ARTICLE:

Electronic Execution of Documents Interim Report: a critical analysis

By Mark King[1]

An Interim Report has been produced by a government-selected 'industry working group' on electronic signatures for execution of documents.[2] It aims (at ii):

> '(a) to analyse the current situation in England and Wales,
>
> (b) to set out simple best practice guidance which can followed immediately, using existing technology, and
>
> (c) to make recommendations for future analysis and reform.'

It notes (at iv):

> 'Under the eIDAS Regulations, the law currently provides for three levels of electronic signature.[3] The group's view is that these levels of signature provide a useful framework. They are:
>
> a. Simple or Standard.
>
> b. Advanced Electronic Signature (AES); and
>
> c. Qualified Electronic Signature (QES).
>
> The details are explained in the Report and the [very] limited uptake of AES and QES in this jurisdiction is also addressed. The Report sets out how the formality requirements for some common documents can be fulfilled using these techniques, addressing a few uncertainties and misconceptions which arise. The Report then briefly summarises the existing technology that is available and explains how it can be used.
>
> The Report's objective in this section is to de-mystify electronic signatures and demonstrate how they can be incorporated into transactions of all kinds, including those involving vulnerable individuals.'

[1] The author thanks Nicholas Bohm (a retired solicitor, and member of the Advisory Panel to the Law Commission for its report on 'Electronic Execution of Documents' for the comments that are wholly legal in nature), and Thomas Smedinghoff (a US lawyer involved in drafting the domestic U.S e-commerce and e-signature laws, as well as the international initiatives mentioned).

[2] *Electronic Execution of Documents Interim Report*, Ministry of Justice Industry Working Group (1 February 2022), https://www.gov.uk/government/publications/industry-working-group-on-esignatures-interim-report.

[3] This focus on levels is misleading. Electronic signatures come in different forms, as outlined in chapter 7 of Stephen Mason and Daniel Seng, editors, *Electronic Evidence and Electronic Signatures* (5th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2021), open source at https://humanities-digital-library.org/index.php/hdl/catalog/book/electronic-evidence-and-electronic-signatures.

The international aspects of the remit are noted as not fully included in the Interim Report, but it also does not include consideration of the practicalities of legal process and the effect of the model envisaged on those whose identity has been adopted by another when faced with the asserted reversal of the burden of proof, or at least with obstacles to obtaining evidence.

The general sense is that there is a structure associated with a particular technology that provides the solution, namely 'Qualified electronic certificates supporting signatures and seals' and (along with the Land Registry) the authors appear to be working hard to get this security technology to fit in with legal reality. This review questions some details about the confusingly named 'qualified' signatures but recommends for future consideration other aspects that have not been addressed and yet may prevent progress.

Observations on the scope

The group was not tasked to look at the use of electronic signatures in general. For example, digital watermarking is a technique/technology that is relevant for signing artwork for claiming copyright; this would appear to comply with the definition of e-signature, but cannot even be 'Advanced', let alone 'Qualified', since, by design, watermarking is intended to work after changes to the data, which Advanced electronic signatures do not. This aspect might not be within the scope of the execution of documents but is a legal matter that should not be overlooked when ensuring courts or tribunals are sufficiently knowledgeable about this topic when it comes to handling electronic or digital evidence.

The focus is very much on the process of signing and the use of technology, yet the real use of signatures is not just a matter for the signer but also for relying parties; these parties are not necessarily known at the time, and the implications for the practicality in courts or tribunals, forensic evidence, and prosecution have been side lined. The unprecedented miscarriages of justice in the Post Office Horizon criminal cases resulted largely from the improper reversal of burden of proof.[4] This illustrates the importance of the failure to consider the implications for those who have been impersonated.

International issues

On the international aspect, the Interim Report does mention a central issue of consideration – that the US does not have an equivalent to the QES. The Report omits to mention that the US has a vibrant online economy, no shortage of lawyers, and has actively considered, piloted, and in some states tried out the idea at State level[5] before

[4] For a summary and links to further sources of information, see 'The Post Office Horizon scandal: a brief chronology', 18 *Digital Evidence and Electronic Signature Law Review* (2021) Document Supplement 1 – 9, https://journals.sas.ac.uk/deeslr/article/view/5390 .

[5] 'shall presume' in the Utah Digital Signature Act, Utah Code §§ 46-3-101, which was repealed by the Repeal of Utah Digital Signature Act S.B. 20. The governor signed the Act on 10 March 2006 ('World electronic signature legislation', 15 *Digital Evidence and Electronic Signature Law Review* (2018) 146 – 163); http://www.columbia.edu/~mr2651/ecommerce3/1st/Statutes/UtahDigitalSignatureAct.pdf. Similar approaches were tried in Washington, Kansas, and Minnesota and all have been replaced by the Uniform Electronic Transactions Act (UETA).

determining that it was not appropriate.[6] Given the broad similarity of the legal systems and the common lack of a population register or register of legal entities, there should at least be reference as to why the 'presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked'[7] with qualified e-Seals (which may well work well in Estonia) is thought to be good for England and Wales.

It would have been useful to have mentioned the European Commission's review of its Regulation and their analysis of why eIDAS has fallen far short of the intent in relation to identification: 'The EU Regulation falls short of addressing these new market demands, mostly due to ... the limited possibilities and the complexity for online private providers to connect to the system, ... and its lack of flexibility to support a variety of use cases.'[8] Other international issues arise, such as the standard approach by some regions of the world to include getting a receipt as an inherent part of the signing (and delivery) process.[9] These will presumably be covered in the final Report.

There is good news in that the Foreign, Commonwealth and Development Office is moving ahead with at least a pilot e-Apostille. Since New Zealand was the fourth country to offer these in 2012,[10] and some in Brazil felt it was late to initiate the e-Apostille in 2016,[11] this is a well-established path. No comment is made as to why the self-proclaimed leaders are so far behind the pack.[12]

Another challenge will be that international organizations are so frustrated by Whitehall's repeated calls for advice that is then ignored that active engagement beyond polite words may be difficult; UNCITRAL[13] would be more impressed if the delegation included a lawyer. The choice of 'Digital' being put into in the Department of Culture Media and Sport (DCMS) may be no more than an historical accident as the minister who took it with him from the Cabinet Office could not keep it when moving on to health. Justice ministries find the Ministry of Justice not engaged, and those in the business, industry and commercial sectors complain that the Department for Business, Energy & Industrial Strategy did not carry on with the work by the Department of Trade and Industry (replaced by

[6] Federal: Electronic Signatures in Global and National Commerce Act (E-SIGN), 15 U.S.C. §§ 7001-7003 (note the discussion in footnote 191 in 'World electronic signature legislation').

[7] Article 35(2) eIDAS.

[8] Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity {SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0281&from=EN .

[9] For example, see Stephen Mason, 'The practical issues in using electronic signatures in different jurisdictions', *Computer and Telecommunications Law Review*, 2021, Volume 27, Issue 6, 165 – 179; Stephen Mason, 'International Initiatives and Electronic Signatures', *Computer and Telecommunications Law Review*, 2021, Volume 27, Issue 2, 37 – 48.

[10] https://www.beehive.govt.nz/release/online-authentication-service.

[11] https://www.hcch.net/en/news-archive/details/?varevent=514.

[12] See also the National Notary Association of the United States of America: *Model Notary Act* (1 January 2010) https://www.nationalnotary.org/file%20library/nna/reference-library/2010_model_notary_act.pdf; *Model Electronic Notarization Act* (January 2017) https://www.nationalnotary.org/file%20library/nna/reference-library/model-enotarization-act.pdf.

[13] https://uncitral.un.org/en/working_groups/4/electronic_commerce.

Department for Innovation, Universities and Skills and then by the Department for Business, Enterprise and Regulatory Reform). The Home Office stance on biometrics must be in the queue to be struck down again by the courts,[14] and their position on mandating employment checks for UK and Irish citizens using (yet-to-be) approved commercial providers of government data whilst providing identity checking for resident continental European Union citizens is bizarre, but this a domestic issue. Yet the description, at paragraph 87, of the user experience suggests John McEnroe's 40-year-old outburst: you can't be serious …

eIDAS background

The terminology used in the Report naturally follows the eIDAS Regulation[15] dating from when the UK was a member of the EU, so some history is necessary to understand the nuances and reasons for its non-standard vocabulary. Electronic signatures have been used since the invention of the telegraph in the 1800s, with the General Post Office also providing identifiers for the sender and recipient of a telex. The idea of '*digital* signature' was published by Diffie and Hellman in the 1970s,[16] although the available technology to handle the public and private keys restricted use, and the public key needed to be associated with some identifier of an entity. This was done with a certificate, or rather a chain of certificates from a 'root' or 'anchor'. The public key infrastructure (PKI) was developed and has had large-scale adoption for a variety of security functions such as access control in passports, mobile telephones, and internet protocols. The digital signature supported by a certificate chain differs significantly from the features of manuscript signatures, which are used in different contexts for some or all the following: identification, intention to be bound, completeness, correctness, and awareness. For example, a gatekeeper at a factory gate signing for a delivery of three parcels is indicating completeness and correctness of the delivery note but is not entering into a contract.

As well as involving complex technology to generate, store and use the private keys, certificates have an expiry date which manuscript signatures do not, and there are entities along the chain that introduce additional potential points of failure but must be relied upon, and paid for by somebody. These entities might revoke or suspend a certificate, which makes good sense for physical access control but is not helpful for later use in evidence. An additional divergence from reality has been caused by the spill-over from security systems in having more than one 'level of assurance' which commentators from the Talmud onwards have noted is not appropriate for signature when used

[14] See, by way of example: *R (on the application of SGW) v Secretary of State for the Home Department (Biometrics, family reunion policy)* [2022] UKUT 15 (IAC); regarding Automated Facial Recognition technology, see *Bridges, R (On Application of) v The Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin), both available at https://www.bailii.org/.

[15] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L257, 28.8.2014, pp. 73–114.

[16] Whitfield Diffie and Martin Hellman proposed the concept in 1976: https://ee.stanford.edu/~hellman/publications/24.pdf.

for identification.[17] From the Commission of the European Communities' DGXIIF 1992 Workshop report[18] onwards, there has been a desire to use the power of public key cryptography to provide *electronic* signatures with adequate security. The OECD working party on security and privacy[19] and UNCITRAL model laws[20] from the late 90s also include this technology. The Commission developed a Directive (e-Signature Directive), but on the grounds of being technology neutral, it used its own words to describe the public key infrastructure (PKI).[21] An important part for some non-common-law counties was the permissive aspect (where explicit provision in law is required to permit certain acts, unlike in England and Wales where the public sector 'In general, may do anything that legislation does not prohibit or limit'[22]), so this was not relevant to England and Wales, where there is not only no generic prohibition but also no appropriate authority to give or take away permission. (It is surprising to see echoes of this 'permit' approach in paragraph 16 of the Report regarding electronic signatures, contracts and invoicing especially because electronic signatures are valid between jurisdictions anyway – since international telex became available in the 19th century – and have been used widely.)

The e-Signature Directive was not consistently interpreted when it came to 'remote signature', which still has no widely agreed definition. For some it is when, by way of example, the bank holds your private key and uses it when you ask for a signature to be applied. There was no agreement as to whether this was 'under the user's control'; this was addressed by the later Regulation and is again under review. Others use the term 'remote' to mean not physically present, so there is no one to detain or arrest when fraudulent activity is suspected. The 'qualified e-signature' is often and equally confusingly named 'secure' or 'enhanced', and in some jurisdictions,[23] it meant the use of approved PKI without explicitly saying so.

---

[17] https://chyp.com/2014/09/22/what-does-the-talmud-tell-us-about-applepay/.

[18] Electronic signature – The Key to Mobility (December 1992). No longer available online.

[19] 'Inventory of approaches to authentication and certification in a global networked society', OECD (DSTI/ICCP.REG(99)13/FINAL, 4 October 1999), https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg%2899%2913/FINAL&doclanguage=en 1999.

[20] The Model Law on Electronic Commerce was adopted by the Commission on 12 June 1996, following its 605th meeting, which in turn was adopted by the General Assembly in Resolution 51/162 at its *85th plenary meeting on 16 December 1996,* and includes an additional article 5 *bis* as adopted by the Commission at its 31st meeting in June 1998. The Commission at its 727th meeting on 5 July 2001 adopted the Model Law on Electronic Signatures. See also the 2005 United Nations Convention on the Use of Electronic Communications in International Contracts, New York (2005), adopted on 23 November 2005, entered into force on 1 March 2013.

[21] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.01.2000, p.12.

[22] *Managing Public Money*, HM Treasury (May 2021), page 8, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/994901/MPM_Spring_21_without_annexes_180621.pdf .

[23] By way of example, see the Secure Electronic Signature Regulations (SOR/2005-30) issued under the Canada Evidence Act (R.S.C., 1985, c. C-5), https://laws-lois.justice.gc.ca/eng/regulations/SOR-2005-30/index.html; Howard R Fohr, 'Legal update, Canada: PIPEDA's Secure Electronic Signature Regulations have been published', 2 *Digital Evidence and Electronic Signature Law Review* (2005) 71 – 72.

There was no 'market' for the 'qualified' signature in the UK, except for an occasional application where they were mandated, for instance in the European banking infrastructure. The Commission review of the e-Signature Directive noted just one UK user in 10 years,[24] compared with tens of millions in other countries, typically because they were included with mandatory identity cards in other jurisdictions. (The problem of 'the excluded' then merely becomes one of what to do about illegal residents, but no industry group can solve inconsistent policies and approaches across government departments.)

The eIDAS Regulation was in two parts, with different legal bases: one part referred to cross-border recognition by public bodies, the other part to five specific 'trust services' (signature, seals, timestamping, recorded delivery, and website authentication).

The former was removed in the UK on leaving the European Union by Statutory Instrument[25] by the wording 'Omit Chapter II', but the vocabulary of mutual recognition seems to have survived in the Report. Although 'mutual recognition' was used as the title for a section of the eIDAS Regulation, the text was entirely about one country 'notifying' and all others having to accept their certificates, regardless of whether they also had a notified system. The cross-EU internal border aspect overcame the objection from system security risk managers being forced to accept certificates by placing the liability on the issuing country, and yet taking on the unspecified liability (for the public sector) for free.

Despite the desire to be technologically neutral, the latter part of eIDAS talks of five very specific services, but there is no explanation as to why, for example, time gets special treatment but not location (which appears in the foundational UNCITRAL 1996 model law[26]), nor special provision for *website* authentication rather than more general application programming interfaces (APIs). In fact, some of their 'services' would more plausibly be component parts of something like a document management system, and it would be unusual to treat them (and pay for them) in isolation.

It should be noted that qualified electronic certificates are required to be identified as such, which would presumably mean re-issuing, or phasing in replacements, for all subscribers of any existing provider. For instance, Annex I of Requirements for Qualified Certificates for Electronic Signatures[27] provides that: 'Qualified certificates for electronic signatures shall contain: (a) an indication, at least in a form suitable for automated processing, that the

[24] Commission Staff Working Paper Impact Assessment Accompanying the proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, /* SWD/2012/0135 final - COD 2012/0146 */, page 70, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2012:0135:FIN:EN:PDF .

[25] The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019, https://www.legislation.gov.uk/uksi/2019/89/made.

[26] https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf.

[27] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L257, 28.8.2014, pp. 73–114, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910#d1e2373-73-1.

certificate has been issued as a qualified certificate for electronic signature.' It is common to find misleading advertising in this field, and some laws provide that an electronic signature can only be valid by using a particular technology. The Report omits to mention options other than eIDAS.

Non-repudiation

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

The first point to make is that the use of the term 'non-repudiation' is not relevant regarding legal form. It is possible that paragraph 79 is asserting not that the law (eIDAS) provides for an irrebuttable (or any) presumption (which it does not) about signatures,[28] but that the level of security and proof defined in eIDAS are such that anything that complies with them (namely a QES) *de facto* has the engineering property of non-repudiation. This understanding may be wrong: it may instead be asserting that eIDAS *requires* the achievement of engineering non-repudiation by laying down conditions which cannot otherwise be satisfied.

Taking 79 and its footnote together (the latter with its reference to 'the technological analogy to reversing the burden of legal proof'), this appears to be a claim that a QES achieves what is best called 'engineering non-repudiation'[29] — that they claim that nobody other than the true intended signatory can in fact make a QES in the signatory's name.

Either way, it seems to be asserting something both novel and contentious, either practically or legally, without apparently seeing any need to justify it.

Legal status of QES

Paragraph 24 describes the QES as having a special legal status of being equivalent to a handwritten signature (when that is very much not a special legal status, at any rate in English law) and claims that it reverses the burden of proof[30] (without explaining what it means by that or citing any kind of authority). This theme is repeated at paragraph 31:

[28] Article 35(2) provides 'A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.' The presumption here refers to the integrity of the data and of correctness of the origin of that data – this is an important issue that requires further discussion, but is not the topic of this article. It does not refer to a presumption about signing, but about the correctness of the data in the certificate in this context.

[29] Non-repudiation is discussed in detail (both in the technical and legal senses) in *Electronic Evidence and Electronic Signatures*, 7.286 – 7.297.

[30] At common law the general rule that the claimant must prove his case, if challenged by the defendant, includes the rule that where the claimant relies on the defendant's signature to a document, it is for the claimant to show that the defendant (or someone acting on his authority) signed it. When the common law was consolidated in its application to bills of exchange, section 24 of the Bills of Exchange Act 1882 set out the effect of this rule with great clarity: a forged or unauthorised signature 'is wholly inoperative.' For other documents the common law remains unchanged. See also Chapter 7 of *Electronic Evidence and Electronic Signatures*.

> '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.'

and 49:

> 'QES provide legal certainty under eIDAS because they are given legal equivalence to handwritten signatures, in terms of the presumption of legitimacy.'

These passages seem to suggest that the authors think that manuscript signatures benefit from a presumption of authenticity or legitimacy, which does not accord with English law.

Use of electronic signatures with public sector bodies when not a matter of contract

There are two separate parts to what the Office of the Public Guardian (OPG) does for powers of attorney, as there are for grants of probate by the Probate Registry: input – that is, getting the information and checking it, and output – that is, issuing an official document or grant. There would be enormous benefits for executors and administrators to have these resulting official documents in a *digital* form (e.g., pdf, QR code), not to be confused with online (i.e., connected to a network), and this could be done (with a *digital* signature on a pdf) without the panoply of services by publishing the few relevant public keys in, for instance, the Gazette (formerly the London Gazette), newspapers, and perhaps Hansard. (They would also be available online, but the printed record ensures that relying parties can check that what they are using has not been tampered with.) Recommending (on page 6 of the Report) the government to be early adopters rings rather hollow when the early adopters were operational last century.[31] There could be wider questions about the impossibility of demanding an original of an electronic document or anachronistic use of crown copyright that need to be addressed, but these may not come under the report's restricted focus on execution.

The more difficult problem for the inputs to the OPG and others of working in an open system without any canonical registers for the population is a separate issue.

HM Land Registry are clearly working very hard to provide not just a digital but an online service, having acknowledged extra liability in Parliament,[32] and having earlier had difficulties with gov.uk Verify,[33] but there is a sense that they are changing the problem to fit the desired solution. They are doing this by playing down the value of a witness and restricting the application to its use by conveyancers acting for the parties. In doing this they are

[31] Robert Lemos, 'Clinton, Ahern digitally sign e-commerce agreement', *Zdnet*, September 4, 1998, https://www.zdnet.com/article/clinton-ahern-digitally-sign-e-commerce-agreement/.

[32] Written statement to Parliament: Departmental contingent liability notification: HM Land Registry digital mortgage service, The Rt Hon Greg Clark MP, 18 January 2018, https://www.gov.uk/government/speeches/departmental-contingent-liability-notification-hm-land-registry-digital-mortgage-service.

[33] Law Commission, Making a Will, Consultation Paper 231 (2017), 'Verify does not currently ensure that the person entering the information is in fact the person he or she is purporting to be; rather it focuses on verifying that the person exists' (paragraph 6.67, page 119), https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2017/07/Making-a-will-consultation.pdf.

reducing it to a problem that has been solved, but also taking it outside the scope of eIDAS because it explicitly excludes closed systems[34] (e.g., Visa and Mastercard) based on contract. It is very brave to take such a hard case first, especially when there is such high liability, yet this is for something which most people would not be involved with more than once in a decade.

At paragraph 172 the Report correctly lists the many functions a witness to a signature neither performs nor could reasonably be expected to perform (although omitting the primary function a witness can perform if required, of testifying whether a given person is or is not the one whom the witness saw sign). This list of the functions a witness does not perform, however, provides no support for the contention, if the Report is trying to make it, that a QES performs all or any of them.

e-Seals

The complication of e-Seals rather than e-signatures for organisations is mentioned, but there is no reference to section 44 of the Companies Act 2006 which post-dates the e-signature legislation but makes no provision for electronic sealing. If the Japanese were to use the EU approach, personal seals would be replaced by e-signatures, so it may be that there are examples here where something previously signed by an entity would be using an e-Seal. This is a distinction without a difference for the technology involved, but not for those issuing certificates to support e-signatures or e-Seals, which have different legal effects under eIDAS (unless the different wording gives the same result). There will also be an issue for international interoperability for those who have taken the simpler approach by adopting the UNCITRAL model law where the distinction was not made. A human remains responsible, even if only as an agent: that is, only humans can sign a document (whether on paper or electronically), yet only organisations can have e-Seals under the provisions of eIDAS.

Is 'best' relevant?

There is an extensive summary of the risks and 'best practice', although 'good practice' is a less problematic term suggesting long-term relevance for not just extreme cases.

User choice

It is often unclear who the 'user' is,[35] indeed reference to larger users suggests it is the recipient not the signer. A 'signing platform' is to be selected, which presupposes the need for one, or perhaps a choice of them, but whose choice would it be? The values (and 'risk appetites') may be very different for the two parties. If a market is envisaged, it would be helpful to distinguish the dynamics of business-to-business contracts, consumer contracts, and interactions with government covered by statute but not a matter of contract.

[34] Article 2(2) eIDAS.

[35] Often 'signer' (apparently assumed not to be an imposter) but for example, see paragraph 35 'potential user must navigate complex legislation'; paragraph 109 'a ... user choice …. and larger users should establish policies'.

The concept of levels is useful in security and extends to many standards where essentially arbitrary choices are made for compatibility (e.g., 3A and 13A fuses), but the relevance to signature is not explained. In English law either something has been validly signed or it has not.

Sundry detail

(1) Paragraph 58 offers: 'A plethora of technologies exist, and it is important for users to differentiate between different signature types, and to have the ability to prove the authenticity of, and connections between the signature, document and signature enablement providers.'

Observations:

'it is important for users' – there is no indication as to what this means

'differentiate between different signature types' – there is no indication as to why this is relevant as it should be obvious in most contexts

'and to have the ability to prove' – there is no indication to suggest for whom this applies, or when

Generally, it is far from obvious why the Report says it provides 'ability to prove the authenticity of, and connections between the signature, document and signature enablement providers [a previously unknown role]'.

(2) Paragraph 59 reads: 'Each technique carries a different profile of legal admissibility and evidential weight. For relying organisations (who intend to use eSignatures with customers) to assess suitability to meet a use case requirement, business processes may be analysed for match and categorised according to key requirements such as:

• legal signature level, which defines the legal validity of the eSignatures,'

Observations:

'Each technique' – do the authors mean technique or technology?

'profile of legal admissibility' – what does this mean (in England & Wales)?

'For relying organisations (who intend to use eSignatures with customers)' – this appears not to include the signers – is this correct?

'defines the legal validity of the eSignatures' – it does not appear to be clear where the legal validity will occur.

On page 77, the Report states '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'. This ignores the point that eIDAS defines three 'levels' of assurance for *authentication* which, at length, it specifies as *high*, meaning high, *substantial* meaning substantial, and *low* meaning low, which is hardly enlightening. Whilst how these are to be achieved is elaborated in implementing legislation, what they are good for is not (and would not expect to be). eIDAS also implicitly sets an upper bound of its 'high' as going beyond that would be a barrier to trade within the common market. Many countries appear to

consider that 'high' is needed for something, and if everyone has it, then 'high' must be available for all, and on equal terms, and why have anything else?[36] It is possible that the authors of the Report equate these three assurance levels with the three types of signature. If this is the case, this should be explicit, otherwise we have 9 cases to consider. (HMLR wants QES but has been using Verify which was only offered at 'Substantial'; all QES are necessarily AES.) eIDAS differs from earlier UK attempts to establish levels based on a simplistic distinction between criminal and civil procedures, such as those in the Good Practice Guide 'Requirements for Secure Delivery of Online Public Services' (GPG 43),[37] although the web site warns that 'Some parts of this guidance are now out of date. The Government Digital Service and the National Cyber Security Centre are currently reviewing this guidance and it will be updated soon.' (15 December 2012).

(3) Paragraph 178 reads: 'only those *elements of identity* [sic] that a user chooses to share with any entity and for specified purposes, will be shared at any one time, thereby maintaining user control'

Observation:

This is an important topic for privacy, pitting individual rights against teamwork, couples, families, or just tour guides, and is under review as part of what should be in the revised eIDAS Regulation, but the direct relevance to executing documents is not obvious.

(4) The phrase 'real estate' is used six times in the Report. 'Real property' is a concept known to English law, but leaseholds are personalty. No doubt the report intends leaseholds as well as freeholds to be covered. Perhaps the Report might more usefully just refer to 'land'.

(5) Paragraph 55 considers the position where there is no legal requirement for a contract to be in writing. The parties may nevertheless contract in writing '(for certainty and evidential reasons)' – which is really just one reason – and 'so that there is then no question as to the legal validity of the contract form.' The question that arises is what question do they think there could be if there is no legal requirement for a contract in writing?

(6) Paragraph 109(e) reads 'Intention to authenticate should be easier to demonstrate for those with secure digital identities, but the latter should not be essential.' Presumably 'identities' here means 'credentials'; but even so this seems a very confused proposition.

(7) The table on page 64 remarks that wills are a type of deed. No authority for this remarkable conflation is offered.

(8) A person is required to use whatever technology an organization imposes on them. The status of those who include the word 'duress' when they sign, or instead of a signature, is unclear.

[36] For the European Commission Trusted List Browser, see https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home .

[37] CESG National Technical Authority for Information Assurance and the Cabinet Office (December 2012 Issue No 1.1), p 34, https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-online-public-services.

(9) Digital Identity (mentioned 15 times) is a Protean concept. The Open Identity Exchange (OIX),[38] for example, presents it (at least for people) as a personal wallet, with a smart digital identity incorporating a 'rules engine'. If the term is used it should be defined. (Note that the vocabulary used by OIX and the Department for Digital, Culture, Media & Sport framework is not consistent.)

Accreditation/Kitemarking

Since the ability to issue 'qualified' certificates is gained by approved/accredited providers, the group is presumably divided about the kitemarking,[39] which would not be the case if it were an obviously good idea to impose a kitemarking marking scheme (beyond making available a clear indicator as to which jurisdiction the transaction was envisaged to be using), with no mention of who will bear the costs. If it is merely branding for some new and previously unnecessary extra step, then treat it as such. Those proposing mandatory use of a specific marking need to provide a cost/benefit analysis for anything that is imposed. Vague notions of 'encouraging trust' should not be invoked to 'sell' the idea of trustmarks; indeed, levels of fraud suggest there is already too much trust in technology, and it would be better to avoid risking theological discussions on the nature of trust.[40]

Composition of the committee

The members of the group producing the Report are a multi-disciplinary mix of business, legal and technical experts. They appear to be heavy on providers of technology and services, with no counterbalance from consumers, victims, prosecutors, fraud investigators, academics, or even public sector service providers. The unfunded status inevitably favours those who stand to make money from developments such as providing new services. If the motivation is about making savings, then there is no business monopoly on the need to do this, and the public sector should also be involved. The project would benefit from some antagonists, or at least doubters, to be involved with the Report, not to mention the authors of the freely available standard legal text on the topic.[41] (Free advice, as given for the privacy principles, is easier to ignore than commissioned work.)

Recommendations

The following recommendations are suggested as a way of improving the quality of the Report for the final version:

(1) The scope should be widened to consider not just the act of signing but also the practical implications for the subsequent uses of the signatures in legal processes.

[38] https://openidentityexchange.org .

[39] Paragraph 184.

[40] Nicholas Bohm and Stephen Mason, 'Identity and its verification', *Computer Law & Security Review*, Volume 26, Number 1, January 2010, 43 – 51; Stephen Mason and Timothy S. Reiniger, '"Trust" Between Machines? Establishing Identity Between Humans and Software Code, or whether You Know it is a Dog, and if so, which Dog?', *Computer and Telecommunications Law Review*, 2015, Volume 21, Issue 5, 135 – 148.

[41] Stephen Mason and Daniel Seng, editors, *Electronic Evidence and Electronic Signatures* (5th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2021).

(2) The reasons for the US rejecting the proposed approach for the 'high' end should be explored, with explanations as to what is different in England & Wales that would make it acceptable.

(3) The envisaged business model should be clearly enunciated, showing who will pay, roughly how much they will pay, for what, and confirming that any choice in the 'market' is made by the payer.

(4) The implications for all parties of the novel features of using previously unknown 'services' should be addressed, including the merger, suspension or termination of service provision and of each certificate having an end date/time.[42]

(5) If there are to be quantified 'levels' of assurance the implications for relying parties must be explained.

(6) The aspirations should just be for 'good practice', not 'best practice'.

(7) The international section should pick up on differences with (at least) Scotland and indicate how and when they might be resolved.

(8) Membership of the group should be widened and centrally funded.

Mark is a retired civil servant. He was the UK technical expert for the working group on the e-Signature Directive, ISO/IEC security standards and the OECD principles. He was the first chair of the NATO PKI working group and led liaison with the US DoD Enterprise Security Management initiative

mhaeaking@freeuk.com

[42] For instance, consideration should be given to the implications of the DigiNotar case when certificates were issued to imposters, for which see *Electronic Evidence and Electronic Signatures*, 7.254, and the UK example dated 15 March 2011, where a Registration Authority partner (Certstar) of the Comodo Certificate Authority suffered an internal security breach where an attacker used the RA's account with Comodo to cause 9 fraudulent certificates to be issued for www.google.com, mail.google.com, addons.mozilla.org, login.live.com, login.yahoo.com, and login.skype.com https://blog.mozilla.org/security/2011/03/25/comodo-certificate-issue-follow-up/.