be used in other instances and is, in any event, unwieldy. In these circumstances, it is appropriate to consider whether the formalities concerning the execution of statutory declarations continue to fulfil any genuine or useful function, in particular the involvement of a person authorised to administer oaths. For example, if the wording required for a statutory declaration referred to the Statutory Declarations Act 1835 and to its being an offence punishable by imprisonment knowingly and wilfully to make a false declaration, would the declaration be any less solemn, serious or reliable than if made before a solicitor? Removing the need for a third party to be involved in a statutory declaration would allow declarations to be made electronically in a straightforward manner and without

58 TEMPORARY INSOLVENCY PRACTICE DIRECTION SUPPORTING THE INSOLVENCY PRACTICE DIRECTION (justice.gov.uk)

risk of invalidity, and would reflect the much reduced role of oaths and their equivalent in society. The very fact that the relevant statute is not far off its 200th birthday suggests to the Group that this is one area that could be considered at the same time, and in the same way, as the preceding comments above concerning deeds.

Further recommendations

153. Consideration be given to the establishment by the Government, or a suitable Department, of a permanent body similar to the Industry Working Group, comprising both legal, industry and academic membership, that is properly funded and which does not consist of voluntary *pro bono* membership. The Group has enjoyed productive and regular meetings, but every single member (other than the permanent secretariat members, for whose assistance the Group are enormously grateful) has other permanent obligations which require most of their time. Meeting more than once a month has proved difficult, and investigation, research, meeting and drafting has had to be fitted around other commitments. The Group has concluded that the multi-disciplinary nature of its membership is hugely valuable, because it has allowed topics to be examined from all different angles. However, this subject and others parallel to it, such as e-commerce generally, as well as the notable aim of having the UK at the forefront of digital developments and e-commerce, are so important for the future of society in the 21st century that a more formalised and focussed approach is, in the collective view of the Group, what is required. This could, as suggested above, be a function transferred to the recently-formed AI Standards Hub.[59]

[59] AI Standards Hub - The New Home of the AI Standards Community

C. Best Practice as explained in the Interim Report

154. The Interim Report set out the Principles of Best Practice for the use of e-signatures, and a Four-Step approach. In accordance with its Terms of Reference, it separately identified specific considerations for vulnerable individuals.

155. For detailed consideration of the reasoning behind those, the full Interim Report should be consulted. However, a summary follows here for convenience and in order that this Final Report can usefully be read as a stand-alone document.

156. It was clear from the Group's work 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.

157. The best practice principles identified by the Group in the Interim Report were intended to enable parties to use electronic signatures in a way which best suits their specific requirements. They are structured 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.

158. Those principles were distilled into five high-level points:
    1. 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.
    2. 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. It is also the view of the Group at the Final Report stage that such minimum functionality for significant transactions should include the

ability for a signatory to propose amendments to the terms of an agreement at the stage of signing, and for any proposed amendments to be shared with the counterparties for approval prior to execution.

3. 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.
4. Where possible, provide multiple options to vulnerable customers or counterparties so that these groups can adopt a method of signing that suits their needs.
5. Intention to authenticate should be easier to demonstrate for those with secure digital identities, but the latter should not be essential.

159. Taking those in a little more detail, sequentially, to assist understanding.

a. Is Electronic Execution Appropriate?

160. 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:

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

161. 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.

Is any party incorporated outside of England and Wales?

162. 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.

163. For example, under local law, a signature may only be recognised in the receiving jurisdiction if it is notarised or apostilled, which may not be possible with an electronic signature.

164. 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.

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

165. 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.

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

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

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?

167. 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. 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.

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

168. 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.

Does the document require signing formalities that cannot be satisfied using an electronic signature?[60]

169. 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.

Does any party have a particular vulnerability?

170. 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 be considered. There is further guidance in Paragraph 124 and following of the Interim Report for the use of electronic signatures where individuals, in particular vulnerable individuals, execute documents electronically.

b. How to choose the best form of electronic signature

171. As already established, the term “electronic signature” covers a broad range of technologies, all intended to link an identifiable person to information held in

[60] The Interim Report contained, at p34, a diagram setting out the various formality requirements for simple contracts and for deeds in England & Wales, in Scotland and in Northern Ireland. That diagram suggested the electronic signatures could not be used in Northern Ireland validly to authenticate deeds. We are very grateful to Tim Dale, a partner at Pinsent Masons, for coming to address the Group on this issue, after the publication of the Interim Report. His view, with which the Group agrees, is that it is better to say that the point is uncertain rather than definitive. His argument is set out in full below, at Appendix 8.

electronic form. The strength of that link varies between different technological solutions.

172. The Interim Report considered, under "Statement of current technological capabilities", 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. 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.

173. 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. These combine to provide a conclusion as to whether any transaction is a significant transaction. The answer to that will depend case to case:

174. **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.

175. **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.

176. Appendices 5 and 6 of the Interim Report provided 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 addressed issues arising from commercial transactions and Appendix 6 was focussed on individuals as parties to a transaction, particularly vulnerable individuals. [These appendices are appended to this Final Report]

177. 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. The Group consider amendment capability to be an essential feature for the e-signing for any significant transaction unless there is good reason to exclude the possibility.

178. 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.

179. 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.

c. Fours steps to follow for electronic execution

180. 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

181. 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.

182. 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.

183. 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?
    xii. 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.
    xiii. 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

184. 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.

185. 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 using the chosen form(s) of electronic signature;
    iv. How the signed documents are to be returned, 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

186. 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 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.

187. 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

188. 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.

d. Identity, Security and Reliability

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

190. 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.

191. 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).

192. 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.

193. 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.

194. These electronic methods have often been retro-fitted from established digital biometric handwriting techniques and their analysis 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.

195. 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.

196. 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.

e. Vulnerable Individuals

197. 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. 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.

198. Anyone who has been asked to sign for a parcel delivery with a bespoke tablet using a stylus will be familiar with what often occurs, a scrawled "signature" (which is technically an e-signature, given the medium) that bears little resemblance to any proper wet-ink signature of their own with which that person is familiar, and may in the experience of the Group often resemble the writing of a small child. Whilst that may be perfectly acceptable for delivery of a book or similar, it is far less satisfactory as one moves up the scale of financial impact.

199. 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.

200. 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; and
    - 'Person specific vulnerability': this derives from a party's personal characteristics, such as a disability or poor mental health.

Market Specific Vulnerability

201. Any individual may become vulnerable because of one or more of the following complex and overlapping factors:
    - **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. There is a wealth of international research on the proportion of adults experiencing a negative life event, and the type of life event. It differs from country to country and over time, but has been estimated in the UK to be approaching three in ten (29%) as at October 2020.
    - **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

202. 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.
    - 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.

203. 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.

f. Best Practice Guidance - Vulnerable Individuals

204. 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 adopt 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 or the Royal National Institute for Blind People to understand the specific needs of signatories with vulnerabilities.
    viii. Consideration should be given to the Web Content Accessibility Guidelines (WCAG 2.1) 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.

g. Other developments since the time of the Interim Report

HM Land Registry

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

206. There is currently a pilot scheme underway at HMLR.[61] The following applies as is stated by HMLR:

"Section 91 of the Land Registration Act 2002 provides for a document in electronic form to be regarded for the purposes of legislation as a deed if certain conditions are met. Not being an actual deed, there is no need for the signatures to be witnessed. One of the conditions for the section applying is that any conditions required by the Land Registration Rules 2003 are met. Some of these conditions are set out in a Notice given by the registrar under rule 54C and one of these is that the document must be signed with qualified electronic signatures. The eIDAS Regulation as amended by the UK eIDAS Regulations defines a qualified electronic signature. Key features are that the signature is:

- uniquely linked to the signatory and capable of identifying them
- linked to the signed data in such a way that any subsequent change in the data is detectable
- supported by a 'qualified certificate' issued by a 'qualified trust service provider'
- created using a qualified signature creation device

The Information Commissioner's Office has produced a Guide to eIDAS that explains the eIDAS Regulation and the UK eIDAS Regulations and their effect, which is found at: https://ico.org.uk/for-organisations/guide-to-eidas/.

"We currently accept electronic dispositions signed with qualified electronic signatures under a pilot scheme involving a small number of conveyancers and a limited number of kinds of registrable disposition: see Rule 54C Notice. We are working on being able to accept these signatures more widely as the next stage of our work on electronic signatures."

61 https://www.gov.uk/government/publications/electronic-signatures-accepted-by-hm-land-registry-pg82/practice-guide-82-electronic-signatures-accepted-by-hm-land-registry#qualified

207. It is to be hoped (and the Group generally expect) that the next stage of work on electronic signatures by HMLR will continue this approach, rather than concluding that e-signatures are to be less widely accepted than before. 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.

208. 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.

209. Prior to the publication of the Interim Report the Group had the benefit of a presentation from the personnel involved at HMLR on this subject, and the draft practice from HMLR will follow upon conclusion of the pilot.

210. The 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 e-Signature. 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.

Notaries and the e-Apostille

211. A notary is a specialist lawyer. In England and Wales notaries are appointed and regulated through the Faculty Office of the Archbishop of Canterbury.[62] Most notaries are also solicitors but they do not have to be, and it is a separate profession. Solicitors are not authorised to carry out “notarial acts” unless they are also notaries. “Notary” or “notary public” is a protected title and only those qualified and registered can call themselves notaries.

212. The principal role of a notary in England and Wales is to “attest the authenticity” of deeds and other legal documents for use abroad. Attesting means much more than simple certification (which would be essentially checking copies against the originals). If the documents in question have been attested by a notary it means that courts and other bodies abroad can accept them without having to make any further checks themselves. Each notary has their own seal which will be attached to the documents.

62 https://www.facultyoffice.org.uk/notaries/customers/what-is-a-notary/

213. Notaries can also prepare powers of attorney, “protest” bills of exchange and offer other legal advice. The profession has for some years been pursuing new technologies as a means of ensuring that they provide a modern service. There is nothing to prevent English Notaries from issuing their certificates in electronic form or from using electronic signatures, as long as those kinds of documents are acceptable in the receiving jurisdiction and all relevant rules and guidance issued to Notaries by their Regulator are followed.

214. The vast majority of documents prepared by Notaries in the UK are for use abroad, mostly in connection with the affairs of UK businesses and private individuals. Many of these documents require some form of “legalisation” before they are dispatched. The most common type is the “Apostille” which is issued by the Foreign, Commonwealth and Development Office (FCDO) and which confirms the status and signature and seal of the Notary and which is accepted by all parties to The Hague Convention 1961.[63] Until recently, the apostille was only available in paper form and was glued onto the back of the Notary’s certificate. Because this Apostille had been available only in paper form, Notaries had been unable to progress their plans to issue their certificates electronically. This development follows the increasingly widespread use of electronic versions of what were traditionally documents printed on paper.

215. On 22 December 2021 the Hague Conference on Private International Law (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. In December 2021, the FCDO also announced its intention to begin a pilot project with a view to implementing the e-APP. The Notaries Society participated in the trial and after publication of the Interim Report in February 2022, in September 2022, the FCDO announced the official launch of the e-APP.

216. In anticipation of this event, the Society worked hard to ensure that once the e-APP became available, the necessary tools were in place to enable its members to issue their documents electronically wherever it was appropriate to do so.

217. The advent of the e-APP provided the initiative to enable the use and circulation of electronic Notarial acts. The Apostille is an important part of confirming the status, signature and seal of public officials and the e-APP meant that this could be done wholly electronically for the first time. It meant that these would be accepted in the relevant overseas jurisdictions that are also signatories to the Convention.

218. The Notaries Society identified a suitable electronic signature platform for processing Notarial documents (including the ability for Notaries, parties and witnesses to sign

[63] Of whom there are over 100

and seal those documents electronically) and to make available to its members the use of the platform at group rates. It also made available alongside and integrated within the platform, a provider to certify the Notary's (and signatories' and witnesses', if necessary) signatures to the level of a Qualified Electronic Signature according to the standards required by EU e-IDAS regulations. This meant that such documents were more likely to be accepted in EU member states.

219. The e-APP and its advantages were also widely publicised. Since its the launch in September 2022 the number of e-apostilles applied for has exceeded initial expectations.

220. Electronic practice is of course still evolving, but this is without doubt a significant change in practice in what is a very ancient profession, and will change forever the way in which Notarial documents are prepared signed, legalised and archived. The Notaries Society also has stated (and the Group agrees) that it also sends a message to the world that the UK is willing and able to adapt to modern technologies and in so doing save time and expense in the preparation and delivery of Notarial acts and instruments. The use of electronic documents is increasing globally, and this development will encourage users to apply these methods as they are undoubtedly more efficient than the traditional ones using paper, post, couriers and physical travel to appointments.

221. The temptation with electronic documents may be to dispense with traditional personal (face to face) meetings and whilst that may be acceptable in the case of people who are already known to the Notary, care will be needed to ensure that all the necessary checks in relation to, for example, identity, capacity, authority, free will and understanding are made in order that the value of electronic acts is no less than it would have been using personal attendance. Identity is of course a crucial ingredient in any consideration of matters such as this within the digital space. Also, when executing Deeds, it does not of course dispense with the need for any witness to be in the personal, physical presence of the signer at the time the electronic signature is applied.

D. The need for rapidity and progress in this field

222. It has already been noted, both in the Interim Report and elsewhere, that the pace of technological change is significant, and indeed is accelerating at an increasing rate. This is driven not only by technical innovations, but also by the way in which modern society is embracing that change. Mobile phones were available for some years before economies of scale made them more affordable, together with a reduction of size that added to convenience. Few people employed in business today in a modern society can be without one. Digital proof of a person's Covid-19 vaccination status, which began to verge on compulsory in some quarters, has only increased wider society's awareness of digital convenience.

223. The observation that the number of transistors in a dense integrated circuit would double about every two years was originally made by Gordon Moore[64] as long ago as 1965, and although it was an observation and projection of a historical trend, it has become known as "Moore's law" and held good until about 2010, after which the pace has slightly slowed.[65] Although historical consideration of what is an empirical relationship linked to a wide number of factors, it is a good example of how what has been called the Fourth Industrial Revolution[66] is changing the world at an increasing pace.

224. More recent observations of this rate of change are well summarised as follows:

> "It is exciting and yet disconcerting to contemplate that there is no finishing line for technology. Our machines and systems are becoming increasingly capable. Aside from the ongoing and radical changes in the underlying and enabling technologies, innumerable new applications emerge on a daily basis. It is bizarre to think that in a few years' time, our online lives will likely be dominated by systems that very few of us have heard of today, or indeed that may not yet have been invented."[67]

225. Both technical innovators and entrepreneurs in the digital economy are pushing ahead with increased use of the digital tools to aid electronic commerce, which include both signatures and other methods of demonstrating assent, as well as

---

64 Now Emeritus Chairman of Intel Corporation

65 This is not to say that technological innovation has slowed: wider technological development has meant that the hardware developments that are the object of Moore's law are no longer required at the same rate.

66 Klaus Schwab, founder of the World Economic Forum

67 Tomorrow's Lawyers (OUP, 3rd ed. 2023) Professor Susskind

trading in digital assets. Proof of identity is a central issue in most of this, as well as flexibility in adapting existing legal concepts to take account of new technological phenomena.

226. So far as identity is concerned, there is, as outlined in the Introduction to this Report, a proposal for advances in this field by Government. New regulation is proposed under the Digital Economy Act 2017 ("DEA") "to strengthen the ability for departments to share necessary information to support identity verification and reuse".[68]

227. In particular, the proposed legislation sets out a new objective under the DEA to enable data sharing by authorities included in Schedule 4 of the Act, and to add four new bodies to the schedule. These are the Cabinet Office, the Department for Transport, the Department for Environment, Food and Rural Affairs and the Disclosure and Barring Service. The proposal would also enable citizens to use several government-held datasets to verify their identity online rather than relying on traditional IDs, to which the government believes many citizens do not currently have access.

228. Digital identity is also a subject being widely progressed by the EU, although given Member States of the EU have existing and compulsory ID card schemes already in place, there are fewer obstacles in terms of adoption there than in the UK, as those countries can simply "bolt on" digital IDs to their existing compulsory schemes.

229. In addition, the Law Commission commenced a consultation in July 2022 on Digital Assets and private property rights,[69] and is in the process of finalising its report to Government on that subject. As it stated in its Consultation Paper, in all of these:

    "Electronic signatures, cryptography, smart contracts, distributed ledgers and associated technology have broadened the ways in which digital assets can be created, accessed, used and transferred. Such technological development is set only to continue." The Final Report is due to be published in 2023.

230. The role that electronic signatures play in signifying assent or approval both in dealing with traditional transactions, as well as dealing in or commerce concerning digital assets, is an obvious one.

231. However, given the non-territorial nature of e-commerce, the digital market is likely to choose territories based upon market perception of the legality and enforcement of transactions, and (the Group assumes) avoiding countries where uncertainty prevails. Rather than have the market decide itself upon the attractiveness of the UK (or otherwise) for such business, timely relevant steps to encourage the complete

---

68 Cabinet Office and Government Digital Service

69 https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/07/Digital-Assets-Consultation-Paper-Law-Commission-1.pdf

facilitation of electronic signatures in all transactions for which they might be desired would send out the right signals to global markets generally. It is also crucial that such steps that are taken are wholly technology-neutral, so as to allow for ongoing technological innovation and development.

E. Certification/Accreditation

232. One subject upon which all members of the Group did not fully agree in all respects was that concerning certification of providers or platforms. It is widely accepted that trust in the platform providers and/or the services provided by the same – whether trust by the public or by commercial entities that wish to use e-signature services – is fundamental to wider adoption and use generally. Few people or companies would willingly use a platform for e-signing if they did not trust what that platform was providing.

233. There are two approaches to such a requirement, which are at opposite ends of the spectrum, and innumerable different points of view in between. One end of the spectrum is the entirely market-forces view, namely that only the best (or the adequate) will survive, and such survival is dependent upon trust from users which should be earned. This viewpoint eschews regulation as being both undesirable but also unworkable in practice, particularly in terms of requirements that are non-technical in nature. Even technical requirements can be viewed as potentially inhibiting of innovation, with the concern that an overly-regulated regime may inhibit international trade and external investment generally. There is the added burden of expense for a system of regulation, as well as the requirement of decision by Government as to which body would oversee this area, and how. This could be described as the “free market” point of view.

234. The other point of view is that some sort of approval or oversight mechanism is required so that some order can be imposed on what is, currently, the technological Wild West. Currently, any entrepreneur can establish a platform offering e-signature services, with no way of a consumer or other user (including business users) being sure of the degree to which security and audit needs are satisfied. Obviously, aiming to use a platform or e-service offered by an existing industry name will minimise or even totally reduce such concerns, but that can simply mean that there are invisible barriers to other, smaller platform providers gaining a foothold in what is likely to become a major market. This could be described as the “pro-regulation” point of view.

235. Within the pro-regulation point of view, or potentially along the spectrum towards that extreme, is the self-certification point of view. This is that there should be a transparent and industry-agreed set of standards or benchmarks against which platform providers could and should self-certify. The majority of the members of the Group favour this approach, although there was a significant minority that did not.

236. The Group does not therefore find itself in a position where it can proffer a unanimous recommendation in this area. Regardless of the views of the majority of the Group, this specific subject would, if it is to be advanced at all, require the setting of specific standards (either technical and/or non-technical) whether pro-regulation or self-certification were to be required or adopted. Such standards would have greater utility and credibility if they were to be established internationally, and in conjunction with those in the industry. Such standards ought also to be established by (or at least in discussion with, or led by) whichever body is to be tasked with their enforcement or audit.

237. However, in order that the Final Report canvass as wide a range of views on this particular issue, it seemed sensible that consideration of different views in this potentially controversial area be cast as widely as possible.

F. Consultation

238. In order to ensure that the content of the Final Report by the Group reflected as wide a view as possible, the decision was taken to put certain questions out for public consultation. The consultation process was administered by the Ministry of Justice and the Secretariat to the IWG. A reasonable number of responses were received, including from major City firms, practitioners and industry specialists, as well as DCMS itself. Adobe Inc. also submitted a response.

239. A summary of the responses to each question is as follows.

The Consultation Questions

240. **Question 1**: eSignature platforms should self-certify against a set of principles formulated, maintained and publicised by an industry or governmental body (such as Information Commissioner's Office, LawTechUK or the National Cyber Security Centre). Do you agree? What (sort of) body is best placed to do this?

241. Many respondents agreed that eSignature platforms should self-certify against a set of principles formulated in order for them to do so. The two main bodies suggested as best placed to do this were either the Information Commissioner's Office (ICO) and the National Cyber Security Centre (NCSC). However, other bodies suggested were also the Information Assurance for Small and Medium Enterprises Consortium (IASME), British Standards Institution (BSI) and even HM Land Registry. In the view of the Group, it is unlikely that the function of HM Land Registry, a non-ministerial department of HM Government,[70] which reports to the Department for Business, Energy and Industrial Strategy ("BEIS")[71] would cover such a remit. The current Government Department with responsibility for digital affairs is DCMS[72] in any event, and the use of e-signatures goes far wider than land transactions, which are effectively a specialist sub-set. The view of DCMS – whose views, as a Government Department, were given significant weight by the Group – was that a body such as the ICO or NCSC could be well placed to do this. It was widely suggested by respondents that the ICO was the appropriate body to uphold a set of principles

---

70 Created in 1862 to register the ownership of land and property in England and Wales

71 BEIS has been split into the Department for Science, Innovation and Technology (DSIT), the Department for Energy Security and Net Zero and the Department for Business and Trade.

72 At the time of consultation, the relevant department was DCMS. Department for Science, Innovation and Technology is now responsible for digital affairs.

under which providers operate, and that the services of, for instance, LawtechUK could and should be used to assist in drafting. Especially given their role in upholding data protection and security, ICO was a particular favourite.

242. However, concerns were raised that regulation may be premature effectively to formulate, maintain and update a meaningful self-certification program, and the Group is aware of the disadvantages of this approach. It was also suggested that an individual regulator for a particular industry may be an option and should be evaluated. If there were to be such a Regulator, this would require legislation and that person, or their office (once created) should undoubtedly be involved in framing and setting the principles.

243. Legal professionals including major City law firms highlighted that the most appropriate principles to use as a benchmark should be the criteria of advanced electronic signature (AES) and qualified electronic signature (QES) which are set out in the UK eIDAS regulation.

244. Some industry respondents recommended that a successful self-certification regime should be the aim, with no appetite for any type of formal regulatory body or authority.

245. For self-certification to be a good process which will obtain public confidence it must be backed up with some type of audit check; respondents were of the view that more was required than merely some evidence of compliance that were self-asserted by the platform. Compliance should require an independent evaluation. This evaluation would help stabilise both the market and the quality of certification, and enable a level playing field between different technology providers.

246. If external audit checks on self-certification are to be adopted, one pitfall which should be avoided in the view of respondents is too many audit/certification bodies or accreditation bodies performing the checks. This usually results in inequality of checking. Most auditors would expect self-certification to be desk-based reviews and checks. Such an approach also reduces the costs but does not impede any follow up checks if necessary.

247. There is however a risk that remote/desk-based self-certification checks can lead to a lack of quality and/or commonality. That can be mitigated through clear baselines and guidance, supplemented with feedback reports, where it would be easy to identify if certain auditing bodies were not applying the same measures. That does, however, create a risk of lack of commonality. Mitigation for that risk is further justification for creating a set of principles and publishing these, and all agreed that published principles assist transparency. Those principles would be the foundation for audit checks and would flow into the feedback reports, with the aim being to provide end to end assurance.

248. However, any such principles would need to be formulated by a group of major stakeholders, and once agreed should be provided to a Government/NCSC type body that would be tasked with ensuring ongoing maintenance of the principles. What must be avoided is the industry moving out of step with principles as technologies evolve. This results in non-common agreement and issues of disparate levels of certification confidence.

249. There is an argument that if such an approach is to be adopted, it be limited to significant or sizeable transactions. This would permit the type of consumer transactions that currently require e-signatures by (say) a supplier to continue outside such a regime.

250. It is also important to be realistic about the role that certification or self-certification could play, and whether it would achieve its aims or simply add a layer of complexity and therefore cost to the process. If it were to be adopted, then to be effective there should be agreement on an objective set of standards, which ought to be internationally recognised, against which the process would be assessed. This could be both in technical and non-technical areas, although the latter would be more difficult.

251. All existing technical standards are defined under the eIDAS Regulation work at either the data level, or at the process level. The EU Trust Mark is aimed at Qualified Trust Service Providers and informs users that the platform with the Trust Mark can be trusted to carry out online transactions in a safe, secure way. EU Regulators have not yet, therefore, chosen to define technical standards. There is some difficulty of doing so in a technology-neutral manner, and it may have been that the EU Regulators concluded that this was difficult or impossible to do.

252. However, mere assertion by a provider that the platform is “safe” has been shown, in other digital fields, not to be reliable. Boeing Commercial Airplanes continued to assert that there were no software issues with its Boeing 737 Max airplane, even after two fatal crashes in which 346 people died.[73] It was not until aviation authorities around the world withdrew the aircraft’s certification that, eventually, Boeing admitted a software problem in its MCAS system. There have been other software scandals in the UK, for example that concerning the Post Office Horizon System[74] where the accounting system for sub-Post Offices was found to be defective.

253. Accordingly, some sort of certification or self-certification against a set of published standards would assist in improving public confidence in e-signatures. It could potentially be limited to e-signatures for significant transactions. Respondents drew

[73] Lion Air Flight 610 on 29 October 2018 and Ethiopian Airlines Flight 302 on 10 March 2019

[74] Currently the subject of a statutory Public Inquiry with Sir Wyn Williams as Chair

attention to programmes in other areas such as in the US and Federal Risk and Authorization Management Program (FedRAMP).

254. In order for the US Federal Government to operate in the cloud with a Cloud Service Provider (CSP), the CSP has to obtain FedRAMP. FedRAMP is a standard that was created by the US Government in order to ensure there is a standard approach to measuring and monitoring security in the Cloud for Federal Agencies. In order to achieve FedRAMP, a CSP has to undergo an audit from a third-party assessment organisation that is approved for the purpose. An organisation can obtain a FedRAMP level of Low, Moderate, and High. The levels each have different amounts of controls for compliance, with High having the most stringent controls. Other similar but non-governmental programmes include Cloud Security Alliance programs such as that of Trusted Cloud Providers and the Star Registry. Compliance with what is called the Cloud Controls Matrix or CCM leads to what is effectively a public statement of approval and compliance. This is, unlike FedRAMP, essentially a voluntary industry process administered by STAR (Security, Trust, Assurance and Risk) and leads to entry upon the Registry. It shares similarity with ISO 27001 in the UK.

255. **Question 2**: Such certification should be based on an evaluation of the way in which the relevant software performs and functions. The underlying code is not a relevant subject for external evaluation. Do you agree?

256. Most respondents agreed that the underlying code of software platforms and functions should not be a relevant subject for external evaluation or regulation. However, there were numerous responses that suggested that the code should still be tested to ensure that it was appropriately secure (these responses from law firms, platform providers and also the Society of Licensed Conveyancers). The Chartered Institute of Legal Executives (CILEX) agreed that security was an important point but felt that appropriate assurances should be given by the provider, rather than the need for regulation or consideration of the underlying code.

257. The Group were also of the view that it would be both impractical, and would also be commercially undesirable, for the code to be submitted for evaluation.

258. There were a small number – three – of dissenting responses. One thought the underlying code should be evaluated, while another considered the question itself to be flawed, suggesting that the underlying code would ordinarily be covered by a non-disclosure agreement. The final dissenting response advocated caution as providers may seek special legal status for their service.

259. DCMS were broadly content that certification and audit controls that evaluated the relevant software and platforms would be an appropriate type of evaluation without the necessity of evaluating the code itself. It was pointed out that underlying code checks could be problematic when included in external evaluation unless protective

measures were put in place due to issues concerning liability, confidentiality, intellectual property rights and so on.

260. Assessing functional ability of software was thought to be appropriate and has the ability to provide many indicators that a properly qualified auditor can use to judge the security and overall risks, without detailed (or any) analysis of the code that underpins that functionality. This could also be assessed by embedding some quantitative and qualitative baselines - similar to the way that penetration testing evaluates systems.

261. **Question 3**: Self-certification should cover both:

    the functionality of the service(s) offered by the platform (in establishing whether those services meet the requirements for an advanced or qualified electronic signature) and the security of the platform.

    Do you agree? Are there other areas against which e-signing platforms could usefully self-certify?

262. Most respondents agreed with the proposed coverage of self-certification, though a number of these felt additional areas should be included such as data protection and retention, accessibility of the service, consumer protection and ease of use.

263. Some law firms that responded, and technology providers too, were content with the proposed areas for self-certification, but also suggested the inclusion of a mechanism to ensure that providers were trustworthy, such as (i) answering basic questions on their history, structure and sustainability, or (ii) providing a detailed report demonstrating how they satisfy the criteria. This overlaps with the areas already considered, such as auditing or checking for compliance with standards. Some professional users suggested that security should not be included in self-certification but assessed against other standards.

264. Other respondents suggested that if there were to be such an approach, the acceptable purposes for electronic signatures be made very clear, including the standards against which self-certification would be measured.

265. The Foundation for Information Policy Research submitted that the decisive factor would be one of user confidence, doubting any benefit from dividing providers between those who complied with the criteria and those who did not.

266. The response from DCMS was one of broad agreement, and it was clear from all responses that the security of any system was essential including at all endpoints. Security is seen as including both physical security (taking account of diverse geo-locations and/or dispersed locations) as well as digital security. The latter includes checking of firewalls, malware protection, checks on data replication and integrity, as well as platform security including data in transit and at rest, access and transfer.

Unalterable capture of signing actions would also seem to be essential, including its proof, as well as other layers of privacy protection for personal information.

267. Other areas suggested were checks on the audit logs and event logs held by any platform. These audit logs are seen as the "gold standard" in terms of what has occurred on any platform for any transaction. These logs can be essential in evidence collection when the authenticity of an e-signature is in dispute. This is essential for attribution.

268. It would make sense to make use of existing eIDAS standards, particularly for PKI-based digital signatures. Issues or pitfalls that ought to be avoided are feature specificity that would either inhibit technical innovation or make the UK less attractive to international users, and blurring the lines between what is the responsibility of a product developer or platform provider, as compared to the platform user. Well-defined "shared responsibility" models were suggested by one industry respondent to avoid potential ambiguity.

269. **Question 4**: Self-certification against these benchmark principles should be a process performed on an annual basis. Do you agree?

270. The majority of respondents, including legal organisations and professionals such as the Law Society, CILEX, Conveyancing Association, the Society of Licensed Conveyancers and major City law firms, all agreed that self-certification against these benchmark principles should be a process performed on an annual basis. The Group's attention was drawn to similar timescales for other comparable schemes. It should be noted that respondents also raised that it should align with any changes to standards and criteria.

271. DCMS were of the view that it should be performed annually, although allowance should be made for checks should there be material changes to regulation, technology, provisions and so on during the year duration in order to retain confidence and ensure changes were adopted promptly by industry.

272. The Group consider that frequency of checks is essentially a subsidiary issue compared to the more central one, which is whether certification (or self-certification) be required.

273. **Question 5:** Self-certification should not be mandatory but should instead be a choice made by platforms on the basis of market considerations. Do you agree?

274. There is no majority consensus on whether self-certification should be mandatory or not.

275. The Law Society agree with the proposal that it should be voluntary, as they believe that enforcement of mandating self-certification would be difficult. They also see self-

certification as potentially redundant if companies are already certified as 'Certification Authorities' and 'Trust Service Providers' under European law.

276. CILEX believe that self-certification should be mandatory to give confidence to consumers and legal professionals that use the service.

277. Both major City law firms and some of the industry respondents are of the firm view that self-certification should not be mandatory, relying upon the market which will self-select providers who give self-certification. Whilst this might be right for sophisticated and business users, it does not necessarily apply to consumers or those with a lower level of existing knowledge.

278. DCMS responded that the preference would be for mandatory self-certification, but this is difficult to incentivise. The suggestion was made that 'strongly-recommended' may be more appropriate in all the circumstances than 'mandatory'. However, many providers are said to be already aware that certification and self-certification are both market differentiators and enablers, and because public trust is such an issue, awareness of this would hopefully lead platforms to wish to self-certify whether mandatory or not.

279. **Question 6**: A failure to adhere to self-certified standards should be addressed through a complaints and investigation procedure, resulting, where appropriate, in enforcement orders, publicity orders and/or fines. Do you agree?

280. The majority of respondents, including legal organisations such as the Law Society and the Chartered Institute of Legal Professionals, agree that there should be a complaints procedure and, if appropriate, enforcement orders, publicity orders, and/or fines, as their view was that these would play an important role in ensuring compliance with the self-certification process.

281. There was strong agreement for this from DCMS, which also observed that suitable sanctions ought to include that self-certificated status could be instantly removed should a complaint be upheld.

282. However, there was a strong countervailing view that this could potentially create a cumbersome level of enforcement bureaucracy that would be costly and of limited utility. Attention was drawn to reputational damage of organisations or providers that incorrectly self-certify against relevant criteria.

Conclusions

283. The results of the consultation did not throw up any surprises but made clear that where there was a divergence of view within the Group, most importantly on the

issue of certification/self-certification and this was reflected in the responses received. That therefore provided confidence to the Group that its members were representative of all the relevant views in the field, and reinforced the value of the diverse membership of the Group, something which is reflected in the final Recommendation at paragraph 294 below.

G. Recommendations

284. The major recommendations in the Interim Report were, repeated here for convenience and updated where relevant:
    a. The group supported 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 DSIT to set up a trust framework as this will facilitate the use of electronic signatures in future. The group also notes that DSIT is moving towards digital identity generally within the UK.
    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 as possible, which the public may have to execute, can be executed electronically. 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. See the Final Recommendations below in this respect in terms of setting a deadline for this.
    f. Standardisation is likely to facilitate the use of electronic signatures. At this Final Report stage, this is bound up with consideration of certification/self-certification, which has been explained in more detail above and which was the subject of public consultation for this Report.
    g. The group recommended that the temporary provision allowing remote witnessing of wills be extended permanently.

285. At this Final Report stage, the Group further recommends the following:

286. **Introduction of a set of minimum standards** to bolster the integrity of, and hence public confidence in, the e-signing experience and process, which can and should be done together with consideration of whether certification/self-certification should be

introduced, but if so, only in respect of significant transactions. That latter term, if it is to be adopted as a threshold, would require consideration.

287. If regulation or certification (other than self-certification) is to be required centrally, consider the appropriate authority, whether ICO, NCSC or alternative. Also, consideration should be given to whether such a way forward should be "bolted-on" to the existing work being done by DSIT in respect of digital identity. Such a body could also provide future guidance on the UK's approach to, and recognition of, eIDAS 2.0 when that is introduced in the EU later in 2023/2024. This concerns digital identity wallets for any EU citizen desiring one, to enable cross-border e-ID.

288. Whichever governmental body is given oversight of this field, consideration by that body to working as a moderator to:
    (1) develop a set of signing platform 'basic performance standards', preferably after both industry and international input;
    (2) publish the standards on a 'dedicated/go-to' webpage that is easily locatable for prospective platform users;
    (3) invite signing platforms to confirm whether they meet the standards;
    (4) publish a list of signing platforms that submit self-certifications on a go-to webpage;
    (5) confirm listing on an annual basis.

289. Confidence in both platforms and performance standards is, in the judgement of the Group, fundamental both to wider adoption and confidence generally in e-signatures and other electronic documentation such as ETDs. Therefore, work towards digital identity by DSIT, and work by HM Land Registry should all align with future steps taken concerning e-signatures.

290. Work towards achieving **uniformity of approach to e-signing and online identification by way of an international standard or mutual recognition**. Although international uniformity of approach may be aspirational, if technologies can demonstrate robustly the critical elements of e-signing (namely proof of identity together with demonstration of intention to authenticate), and a set of minimum standards for e-signing platforms is established to facilitate this, then uniformity of approach would potentially become easier to achieve. The Group cannot see any disadvantages in following developments concerning standards in other developed nations.

291. **Wholesale adoption by Government in the UK of e-signatures for all Government or official purposes**. The Group considers that the aim should be for general acceptance by all Government departments, and a timetable for this where that is necessary, of e-signatures for all purposes. An early date should be publicly stated with the Government's aim of when, in the near future, this will be achieved. This will engender public confidence and also achieve the aim of advertising globally the UK's approach to these technical advancements. It will also show that the UK is

moving at a similar pace to the introduction of eIDAS 2.0 within the EU. Also, some Government issued documents (such as civil status certificates and DBS checks) could be issued with a high-quality electronic signature or a system capable of verifying the documents online using a code or by the use of a QR code or similar.

292. The Law Commission **to consider the reform of the law relating to deeds**, and in particular the formalities surrounding the execution of deeds, including homogenisation of the position of Local Authorities in this respect.

293. **Removal of the requirement for a third party to be involved in making a statutory declaration** and allow declarations to be made wholly electronically in a straightforward manner and without risk of invalidity. This could be considered in conjunction with the preceding recommendation in respect of reform of the law concerning deeds, and again is the province of the Law Commission.

294. Finally, the Group unanimously recommend that consideration be given to the establishment of a permanent body similar to the Industry Working Group, comprising legal, industry and academic membership. This body should be properly funded rather than work on a pro bono basis. The work of the Group, and the results of the consultation, have demonstrated the value of a multi-disciplinary membership, which allows topics to be examined from all different angles. However, this subject and related topics such as e-commerce generally, as well as the notable aim of having the UK at the forefront of digital developments and e-commerce, are so important for the future of society in the 21st century that a more formalised and focussed approach is both encouraged by the Group, and amply justified.

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.

Joan Jolliffe: John Jolliffe is a Senior Strategic Development Manager for Adobe's Document Cloud line of business. In that role 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 verification solutions and trust services 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 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 – *now Department for Science, Innovation and Technology & Department for Business and Trade and Department for Energy Security and Net Zero.*
DCMS	Department for Digital, Culture, Media & Sport – *now Department for Culture, Media & Sport*
DLT	Distributed Ledger Technology
DSIT	Department for Science, Innovation and 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	His 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
Selfie-ID	Requires a user to take and upload a self-image whilst holding a government-issued ID (for remote identity verification)
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.
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

Document Type	Electronic Execution Requirements
	• 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.[75] • 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.
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

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

Document Type	Electronic Execution Requirements
	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. **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

Document Type	Electronic Execution Requirements
	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 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.

Document Type	Electronic Execution Requirements
	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 • 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,[76] 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.

[76] https://sites.google.com/digital.justice.gov.uk/opgmlpa/home

Document Type	Electronic Execution Requirements
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. **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.

Document Type	Electronic Execution Requirements
	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.[77] However, this does not change the conclusion that a digital signature is capable of fulfilling a requirement for a signature in principle".[78]

[77] *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].

[78] 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. However as already noted, any transactions that carry significant financial or personal risk for any of the	• 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, or using “Selfie-ID” methods) 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
	parties may warrant the use of QES ('gold standard' assurance).	• 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. These provide better identity assurance than simple signatures, but less than QES, so may be seen as an upgrade for those not wishing to go to full QES. However as the process friction between AES and QES is constantly reducing, most organisations will likely choose between SES or QES.	• 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) as an additional authentication factor. 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. Alternative technologies to SMS (e.g. authenticator apps, phone audio PINS, reverse phone PINS, email PINS,

Method/type of Electronic Signature	Risk Profile	Best Practice
		etc.) are also being deployed for the same purpose, giving users greater choice of method at the point of authenticating. • 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. • 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.	• 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:

Method/type of Electronic Signature	Risk Profile	Best Practice
	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 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).	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 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.

Method/type of Electronic Signature	Risk Profile	Best Practice
	These are used more widely in Europe and are valid in the UK as described in this report. They may be particularly useful where in-person signing is possible (such as a fixed point of sale or service on permanent devices, or as an app on a portable mobile signing device) and a traditional signing experience is preferable. In addition, individuals that are vulnerable and/or digitally excluded may welcome the chance to use a retail or community facility in order to execute documents electronically, possibly with assistance where requested from trained staff.	• 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. • 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. • As a step-up, automated real-time Identity verification based on biometric handwritten signatures (compared with trusted samples previously deposited) can be utilised for greater assurance at point of use, with additional benefits of fraud reduction and can negate additional authentication steps. • If staff will be used to support customers, it is best practice to provide adequate and appropriate training for not just the signing technology, but more so the use case context and implications of signing (or not).
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.	*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.

Method/type of Electronic Signature	Risk Profile	Best Practice
	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).	• 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 sent to a pre-known device. • 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. • 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

Method/type of Electronic Signature	Risk Profile	Best Practice
		invalid.[79] 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). 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.	• 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 that the signatory is approving the document. This could include: • Use of other identifying approaches, such as 2FA or mTAN SMS codes 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

[79] 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
		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.

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 (if not borne by the requesting party) 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, whether these would be covered or offset, 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. As a generalisation, the broader range of user options covered by the chosen platform, the greater probability of wider use and faster adoption. 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 (per transaction in low volumes) 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 – Electronic Trade Documents Bill

Electronic Trade Documents Bill HL Bill 57 58/3: A BILL TO Make provision about electronic trade documents; and for connected purposes. Be it enacted by the King's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

1 Definition of "paper trade document"

(1) A document is a "paper trade document" for the purposes of this Act if—
- (a) it is in paper form,
- (b) it is a document of a type commonly used in at least one part of the United Kingdom in connection with—
  - (i) trade in or transport of goods, or
  - (ii) financing such trade or transport, and
- (c) possession of the document is required as a matter of law or commercial custom, usage or practice for a person to claim performance of an obligation.

(2) The following are examples of documents that are commonly used as mentioned in subsection (1)(b)—
- (a) a bill of exchange;
- (b) a promissory note;
- (c) a bill of lading;
- (d) a ship's delivery order;
- (e) a warehouse receipt;
- (f) a mate's receipt;
- (g) a marine insurance policy;
- (h) a cargo insurance certificate.

2 Definition of "electronic trade document"

(1) This section applies where information in electronic form is information that, if contained in a document in paper form, would lead to the document being a paper trade document.

(2) The information, together with any other information with which it is logically associated that is also in electronic form, constitutes an "electronic trade document" for the purposes of this Act if a reliable system is used to—
- (a) identify the document so that it can be distinguished from any copies,
- (b) protect the document against unauthorised alteration,
- (c) secure that it is not possible for more than one person to exercise control of the document at any one time,

(d) allow any person who is able to exercise control of the document to demonstrate that the person is able to do so, and
(e) secure that a transfer of the document has effect to deprive any person who was able to exercise control of the document immediately before the transfer of the ability to do so (unless the person is able to exercise control by virtue of being a transferee).

(3) For the purposes of subsection (2)—
(a) a person exercises control of a document when the person uses, transfers or otherwise disposes of the document (whether or not the person has a legal right to do so), and
(b) persons acting jointly are to be treated as one person.

(4) Reading or viewing a document is not, of itself, sufficient to amount to use of the document for the purposes of subsection (3)(a).

(5) When determining whether a system is reliable for the purposes of subsection (1), the matters that may be taken into account include—
(a) any rules of the system that apply to its operation;
(b) any measures taken to secure the integrity of information held on the system;
(c) any measures taken to prevent unauthorised access to and use of the system;
(d) the security of the hardware and software used by the system;
(e) the regularity of and extent of any audit of the system by an independent body;
(f) any assessment of the reliability of the system made by a body with supervisory or regulatory functions;
(g) the provisions of any voluntary scheme or industry standard that apply in relation to the system.

3 Possession, indorsement and effect of electronic trade documents

(1) A person may possess, indorse and part with possession of an electronic trade document.

(2) An electronic trade document has the same effect as an equivalent paper trade document.

(3) Anything done in relation to an electronic trade document has the same effect (if any) in relation to the document as it would have in relation to an equivalent paper trade document.

(4) An electronic trade document is to be treated as corporeal moveable property for the purposes of any Act of the Scottish Parliament relating to the creation of a security in the form of a pledge over moveable property.

4 Change of form

(1) A paper trade document may be converted into an electronic trade document, and an electronic trade document may be converted into a paper trade document, if (and only if)—
(a) a statement that the document has been converted is included in the document in its new form, and
(b) any contractual or other requirements relating to the conversion of the document are complied with.

(2) Where a document is converted in accordance with subsection (1)—
(a) the document in its old form ceases to have effect, and
(b) all rights and liabilities relating to the document continue to have effect in relation to the document in its new form.

5 Exceptions

(1) If an intention that section 3 should not apply in relation to an electronic trade document appears in, or can reasonably be inferred from, the document or terms that have effect in relation to the document—
(a) that section does not apply in relation to the document, and
(b) section 4 also does not apply in relation to it.

(2) Sections 1 to 4 do not apply in relation to—
(a) an uncertificated unit of a security that is transferable by means of a relevant system in accordance with the Uncertificated Securities Regulations 2001 (S.I. 2001/3755), or
(b) a document or instrument of a type specified in regulations made by the Secretary of State.

(3) The Secretary of State may by regulations amend this section so as to amend or remove the exception conferred by subsection (2)(a).

(4) The Secretary of State must consult the Scottish Ministers before making regulations under subsection (2)(b) that contain provision that is to have effect in relation to Scotland.

(5) Regulations under this section—
(a) are to be made by statutory instrument;
(b) may include incidental, consequential, transitional or saving provision.

(6) A statutory instrument containing regulations under this section may not be made unless a draft of the instrument has been laid before and approved by a resolution of each House of Parliament.

6 Consequential provision

(1) In section 89B(2) of the Bills of Exchange Act 1882 (instruments to which section 89A applies), at the end insert “or to anything that is an electronic trade document for the purposes of the Electronic Trade Documents Act 2022 (see section 2 of that Act).”

(2) In section 1 of the Carriage of Goods by Sea Act 1992 (shipping documents etc), omit subsections (5) and (6). 5 10 15 20 25 30 35 40 4 Electronic Trade Documents Bill [HL]

7 Extent, commencement and short title

(1) This Act extends to England and Wales, Scotland and Northern Ireland, except that section 3(4) extends only to Scotland.

(2) This Act comes into force at the end of the period of two months beginning with the day on which it is passed.

(3) Sections 3 and 4 do not apply in relation to a paper trade document or an electronic trade document issued before the day on which this Act comes into force.

(4) This Act may be cited as the Electronic Trade Documents Act 2022.

Appendix 8 – The validity of electronic signatures on deeds in Northern Ireland

The issue

Goddard's case in 1584 said that a deed needed to be written on paper or parchment and needed to be sealed and delivered. The Law of Property (Miscellaneous Provisions) Act 1989 abolished the rule about being written on paper or parchment. However, that Act applied to England and Wales only, and it does not appear that there has been any legislation expressly disapplying it in Northern Ireland ("NI"). Nor has there been any substantive judicial treatment of Goddard's case in NI – so it may be that it is still good law. Whether it is, or not, is outside the scope of this Report. The Act is *necessary* in England and Wales because the rule applied there under the doctrine of stare decisis. That alone may be in itself persuasive that the rule stands in NI.

There are two possible approaches to this issue:

- a practical argument
- a technical argument to show that the rule requiring a deed to be written on paper or parchment has been impliedly disapplied in Northern Ireland for companies signing documents

Practical argument

If a new case came up and was specifically on medium (rather than delivery), a court could find that *Goddard's case* is not a binding precedent because the comments on the medium of a deed were *obiter*. The court in *Goddard's case* was deciding a point on delivery. The standard of reporting in 1584 is not high so we do not know to what extent the court considered the medium necessary for a deed, but fundamentally the court was not being asked to decide that point.

Technical argument

This focuses on Companies Act companies – the Companies Act applies in Northern Ireland.

- A document is validly executed by a company **as a deed** … for the purposes of the law of Northern Ireland if … it is duly executed by the company and is delivered as a deed (s46)
- A document is validly executed by a company if it is signed on behalf of the company by two authorised signatories or one + witness (s44)
- A "document" need not necessarily be hard copy (s1168)
- A "signature" includes making a mark (s46 Interpretation Act (Northern Ireland) 1954)
- In any legal proceedings an electronic signature … shall be admissible in evidence in relation to any question as to the authenticity of the communication or as to the integrity of the communication or data (s7(1) Electronic Communications Act 2000)

- An electronic signature is so much of anything in electronic form as … purports to be used by the individual creating it to sign (s7(2))
- An electronic document shall be admissible in evidence in relation to any question as to the authenticity of an electronic transaction (s7C)

Taking these together, two Directors can sign (make a mark) on a document (which may be electronic) on behalf of a company and create a deed. The Electronic Communications Act recognises the admissibility of electronic documents and electronic signatures.

References

Cabinet Office, *Consultation on draft legislation to support identity verification*, January 2023.

Department for Digital, Culture, Media and Sport, *UK digital identity and attributes trust framework beta version (0.3),* updated January 2023.

Department for Transport, 'Driving Licences', 13 January 2023 < Driving licences - GOV.UK Ethnicity facts and figures (ethnicity-facts-figures.service.gov.uk)>

Department for Digital, Culture, Media and Sport, 'Digital Sector worth more than £400 million a day to UK economy', February 2020. < Digital sector worth more than £400 million a day to UK economy - GOV.UK (www.gov.uk)>

Electronic Trade Documents Bill < Electronic Trade Documents Bill [HL] - Parliamentary Bills - UK Parliament>

European Parliamentary Research Service, *Revision of the eIDAS Regulation: Findings on its implementation and application*, March 2022.

The Faculty Office, 'Notaries: A Trusted Profession' < What is a Notary? – The Faculty Office>

Information Commissioner's Office, *Guide to eIDAS* < Guide to eIDAS | ICO>

International Trade Administration, *Singapore – Country Commercial Guide* < Singapore - Trade Agreements>

Kung, Ong Ye, Minister for Health, *Ministerial Statement*, 6 July 2021 < Ministerial Statement by Minister for Health Ong Ye Kung for Parliament Sitting (mti.gov.sg)>

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

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

The Law Society Company Law Committee & The City of London Law Society, *Note on the execution of a document using an electronic signature*, October 2022, < CLLS-and-Law-Society-E-signatures-paper-October-2022.pdf (citysolicitors.org.uk)>

The Law Society, 'Execution of a document using an electronic signature', May 2020

Law Commission of England and Wales, “Digital Assets: Which Law, Which Court?” < Digital assets: which law, which court? - Law Commission>

National Cyber Security Centre, ‘Principles and how they can help us with assurance’, September 2021 < Principles and how they can help us with assurance - NCSC.GOV.UK>

National Cyber Security Centre, ‘The future of technology assurance in the UK’, September 2021 < The future of Technology Assurance in the UK - NCSC.GOV.UK>

Oliphant, R, ‘Latest trends in the UK e-signing market’ (January 2023), THINK Digital Partners < Latest trends in the UK e-signing market | THINK Digital Partners : THINK Digital Partners>

Office for National Statistics, ‘Internet sales as a percentage of total retail sales’ (20 January 2023) < Internet sales as a percentage of total retail sales (ratio) (%) - Office for National Statistics (ons.gov.uk)>

Professor Susskind, *Tomorrow’s Lawyers*, Oxford University Press, 3rd ed. 2023.

United Nations, *UNCITRAL Model Law on Electronic Signatures (2001)*