The UK digital identity and attributes trust framework

Expert Panel – Age Restrictions

Response to DCMS Consultation Draft

We are grateful to DCMS for seeking the views of stakeholders on the 'apha' version of the UK Digital Identity and Attributes Trust Framework.

This response is prepared by a sub-group of the Expert Panel – Age Restrictions. A description of the Panel and its role is provided below. For ease of reference, a table of contents is produced for this document, related to the questionnaire sections for the DCMS online response form. In addition this response, we have completed the online questionnaire and many of the members of the Panel will have submitted comments directly on behalf of their own organisations.

The Sub Panel consisted of Iain Corby (AVPA), Katherine Waters (on behalf of PASS), Julie Dawson (Yoti), Dr Rachel O'Connell (Trust Elevate), Murray Perkins (1Account).

Table of Contents

Information about the Expert Panel – Age Restrictions

The Office for Product Safety and Standards (OPSS) is part of the Department for Business, Energy and Industrial Strategy (BEIS). The role of OPSS is to make regulation work, so that it protects people and enables businesses to understand their obligations. It has responsibility for trading standards policy locally and nationally, local better regulation, primary authority, business guidance and the UK's Quality Infrastructure (UKAS, BSI, etc).

As a part of its role, OPSS facilitates a series of Expert Panels. These are independently chaired, but subject focussed and include subjects like food standards, product safety, etc. One of those panels is related to Age Restrictions. OPSS leads on enforcement policy for age restrictions and the Expert Panel supports OPSS and other government departments to implement age restriction laws, policy and guidance that will work well in practice to protect children and young people.

There is information about the work of the **Expert Panel – Age Restrictions** on Knowledge Hub.

The **Panel is not a campaigning voice**. It is a matter for Ministers and Parliament to determine what products, content and services should be age restricted and at what age. However, the Panel does have a role in helping government departments to implement age restriction policies in a way that works well. We take a practical and detailed approach. So, for instance, our response to this consultation exercise may, in places, venture into some very specific but, we hope, helpful detail.

Our aim is to draw on the collective expertise of around 50 participants in the Panel. These participants include local and national regulators, retail trade associations, the primary authority network, age verification providers, lawyers and those that work in this regulatory field. Our Panel includes senior staff from major retailers as well.

This response has been prepared by a sub-group of the Panel.

General Questions about the Trust Framework

Do you agree with our trust framework approach for digital identity?

Yes

Do you agree with our open policy making approach of releasing an alpha document?

Yes

Inclusion

To what extent do you agree that the requirement to submit an annual exclusion report will help to hold companies accountable to be more inclusive?

The requirement for inclusivity is currently only applicable to identity services providers but should be applied equally to attribute services providers. You would not want groups of the population to be unable or less able to prove their age online, for example.

There will be a strong market demand for solutions which are inclusive, so whether government needs to impose a reporting requirement pre-emptively, without any current evidence of exclusion being an issue, is questionable. It may be less burdensome to research inclusivity at a Scheme level, where participants could collaborate to share the cost of the research, or trade bodies could commission this work – this would also give a picture of exclusion across the full range of providers covered by a scheme, as it may be that collectively a much more inclusive solution is on offer.

There is also a practical challenge – is it actually possible to create a fully inclusive solution? Different providers will base their solutions on different methods and sources, and those sources may themselves be limited for other reasons beyond the control of the providers. The providers can extend the range of sources but this has a cost, and could be a barrier to entry to the market if the only providers accepted are those who can afford a wide enough range of methods to be sufficiently inclusive.

To what extent do you agree that companies will be happy to produce an exclusion report?

The current draft states:

“You must write the report based on evidence, for example findings from user research or data and analytics for your product or service. You do not need to collect any additional personal information from your users.”

It may well be necessary to collect additional personal information from users to provide such a report. For example, if you want to assess whether your age assurance solution is equally accessible to all ethnicities, you would need to collect ethnicity data of those who were successfully using the solution to compare it to the overall population of the target market. Without ethnicity data from your users, it is not possible to do this comparison.

User research is expensive so this reporting requirement will create a regulatory burden for a problem which is not yet apparent. Perhaps it should be a requirement for a limited period of time

to assess if this is a problem that needs monitoring? (and see above for the proposal this takes place at scheme level)

To what extent do you agree that the trust framework will make it easier for people without traditional identity documents to access an online service?

The opportunity to vouch for someone's identity may support inclusivity for identity. It has limited application for age attributes if the Government Digital Guidance on how to accept a vouch as evidence of someone's identity is extended to age attributes, because this guidance excludes relatives and people at the same address from vouching for someone. So a parent could not provide the date of birth of their child. It is hard to imagine how most professionals would be in a position to know the date of birth independently of information provided to them by the parent or child (unless it is from seeing documentation, which rather negates the point of the vouching process). A doctor or nurse could rely on medical records to vouch for a child's age; a teacher could rely on the school's records but these will have originated from parents' claims. The general point here is that schemes within the overarching trust framework will need to have their own standards for acceptable methods – one size will not fit all. Parents may need to be an acceptable source of vouching for age attributes, albeit to a limited level of assurance that recognises the risk that a parent fails to provide accurate information..

What additional inclusion requirements should be included in the trust framework?

Schemes could instead be required to set a de minimis acceptable level of exclusion for participants, reflecting the technical constraints at the time, which could be reduced as technology improves.

Fraud & Security

To what extent do you agree that the counter fraud and security measures will ensure best practice is upheld by trust framework members?

There will be a limited number of general measures to prevent the abuse of the trust framework mark which can be adopted at that level. Other measures will need to be designed to suit the scheme in question taking into account the level of risk and the likelihood of attempted fraud.

The PASS Scheme requires providers to participate in the Identity Fraud Investigations Team (AmberHill) at the Metropolitan Police and to provide information to and cooperate with Action Fraud. One potential issue for Framework providers having automated fraud reporting tools is the potential to overwhelm the counter-fraud agencies. That having been said, the bigger the data highlighting fraud, the easier it will become to spot trends and emerging threat, contributing to the national threat assessment.

Interoperability

To what extent do you agree that the trust framework facilitates interoperability, as defined by the ability to use a digital identity created in one context in another?

In relation to age attributes, the wide range of methods of age assurance and the differing designs of each providers' technical solution will create a trade-off between the conformity required for interoperability and the diversity of methods, level of inclusion, and cost competition. This will

certainly require a bespoke solution at scheme level for age assurance attributes, because often these are held without retaining any identity data at all, or not holding it centrally.

Privacy

To what extent do you agree that the TF provides enough protection for users on use of their data?

This is a very complex area where users are generally suspicious, and their suspicions will be encouraged by libertarian campaigners. So both the substance and the messaging around the framework will need to provide extensive reassurance to secure user trust. The mere fact that certain functions, such as age assurance, are associated with a trust framework which also addresses identity could cause many users to refuse to participate in both, for fear that one leaks data to the other. For example, a major pornographic website launched an age verification product which was designed to provide complete privacy to users with "ID" in the product name. So an age assurance network carrying a "UK Government Digital ID trustmark" would be counterproductive in some circumstances or to some users.

Where the purpose of sharing an attribute – be it employment status, age, health conditions, does not require the disclosure of identity to fulfil the object of the exercise, then users should be able to participate in the process without their identity being required, or at least not retained any longer than necessary to establish the attribute and bind it to the user.

The record of data breaches, and the everyday experience of digital marketing, has made many users reluctant to store or share data, so solutions need to accept this reality and provide substantive reassurance through privacy-by-design, data-minimisation and institutional separation.

Are there any obligations or requirements which may harm the interests of users?

The prohibition on the use of data to profile users for marketing may inadvertently prevent a gambling operator from checking their adverts are not shown to children under 18.

Are there any obligations or requirements which may make digital identity impossible to implement for your organisation?

Note that age verification providers do not universally retain identity data.

Detailed Feedback of Specific Provisions

Introduction

The introduction appears to assume there will be a legislative basis for the TF. It may be that the TF is implemented ahead of legislation commencing, so "must" may not be the correct term.

It may be more appropriate for individual schemes to set the certification profiles, and for the framework to approve the approach taken by each scheme. There may be some common requirements which could be included in the TF, but these may be relatively few.

It is more usual in writing standards to use the term "shall" rather than "must" e.g.

a. "shall" indicates a requirement
b. "should" indicates a recommendation
c. "may" indicates a permission
d. "can" indicates a possibility or a capability

What are digital identities

While, 'a digital identity is a digital representation of a person' is a good succinct way to introduce the concept, it isn't necessarily accurate nor does it square with the potential use cases of digital identity which are recognised elsewhere in the framework (eg. that a digital identity might have a very limited application, even a single transaction, or that an identity could be held by an organisation). A digital identity is also not the whole of a person. So, it seems more accurate to say that a digital identity facilitates the provision of an entity's attributes from, for example, biometric information to legal documentation which have transactional or information sharing value.

It is also worth noting that which a digital identity is not. A digital identity is not age-verification or age assurance, for example. A digital identity product can provide verification of age. But age-verification and age assurance are separate products / services which certainly can be and, in some cases, should be distinct from identity. To fail to recognise the distinction would be a failure to recognise properly the distinction between non-identifying attributes and identity and the importance of understanding that some attributes should be shared only in privacy protecting isolation.

While the TF says that a digital identity can only be created for a real person, 5.1 discusses digital identity and attributes being linked to businesses and what different attributes might be held by the identity in such cases. So, should this be 'can only be created for a real person, who has evidence that shows they exist…' or, 'can only be created for a real entity, that has evidence that shows they exist…'.

It may be better to say "Anyone can choose to create one or more digital identities. They do not have to create any."

While the limited use case is understood, this example would seem to confuse a digital identity with the sharing of individual attributes, the authenticity of which have been verified. A digital identity need not be necessary in all such cases. In the case of a transaction, or to access a service, for which

the only necessary attribute is that a person is over and above a certain age, the need can be met without the transaction being linked to identity. Any encouragement to create a digital identity to carry out 'just one type of transaction' for which identity is wholly unnecessary, and most especially when linking or sharing identity is undesirable, introduces a potential risk of harm to the user by introducing a further holding of identifying attributes which could be compromised. In such use cases the creation of a new identity for such a transaction is not only not needed, it should be discouraged.

Where a user already holds a digital identity which they know (and can trust) will share only the one attribute that, in this case, they are over and above a certain age, without linking any other personally identifiable information, they could of course be expected to use that digital identity product to complete the transaction.

This point speaks not about limiting the value of digital identity products, but only discouraging the creation of limited use identities to share an attribute for which a transaction has no need of identity and where that attribute, for example that a person is over and above a certain age, can be confirmed without proving identity.

Such a reusable identity must be the objective. Otherwise, there is little to be gained by the consumer, or the various entities which might need to confirm identity or other linked attributes.

In order to best deliver the benefits digitally Government must guard against the potential for identities to be created too widely and on the back of small transactions where identity needs to be proven. It otherwise benefits no-one other than those seeking to abuse identity and linked attributes by widening the potential targets. While regulators can govern security and data protection standards, it doesn't stop rogue interests and doesn't prevent breaches of security. A regulator might be forced into a position of acting after the horse has bolted. The creation of digital identities can and should be well regulated and those who only need to prove identity for a single transaction should be discouraged from creating identities themselves, but rather use digital identity services.

What are attributes

The TF takes particularly broad approach and by no means necessarily a bad one. However, there is currently no single official or verified source or holding of such a broad scope of data about any individual in the UK as this proposes, beyond an individual themselves. If a person's identity is compromised, for example by the hacking of a bank database, the individual could expect to fall back on other personal data not held by the bank (and in this example now not held by a rogue player) in order to confirm their true identity and confirm that their identity has been compromised. While creating a comprehensive digital identity allows an individual greater freedom to efficiently complete a wider variety of transactions, it also puts that individual at greater risk if that data store is compromised. No one database currently holds such a comprehensive collection of personal data as the example above envisages. Should the DVLA be breached, an individual's passport credentials would be secure and the individual has an uncompromised means to repair the damage of a breach of their identity.

What data is stored and how it is stored to ensure that breaches of databases do not compromise individual identities is both critical and achievable. But this is best achieved by ensuring that digital identities are created by a well-regulated digital identity industry and not left to a multitude of

individual companies who only need to prove identity for a transaction and not to create a new digital identity in the process.

This also speaks to the need to ensure that age-verification alone is not conflated with digital identity where only the former is necessary to complete a transaction.

However, what remains unanswered is how attributes are shared and made available. Attribute look-ups tend to cost money. So, does an attribute provider share the information and is that information added to a digital identity or, when an attribute is required, does an attribute provider confirm that attribute on a single use basis (consequently paying each time for the look-up)? On the one hand, a consumer might perceive that they are better protected if the attribute is not centrally stored but provided external to their digital identity on an as and when needed basis. But this creates an inefficiency and added cost which may make the accessibility of certain attributes less viable. There are a number of ways to store data and secure it. Ensuring that data is efficiently available will benefit all users. So it should be that a regulator sets high standards for the storage and use of data, rather than limiting, and potentially making unviable, what data might be held.

What the UK digital identity and attributes trust framework does

The UK digital identity and attributes trust framework will let people use and reuse their digital identities. It will also give them a way to share their attributes with other people and organisations more easily. This is true if what constitutes a digital identity is better defined around what we would expect to be common sense understanding, aligned with offline identity, and not potentially open to, or being a result of, any transaction in which the proving of identity is required.

The TF remains very broad and less than as coherent as it needs to be. In order to be more effective and, crucially, to gain the necessary level of public trust in the broadening of attributes most especially, this collection of legislation and standards must surely become more united and understandable.

Is it envisaged that the collection of legislation, standards, GPGs and this document will be distilled into a set of rules against which an organisation can be certified? This would be desirable.

The TF would seem to introduce a wealth of pitfalls. Most especially and dramatically if a user is creating a single use digital identity in order to complete a single transaction, as the earlier example proposes. How is a regulator, where any technology is potentially available and any entity proving an identity to complete a transaction could be creating an identity in the process of approving that transaction, realistically positioned to protect consumers? It rather raises the potential for myriad identities to be created and protections to be weak. It would surely be desirable to best regulate ISPs and better make the distinction between those providing the identity service and those with the identity need.

Benefits for users

It's worth highlighting the distinction in these lines between identity and eligibility. The two are, of course, not the same thing and this speaks specifically to age-verification as distinct from digital identity. An individual's eligibility to purchase certain products or access certain services may have nothing at all to do with their identity, but only their eligibility as an adult. It's a distinction which reaffirms the need to ensure that digital identity and age-verification are not conflated to the detriment of the latter.

Who runs the trust framework

It seems that two primary candidates emerge given both the focus on personal data and the often financially motivated uses of that data: the Information Commissioner's Office and the Financial Conduct Authority. Who is the better of the two most obvious regulators, if one is not already considered most suitable, will require not only more investigation of these regulator's capability, but also responses to questions raised and better defining of exactly who is being regulated and to what standards.

Realistically, it is difficult to envisage a 'generic' trust framework certification scheme covering any type of identity or attribute for any use case. It would seem more likely that there would be a series of vertical schemes supporting particular use cases, like conveyancing, pensions, financial transactions, age assurance, etc. Although ultimately the market will decide based on demand and throughput of certification activity, it is also difficult to see there being many multiple certification schemes in each vertical. There's probably simply not enough certification clients in the market to make that realistic.

It is also important to recognise that some Digital ID and Attribute Services support multiple use cases, so either they will have to get certification through multiple vertical certification schemes or there is some form of mutual recognition and respect for other certification providers. One option is to have 'common' features across all certification schemes and then 'bespoke' provisions specific to that vertical. A provider across multiple verticals would then only need to prove compliance with all of the common features by one certification scheme, adding just the bespoke provisions as they expand into new markets and use cases for Digital ID and Attributes.

Who can use the trust framework

There may also need to be the ability for a scheme to disapply some rules of the trust framework as one size fits all may not be tenable.

The Age Verification sector is developing interoperability within a trust framework built on BSI PAS 1296:2018; this is being extended across the EU under a new draft ETSI standard and there is an intention to develop an ISO as soon as possible. Accepted practice is to build standards as globally as possible

There has been considerable activity on Age Assurance Certification over the last few years since the publication of PAS1296:2018. Although not directly an auditable standard by itself, it gives sufficient frameworks for narrative certification of age check systems.

It would be useful to map the existing schemes or emerging schemes for the benefit of having a wider understanding of the market place.

Need to be careful (potentially) to distinguish between a 'Scheme Owner' and a 'Certification Scheme' or a 'Conformity Assessment Body'. They may be the same or they may be different. Note 1 in the definition of Scheme Owner is ISO 17067 states that they could be the Certification Body itself, a governmental authority, a trade body, a group of certification schemes or others.

A rule that the scheme operator must not do anything that stops digital identities or attributes from being shared between members of the trust framework may not be practical where attributes are not associated with identity or permission has not been granted by the user for those attributes to be shared or associated with their identity externally to the attribute provider

There may be certification rules that are deliberately and properly restrictive about the onward usage of data for good policy reasons. As an example, the PASS Scheme rules prohibit the use of personal data from ID verification for marketing purposes They have to get a separate consent regime); so if there were a separate scheme regarding Marketing Digital ID, then this provision would effectively permit cross-use of the data.

There are also concerns about lawful basis for processing and compliance with the ICO's Data Sharing Code. Such a blanket ban on sharing across members of the trust framework would remove consideration of necessity and proportionality.

The ability for Scheme Owners can also give members guidance and support on how to build products and services that are optimised for their users is a risk to impartiality. It potentially confuses the role of a certification body with that of a consultancy or advisory service. As a fundamental principle, a certification body should not find themselves in a position where they are marking their own work.

The use of the words 'for the role you want to perform' means that it is critical that the target of evaluation for the certification process is fully and adequately identified. This can be very challenging and end up being quite long winded. It is obviously important that certification by one scheme in one vertical does not suddenly approve a provider to provide any kind of Digital ID or attribute service across any vertical. This would need some very specific guidance on what the target of evaluation is.

We are not convinced that all attribute services are necessarily always needing the user's agreement. The lawful basis for processing of personal data are wider than that. As an example, you might have an attribute detection service 'detecting whether or not the cognitive ability of a user is/is not likely to suggest that they are an adult' - this could be operating within a system and indicating (sharing) with a relying party that a particular user may not be an adult. That would prompt the relying party to undertake secondary checks if being an adult was a pre-requisite of user access to the service. Such an attribute detection service would not necessarily be done with the users agreement and, indeed to seek the users agreement may defeat the object of the service.

Rules for identity service providers

Create a digital identity

The term 'must follow the guidance' is poor use of language in certification/standards/requirements.

There is ambiguity here: "must follow the guidance"...."might not need to follow the whole guidance". Should also say something along the lines of, set out in the most recent update, given it was first published in 2014 and then reiterated, most recently in 2021

Manage digital identity accounts

The ability to close accounts needs considerable consideration. We are effectively granting an authority to a Digital Identity provider to decline access to someone's digital ID or even delete it entirely. That could have serious consequences for the individual. There is no doubt that this could be appropriate, but who decides what is appropriate? Is there a right to appeal/redress?

It may not be appropriate to close an account because the user has died. Although you would expect the fact that the user has died to be a new attribute associated with the account. This would be rather dependent on the circumstances of the use of the digital ID. And on whose authority, would an ISP assume death. Production of a death certificate?? How would next of kin necessarily know someone had a digital ID?

The ability to close the account if you have evidence it's being used by someone who should not have access to it has very significant unintended consequences – particularly for hijacked or compromised identities.

We think there is considerably more to identity recovery services than just a reset password. Compromised and hijacked identities can be very difficult for the genuine holder of that identity to recover.

The monitoring of transactions implies that you must track the use of the digital identity for transactions. Does this create a digital footprint of behaviours of the individual.

Make sure your products and services are inclusive

There are many potential reasons for inherent bias, the training data used to establish the algorithm, the quality of the capture device used, the physical properties of light, the behaviour, predilections or attitudes of users, cognitive abilities, and many more.

Rules for attribute service providers

There may also need to be the ability for a scheme to disapply some rules of the trust framework as one size fits all may not be tenable.

Create attributes

You could give PAS 1296:2018 as an example of a framework for scoring an attribute's reliability and security

The use case may not require that the attribute is bound to a person, but perhaps to a transactional decision – a gateway decision. Age Assurance is a good example of this. A gateway may need to 'attribute' of a person engaged in a transaction or at a gateway indicates that they are over 18 – you can do that without an 'identifier' of the person.

Some attributes do not require updating per se – age is a good example. But there may be a requirement in specific use cases for a verification to have been completed within a specified time period, or even for a fresh verification to be carried out. Attribute providers should not be required to share the date on which the attribute was last updated; merely to confirm it is sufficiently recent for the purpose at hand. This is to preserve the value of attributes and mitigate the risk of a secondary grey market in previously shared attributes, because it will not be possible to confirm that a second-hand attribute is still recent enough without reverting to the original attribute provider.

Rules for all trust framework participants

Providers may not wish to disclose their data sources - instead reference should be made to standards, and the provider audited and certified to confirm that their methods meet those standards.

It will be imperative to resource the relevant authorities to provide appropriate channels to receive regular reporting and analysis of identity fraud and identity misuse and a subsequent feedback loop.

A distinction needs to be made in terms of checks when an account is created; versus fraud or crime that may be committed post account creation. Some providers may contract with relying parties to provide identity or attribute checking throughout a customer lifecycle. Some may be purely involved at the stage of account creation. Hence the window for meta data and artefacts may differ in duration.

Respond to incidents

Companies require a process to review requests to disclose personal information from law enforcement or bodies from the UK and overseas and need to ensure that:

- the request is valid;
- the information requested is no more than necessary;
- It can be disclosed compliantly

Organisations must undertake industry best practice to prevent the creation of synthetic digital identities or fraudulent digital identities, as detailed in its GPG 45 compliance.

In addition it will be imperative to resource the relevant authorities to provide appropriate channels to receive regular reporting and analysis of identity fraud and identity misuse and a provide back a subsequent feedback loop.

A different entity may manage the investigation will depend on the industry or sector where the incident happened.

Keep records

The private sector does not usually have a dedicated records management function as you would typically find in a public sector body. These duties may be managed by a data protection officer and a CISO (Chief Information Security Officer). An Information Security Management System may be established to protect and maintain the confidentiality, availability and integrity of all a company's information assets.

Glossary of terms and definitions

Attributes:

"information about a subject which relates to an individual" [BSI PAS 1296:2018]

Relying party:

Organisations that rely on (or 'consume') products or services from trust framework participants.

Scheme:

A group of different organisations who agree to follow a specific set of rules around the use of digital identities and/or attributes.

Trust framework:

Underlying legal structure of standards and policies that defines the rights and responsibilities of participants in an identity ecosystem, specifies the rules that govern their participation, outlines the processes and procedures to provide assurance, and provides the enforcement mechanisms to ensure compliance [BSI PAS 1296:2018]

Vector of trust: string-based representation that communicates the level of reliability in the processes leading up to and including the authentication process itself [BSI PAS 1296:2018]

Vector: multi-part data structure, used here for conveying information about an authentication transaction [BSI PAS 1296:2018]

Level of assurance: process by which a provider is able to confirm an attribute to a specified degree of confidence [BSI PAS 1296:2018]

ENDS