October 1st, 2020

To whom it may concern

In the matter of the eIDAS Open Public Consultation
https://ec.europa.eu/eusurvey/runner/EUDigitalIdentity2020?surveylanguage=EN
Kantara formed a special sub - group of its open international community Identity Assurance Work Group (IAWG) to review the document.

As a result of the work of this sub-group Kantara is pleased to offer the following responses to the eIDAS Open Public Consultation.

Kantara notes that the recent State of the Union speech indicates another intent to seek extension of competence on identity to EU-level. No details are known as to the likelihood of this coming to pass, so these comments are restricted to the *status quo*.

The following comments cover a review of eIDAS (including implementing Acts) from a range of different aspects and is offered in response to the consultation.

Yours sincerely

Ruth Puente
Director

……

Comment: 1. General. Terminology.

The terms 'identification' and 'authentication' are defined in the consultation with a different meaning from that given in Article 3 in eIDAS, let alone elsewhere, making it difficult to formulate a response. Kantara believes that there are different scenarios that can be found under the topic of identity, including:
A. Hello, I'm new here….
B. I'm already known to you but now want to transact electronically.
C. It's me online again.
D. I assert that I'm in some specific category.

The requirements for these differ, and many systems will cover more than one. Kantara believes that the first two appear to be covered by 'electronic identification' in the content of the Regulation, and some identifiers are recognised as national competence and so excluded. Kantara further believes that the third is covered by 'authentication'.in Kantara's opinion the last scenario is not in scope. However, this interpretation does not align with the headings, e.g. Chapter II's is entitled ELECTRONIC IDENTIFICATION but ends up just covering use for authentication (Article 6: the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication …), and suggests that requirements have been merged. This conflation may also have raised both expectation and concerns.

Recital 12 encourages secure electronic identification and authentication, but features pertinent to privacy protection for authentication (in scenario C) have rendered the minimum data set defined in the Implementing Acts insufficient for identification for enrollment (in A or B).

Article 3 (5) 'authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed. This omits scenario B when it would seem to be wanted.

Article 7(d) requires that the notifying Member State ensures that the person identification data uniquely representing the person, but then Implementing Act 1501 (Article 11 Person identification data) gives:
1. A minimum set of person identification data uniquely representing a natural or a legal person shall meet the requirements set out in the Annex when used in a cross-border context.
The Annex gives: (d) a *unique* identifier constructed *by the sending Member State* in accordance with the technical specifications *for the purposes of cross-border identification* and which is *as persistent as possible* in time.

Authentication (scenario C) does not require and should not demand uniqueness, and a choice of method and identifiers can be useful, but identification (when it is needed) does.

Proposed Change: Align the terminology with an international group such as UNCITRAL Working Group IV Electronic Commerce, Provisions on the Use and Cross-border Recognition of Identity Management and Trust Services.

Comment: 2. Changed environment.
The Regulation was justified using an impact assessment. In Kantara's opinion it would seem entirely reasonable for an objective measurement comparing outcomes with the predicted benefits to be produced and published to assist the review. Anecdotal evidence suggests that adoption has been primarily only where mandated, suggesting that issues about trust raised in Recital 1 have still not been solved in the upgrade from the earlier Directive, and the market has adopted techniques such as zero-knowledge which do not fit into the old structure.

In Kantara's opinion the peer review appears to be very onerous, and some reports suggest considerable disagreement, which may not be surprising given the adoption of an implementing act against a (non-blocking) majority under time pressure. Note also Implementing Act 1502 recital 12: The Committee referred to in Article 48 of Regulation (EU) No 910/2014 has not delivered an opinion within the time limit laid down by its chair… This indicates that there was more work to be done than administrative detail, and the issues raised then need to be reconsidered. The proportion of genuine passports falsely obtained in some countries is estimated to be between 2 and 5%, suggesting that acceptance offers up significant opportunities for fraud, not just a real market in fake ID. The supposed 'market' appears to have diverged from what must have been imagined.

Proposed Change: Issue and make reference to a formal review of the original business case, including the costs.

Comment: 3. Levels
The question of levels should be reviewed. Kantara believes that if three levels for authentication are found to be needed, the need for anything other than HIGH for identification is not explained. The same signature is used in the physical world for all transactions and advice stretching back to the Talmud envisages something either it is or is not a signature.

Proposed Change: The choice of levels should make reference to how it has addressed the issues identified by STORK.

Comment: 4. Brexit Implications
The acceptance of the UK's notification of a system where each person could have 7 or more concurrent identifiers, chosen by independent private sector providers, hashed by the state to offer cross-border authentication is a good example of where a system that is sufficient for scenario C fails to provide for scenario A. Despite ten years of incantations that it is intended for private sector relying parties, suitable commercial models are still only under discussion. It might be thought that Brexit would remove this complication, but it suggests that there will be now be a need for far more cross border interactions with foreign public sector bodies than there was before.

The UK statutory instrument SI2019 No. 89 simply disconnects the eID (7. Omit Chapter II.). This emphasises that by being silent on external connection, it offers a barrier to those outside the EEA wishing to invest, buy, or visit. The UK SI does retain Chapter III on trust services, *mutatis mutandis*.

Proposed Change: Brexit implications should be included in the revised business case.

Comment: 5. Private sector.
The envisaged role of the private sector as providers varies by nation and is of narrow interest, but the need for identification by all organisations (worldwide) as relying parties to cope with GDPR subject access requests. GDPR also calls for attribute checking such as age verification. Indeed much of the private sector's need for identification results from legal obligations, and it makes sense for those imposing the obligations to ensure that the infrastructure is there to support compliance.

Areas such as payments systems were explicitly excluded from the eID scope (although qualified certificates are highly relevant for the second Payment Services Directive (PDS2) infrastructure), which is unfortunate, because interaction with the public sector does require payments, identification is vital for anti-money-laundering (AML) and sanctions enforcement, but mostly because payments are something done almost every day by almost everybody and are inherent in any genuine 'market'. On the other hand, there is, by definition money in payments, and clearly defined liabilities, whereas many public services have no direct financial value.

Proposed Change: A recital to cover PSD2 implications is needed, and should encourage the public sector to engage with the *payments* industry in a coordinated fashion, which could be mentioned in a recital, and to remove the expectation of simply growing whatever is mandated in eIDAS to cover private sector use.

Comment: 6. Market
An unexplained feature of the imagined market is who makes choices; in any normal market, and to obtain market dynamics, the payer chooses. If the relying party needs SUBSTANTIAL, and is paying, but the customer only has HIGH, would the IDP accept a lower charge? Such blockers to adoption fall outside the currently defined scope, and are not necessarily best tackled though legislation.

Proposed Change: Include reference in a recital to where such obstacles to adoption have been or will be resolved.

Comment: 7. Inconsistent provision for private sector relying parties
Recital 17 notes that the authentication possibility provided by any Member State should be available to private sector relying parties established outside of the territory of that Member State under the same conditions as applied to private sector relying parties established within that Member State. Including EEA, this still means 30 or so sets of conditions with a wide range of charging policies and different rates. Again, it's identification that the states offer; authentication (scenario C) is increasingly something that innovative commercial solutions can be used; why would they do it the hard way with identification when that's typically not needed?
States should provide identification on the conditions to all relying parties worldwide to support Subject Access Requests required by the General Data Protection Regulation (GDPR). The costs of satisfying subject access request cannot be recovered (except for US organisations under Privacy Shield, which is still available from the US end, and in countries such as New Zealand with adequacy decisions).

Proposed Change: Either the national supporting infrastructure from eIDAS should be free or GDPR should be changed back to allowing reasonable actual costs. The latter would be preferable to shield all organisations, including charities, from responding to unlimited non-genuine Subject Access Requests SARs.

Comment: 8. **Upper limit on assurance and implications for due diligence**

The constraints on interoperability have an implication for national usage: an upper bound of EU-HIGH (otherwise it would block cross-border use). This needs to be aligned with requirements under legislation for AML. Liability is considered in detail in eIDAS, but it sets an upper bound on assurance requirements without mentioning the implications for Due diligence in other legislation, e.g. where 'all reasonable steps' are demanded for demonstration of compliance.

Proposed Change: Make it explicit that Due diligence requirements cannot exceed HIGH.

Comment: 9.
The approach taken in International Aspects (Article 14) could lead to sudden collapse of confidence and legal certainty, as experienced in 'Safe Harbor' and 'Privacy Shield'. EU signatures would be valid in the US, UK, China, and many other countries (but not all) simply because there is nothing to say they would not be. As with passports, recognising another country's signatures is a unilateral choice, so for those EU member states where permission is needed, a mechanism such as a commission determination should be available without the need for an agreement.

Proposed Change: Include the additional option of Commission Determination.

Comment: 10.
Recital 16 calls out ISO/IEC 29115:2012 Entity Authentication Assurance, which should be taken into utmost account in establishing minimum technical requirements. But Implementing Act 1502 (Annex) notes: "However, the content of Regulation (EU) No 910/2014 differs from that international standard, in particular in relation to identity proofing and verification requirements, as well as to the way in which the differences between Member State identity arrangements and the existing tools in the EU for the same purpose are taken into account." This mismatch is in danger of erecting a barrier to trade with the rest of the world.

Proposed Change: Member states via standards bodies and the commission through liaison should seek convergence of ISO29115 with whatever is the reality in Europe.
(Note: At its 30th meeting of ISO/IEC JTC 1/SC 27/WG 5 (virtual), September 12th - 16th, 2020 Working Group 5 (digital identity and privacy technologies) cancelled the project to revise 29115 at WD4, replacing it with a Preliminary Work Item 'Examination of scope and structure of ISO/IEC 29115:2013 Entity Authentication Assurance Framework for possible revision').

Comment: 11. Explicit connections with wider international initiatives.
There is also related work in UNCITRAL (mentioned above) on private sector uses, and by the World Bank, which has noted that the need for a joined-up approach the public and private arena.
https://uncitral.un.org/en/working_groups/4/electronic_commerce

Proposed Change: These initiatives should be acknowledged in a recital.

Comment: 12. Scope: users.
The Estonian e-Residency card is instructive: in order to support private industry to go fully digital, provision was made for non-resident non-citizens to be shareholders or directors of Estonian companies. The extra step of notification of this laudable initiative to support inward investment results in liability for transactions for non-resident non-citizens' interaction with public sector entities in other nations – a step too far. On the other hand, the UK's system - providing in practice for a subset of residents with fixed abode but in theory for anyone needing to deal with certain government services - is entirely unrelated to any citizenship. This raises an issue that cross-border is not defined in Article 3, and although it has a clear meaning for the movement of goods and persons, does it apply, for example, to a Frenchman dealing with French Authorities when in Germany, using an Estonian e-Residency ID?

Proposed Change: Either a definition is needed (with consequential corrections) or the scope of mandated cross-border acceptance of notified systems should be restricted to support for citizens of the notifying state (and possibly for those given asylum).

Comment: 13 Multiple Sources of ID
Multiple sources of ID, (unlike dual citizenship in the physical world) highlights the need for a repair service, as outlined in the 2008 Crosby Report. When the identity provider is hidden from the relying party, those whose identities have been usurped have no idea where to start, and the relying parties cannot help them.

Proposed Change: a workable system for repair must be included in requirements and elaborated in the implementing acts.

Comment: 14. Scope: market.
Recital 2 limits the scope to "electronic transactions in the internal market"

Proposed Change: this should be expanded to include whatever is offered in Article 14.

Comment: 15. Article 2 Scope 1.
This Regulation applies to electronic identification schemes that have been notified by a Member State, and to trust service providers that are established in the Union.

Proposed Change: A Recital should note that the providers of notified schemes do not have to be established in the Union.

Comment: 16. Mutual
The term 'mutual' in the heading of Article 6 (and in many recitals) is very misleading and gives the impression of reciprocity, which may be the desired aim, but the obligation in Article 6 to accept what is notified is entirely one-way.

Proposed Change: Re-title Article 6 to cross-border identification (if the content is changed, or authentication if left as is).

Comment: 17. Seals
Seals and signatures were separated by the Regulation, but then the subtle distinction relating to reversal of burden of proof is undermined by Recital 58: "When a transaction requires a qualified electronic seal from a legal person, a qualified electronic signature from the authorised representative of the legal person should be equally acceptable." Recital 59 does not provide an explanation.

Proposed Change: The need for the distinction should either be explained or, if others cannot justify it, be removed.

Comment: 18. Ambiguous requirement
There is an ambiguity (not just in the English version) in
Article 6 Mutual recognition 1. When an electronic identification using an electronic identification means and authentication is *required* under national law or by administrative practice to access a service provided by a public sector body online in one Member State….
Does this refer to required when wanting the online version of a service, or if the service is only available online? Recital 12 suggests it should be the former, but failure to deliver has been excused by pleading the latter.

Proposed Change: Reword to 'an online service provided by or on behalf of'

Comment: 19. Suspension
Recital 53 notes that "The suspension of qualified certificates is an established operational practice of trust service providers in a number of Member States…"

Suspension can be used as an access control security mechanism in real-time systems, but is incomprehensible when it comes to electronic signatures. If, unknown to me, my certificate has been suspended, is the signature somehow not valid? If knowingly used when suspended is reliance when unsuspended valid? Whilst common law countries struggle with 'legal certainty', suspension does not assist with it. If suspension is still used it must be made clear to the other nations what all the different scenarios that they may have to deal with are.

Proposed Change: Define a limited scope of usage for suspension, or remove it entirely if no longer used.

Comment: 20. Consent
As GDPR RECITAL 43 notes, consent is rarely the legal basis for public sector data processing, but consent is mentioned in eIDAS Article 24(2)(f)(i).

Proposed Change: Provide for a consistent way to record awareness or consent, e.g. by using ISO/IEC 29184:2020 Online privacy notices and consent, which includes a sample of Kantara's consent receipt in its annex.
https://www.iso.org/standard/70331.html and https://kantarainitiative.org/download/7902/

Comment: 21. Advice and confirmation of location
Assured Location is a service of increasing interest for public transport and pay-by-use insurance, as well as being used e.g. for tailoring services, checking eligibility, or checking and recording applicable jurisdiction, but also for speed limit enforcement and alibi evidence.

Proposed Change: Location should be considered for inclusion as a trust service.

……

References

State of the Union addresses:
https://ec.europa.eu/info/strategy/strategic-planning/state-union-addresses/state-union-2020_en

STORK Secure idenTity acrOss boRders linKed
https://ec.europa.eu/digital-single-market/en/content/stork-take-your-e-identity-you-everywhere-eu