Open Identity Exchange

The UK digital identity and attributes trust framework

ALPHA – February 2021 release

OIX Response

11th March 2021

Version 1.0

Author: Nick Mothershaw
Email: nick.mothershaw@openidentityexchange.org
Mobile: 07885 618523

1 Foreword

On 11th February 2021 the Department for Digital, Culture, Media and Sport (DCMS) released the ALPHA version of "The UK digital identity and attributes trust framework" for review.

OIX sees the ALPHA UK Trust Framework as a good step towards defining how Digital ID can work successfully to support the UK economy.

Our feedback is extensive and designed to be taken as a whole to improve the framework and make sure it's pitched at the right level: not too detailed, but not too light. It must be "just right" to ensure trust and security are achieved whilst allowing private sector adoption and innovation. In summary, OIX calls for the government to consider:

- **Identify Proofing** (GPG45) to be more clearly positioned as guidance, not rules. Move to a joint drafting team with private sector input. The profiles defined then become start points for sector Scheme overlays and comparison points to assist interoperability.
- Define binding processes for **Attributes** so relying parties can better understand how an attribute has become associated with a user. But a scoring methodology for attributes is not necessary.
- Identity Service Providers that specialise in **Inclusion** should be encouraged. Inclusion success is then measured as a whole across the ecosystem.
- Introduce **Interoperability** rules that ensure users can use an ID of their choice across multiple sectors.
- Simplify **Operational, Security and Legal** rules: create lists of supported standards and regulation, then simply refer to these from the trust framework.
- Create a new specialist identity **Governance Body** as a private-public collaboration to ensure private sector suitability and innovation.

The ALPHA acknowledges that it does not yet cover the detail required in some key framework areas, such as Accreditation, Liability, Trustmark, Interoperability and Governance. These are some of the fundamental areas of trust formworks that OIX is most often asked about. They are some of the most challenging areas in a trust framework and need to work in harmony. Get these areas right and the trust framework will be a success, get them wrong and it will fail. This is particularly true when a framework is designed to create a commercial marketplace of ID services, as this the UK government's objective. OIX is keen to collaborate and co-create in these areas to ensure Digital ID in the UK is a success.

We welcome the consultative approach government is taking in the definition of the UK Trust Framework. OIX would like to see this go further and move immediately to co-creation. UK government should create the seeds of the required governance body for Digital ID as a public-private co-creation team to complete the UK Trust Framework. This will help ensure it is embraced by the private sector and becomes a success for the UK.

2 Introduction to OIX's Responses

This review was produced by OIX members through a series of workshops.

OIX key recommendations at this stage of the Trust Framework are highlighting in the next section.

The DCMS online survey imposed a word count limit on each section. Where OIX's response was too verbose it was condensed to fit into the survey. This document contains the full responses prior to them being edited down. These response points are highlighted in grey in the detailed section of this response. Key areas where OIX had to condense comments in the survey submission were around:

- The proposed Governance Body
- Identity Proofing
- Examples on Bank and Electronic signature use.
- Attribute Scoring
- Interoperability

In this response document, OIX has also called out:

- The importance of the response point on a High, Medium, Low basis. The reader's attention is drawn to those marked as High as the most important points DCMS are asked to consider in the evolution of the framework. These have been highlighted in yellow in the Importance column below.
- Where the current level of detail in the ALPHA framework is "too little" or "too much".

3 OIX Key Feedback

Key feedback from OIX on the ALPHA version of the UK trust framework is summarised as:

Principles: The trust framework does not reference the Principles that have been defined for Digital Identity by HMG. These should be in this document or referenced through a link.

Mixed level of detail: Some areas of the trust framework need more detail to ensure clarity, consistency and compliance. Other areas are too detailed, often reciting selected rules from referenced legislation or standards.

Rules not Recommendations. In several areas the ALPHA framework reads more like a guide with recommendations than a set of firm rules. An example is in the section on Interoperability: "Future iterations of the trust framework will **recommend** technical specifications to **encourage** interoperability". A Trust framework should set clear rules to achieve its aims, not make recommendations. There may be areas where there are different options that are acceptable to meet the rules.

Interoperability. If users are intended to be able to use a single ID of their choice across many different sectors, use cases and schemes, then the framework needs to make this a clear objective and include rules to ensure this is achieved.

Identity Proofing. OIX would like to see DCMS working more closely with the private sector on the definition of guidance – perhaps through a joint drafting team? More levels in GPG45 may be required to allow for private sector adoption, otherwise inclusion will go backwards, not forwards. Or should the GPG confidence levels be regarded purely as a starting point for Schemes to build from to apply sector specific rules?

Attribute Scoring. An attribute scoring methodology as outlined in the ALPHA trust framework is not required. Relying Parties can and do interpret securely delivered trusted attributes for themselves without the need for a centrally defined scoring methodology. An attribute binding process definition however would be useful.

Liability: The framework should lay out liability options - not rules. If the framework attempts to address liability and gets this wrong the framework will fail. Liability is a commercial matter; government should not set conditions for liability or limitations. Liability considerations should be left to sector based Schemes as each use case has different liability considerations.

Trustmark: There must be a single Trustmark for the UK if IDs are going to be interoperable across sectors.

Governance: OIX recommends a private-public governance partnership to ensure customer focus, innovation and help drive and support adoption. This should be a new specialist governance body specifically created for identity; it should not be appended to an existing body.

Roles. Clear roles are necessary for framework adoption. Schemes need more definition; are they always groups of Organisations? Within Orchestrators: Brokers and Distributed ledger services are very different. Where do CIAM solutions fit? Should CIAM solutions be able to get certified as a selling feature to RPs? Where do SSI providers fit (in Attribute Providers we think)?

Applying Rules to Roles: Do all of these the section 5 rules always apply to all roles in the framework? There should be a cross reference to which part of this section applies to each role.

Inclusion: Are all IdSPs compelled to be equally inclusive? – if so, the market is unlikely to be very competitive. Or can IdSPs specialise in particular demographic and still be accepted?

4 Detailed Comments

Section	Existing Wording	Level of Detail (Too Much, Too Little)	Importance of Comment (High, Medium, Low)	OIX Comment
1.0 Introduction	This document explains what requirements organisations will need to meet to be certified against the trust framework in the future.		M	It could be clearer that both centralised IDs and wallets are supported, as equal.
1.0 Introduction	This document explains what requirements organisations will need to meet to be certified against the trust framework in the future.		L	Whilst the examples add colour, OIX would not expect to see specific examples in a Trust Framework. They may be in a supporting document that explains the Trust Framework.
1.0 Introduction	Organisations must meet these requirements alongside the rules of any other contracts, policies or legislation that they already follow.		H	The Trust Framework does not reference the Principles that have been defined for Digital Identity by HMG. These should be in this document or referenced through a link.
1.0 Introduction	Organisations must meet these requirements alongside the rules of any other contracts, policies or legislation that they already follow.		H	The trust framework does not reference existing guidelines for ID verification and ID generally. These often refer to global and EU standards for ID. Does the UK Trust Framework supersede these? Examples are: PAS499 PAS1926 PAS8626 JMLSG Guidelines for ID verification and anti-impersonation.

1.0 Introduction	This document does not explain: what requirements (or 'certification profiles') organisations will be certified against - these will be published later this year following the first round of feedback what legislative or governance arrangements are needed to make sure the trust framework is ready for use in the economy		M	There are other UK guidelines / standards that already refer to, of lift sections from, the Good Practise Guides. Will these standards be updated to be part of the new UK Trust Framework, perhaps through Schemes that will own the intersection of the trust framework and the needs of different sectors? Examples are: Land Registry Safe Harbour NHS Patient Online Services in Primary Care
1.0 Introduction	There are still some elements missing from this document.		H	It is difficult to comment on the Trust Framework when major and key elements are missing. (e.g., interoperability/ liability). The requirements for the missing elements may colour the rest of our comments.
1.0 Introduction	limitations on liability (including unlimited liability, limited liability and excluded losses)		H	The framework should lay out liability options - not set hard rules. If the framework attempts to address liability and get this wrong the framework will fail. Liability is a commercial matter. Government should not set conditions for liability or limitations. Liability considerations should be left to sector based Schemes as each use case has different liability considerations.
1.0 Introduction	We use 'user' to refer to people who will use digital identity or attribute products and services to prove their identity or eligibility.		L	As user could be an individual or a legal entity. Also "things" can be users.
1.1 What are digital identities	A digital identity is a digital representation of a person. It enables them to prove who they are during interactions and transactions.		L	Are you aiming to say that under this framework a Digital ID has at least some degree of trust? Whether it is re-usable or one off.
1.1 What are digital identities	Other digital identities will be 'reusable', which means they can be used again and again for different interactions and transactions.		H	There must be a single Trustmark for the UK if IDs are going to be interoperable across sectors. The OIX paper on trust marks recommends an overarching trust mark with sector (scheme) specialisations to enable relying parties who understand who is certified for their sector and users to understand where they can use their interoperable IDs. From an end user perspective, the Trustmark won't work

				unless it is clear where a user can use a particular ID: where is their ID certified for use? Will users need different IDs for different sectors? What consumer positioning and promotion will the framework governance body undertake to ensure users understand where they can use their ID?
1.1 What are digital identities	Example: Peggy is buying her first home…		L	Needs to be clear what roles in the framework the credit scoring agency and bank are playing. Being a member of a Scheme does not mean they are an account issuing IdSP.
1.2 What are attributes	Some examples of attributes are:		L	More diverse examples: behavioural, biometrics.
1.2 What are attributes	Attributes are created, collected and checked by an attribute service provider. An attribute service provider could be an organisation or a piece of software, like a digital wallet.		M	Is a wallet an ASP or an IdSP? If the wallet is a reusable account, isn't it a form of IdSP? Especially if the wallet issues authenticators to the user to enable them to access the wallet and present credentials.
1.3 What the UK digital identity and attributes trust framework does	To meet the rules of the trust framework, you will need to prove you're able to safely manage users digital identities or attributes. The rules will be 'outcome based'.		M	What is meant by "outcome based" needs further explanation.
1.4 What you get from being part of the trust framework	What you get from being part of the trust framework		L	Should 'benefits' be listed in the Trust Framework? These should perhaps in a separate document promoting the Trust Framework.
1.5 Benefits for users	Benefits for users		L	Legal Entity benefits are not listed? Or, should user Digital ID be prioritised and then legal entities tackled as a second step?
1.5 Benefits for users	The UK government plans to make it possible for this to happen across different industries, sectors and countries where it's safe and legal to do so.		H	Clearer objectives for interoperability for users are required. The Trust Framework should contain rules that enforce interoperability for ID for users, not make it a plan. There should be success criteria for interoperability e.g., if they choose to, a user can use a single ID across all Schemes and all use cases.

1.6 Who runs the trust framework	Who runs the trust framework		H	OIX recommends a private-public governance partnership – for the following reasons: • Continued Innovation more likely • More Customer Experience and Service focused. • Introduces a level of commerciality: rules must enable a private sector market, rather than put barriers in place. • Can help private sector build benefits cases for use. • Ensure transparent fair exchange of value, not a regulatory tax on identity consumption. • More likely to create a market for Digital ID.
1.6 Who runs the trust framework	The trust framework will be overseen by a governing body		H	Any such body needs to be responsible for the definition, implementation, operation and ongoing innovation of the trust framework. This is more than just an oversight role, it's a market development role. Again, best served by a private-public partnership.
1.6 Who runs the trust framework	The trust framework will be overseen by a governing body		M	What are the measures this body will report on? Are these the outcomes previously mentioned?
1.6 Who runs the trust framework	chosen by the UK government		M	"Chosen" implies an existing body. The governance body needs to be specifically created for this purpose as Identity is a specialist area. Designating as a service such as OFCOM is not the right thing to do. Digital ID is much more complex and layered market. Identity doesn't fit into any existing "OFxxx" at the moment. Appending this to another body is unlikely to result in identity getting the focus it requires.
1.6 Who runs the trust framework	chosen by the UK government		M	Is this going to be part of the Critical National Infrastructure? If so, what does this imply in terms of the selection / creation of the governance body.
1.6 Who runs the trust framework	The governing body will work with other bodies and organisations to make sure that using the trust framework is as straightforward as possible.		M	OIX wishes to work with the governing body on behalf of its members and the broader ID community to ensure OIXs vision of interoperable trusted Digital IDs is achieved. OIX could be considered as a start point for the private sector element of a governing body.

1.6 Who runs the trust framework	The governing body could be responsible for		M	Should there be clear separation between policy / governance and operational elements? Conflating means there is potential political conflict.
1.6 Who runs the trust framework	The governing body could be responsible for		M	OIX recommends the following additional responsibilities: • Making sure user and technical interoperability is achieved and is successful across the market. • Accreditation and Auditing on an ongoing basis. • Handling termination / withdrawal of accredited bodies to the market. • Preventing unauthorised use of the Trustmark.
1.6 Who runs the trust framework	making sure all participants follow the rules and standards		M	Will there be fines for those who fail to comply with the framework? If so, this might affect who the governing body may be.
1.6 Who runs the trust framework	system level security and fraud, including sharing information and early warnings about anything that could affect the security of the trust framework or its participants		M	Too detailed for the framework. May report on this, but not responsible for. What does "system" mean in this context?
1.6 Who runs the trust framework	approving the creation of schemes and maintain oversight of them through the scheme operator		M	Approving the creation of a scheme sounds like the governance body is controlling the free market. Accrediting schemes to the framework would be a more acceptable responsibility of the trust framework.
1.6 Who can use the trust framework	Organisations can use the UK digital identity and attributes trust framework: by themselves as a single organisation as part of a 'scheme'		M	How do single organisations use the trust framework? Can they get separately accredited by playing the other roles in the framework? For example, a relying party who also does their own ID Proofing? Or a commercial organisation who plays the role of an IdSP and ASP but is not part of a Scheme? When is a single org going to use the trust framework without a scheme? What determines when a single organisation can or can't join? Could you provide an example of an organisation who might be a "single organisation" in his context?

				Can a Scheme be a single organisation? It must always be a group of organisations?
1.6 Who can use the trust framework	A scheme is made up of different organisations who agree to follow a specific set of rules around the use of digital identities and attributes. These organisations might work in the same sector, industry or region, which means they will build products and services for similar types of users. A scheme can help organisations work together more effectively by making it easier for them to share information. They can do this by adding additional requirements to the rules of the trust framework.		H	Is OK for an organisation to play the role of IdSP and orchestrator and scheme all the same time? Or should there be clear separation of responsibilities between Schemes and the other roles in the Trust Framework? Suggest this paragraph is extended to include: "A scheme might address specific regulatory, or compliance needs that the framework doesn't cover". How is the framework going to require schemes to work together to ensure interoperability?
1.6 Who can use the trust framework	Some relevant schemes already exist or are being developed, while others could be developed in the future.		H	This describes the sector based collaborative schemes well such as the TISA and HBSG schemes well. Are commercially led propositions, where one organisation is creating the scheme and the other organisations are their customers also a scheme?
1.6 Who can use the trust framework	The scheme operator must follow the rules of the trust framework.		M	Can the scheme operator agree with the governing body that a rule does not apply or can be varied in the scheme's operational context?
1.6 Who can use the trust framework	A scheme is created and run by a scheme operator. The scheme operator must follow the rules of the trust framework.		L	The scheme operator must ensure that members of the Trust Scheme follow the rules. Not follow the rules itself.
1.6 Who can use the trust framework	explaining how the scheme has been certified		L	Does this mean explaining how the scheme certifies it members?
1.6 Who can use the trust framework	explaining how the scheme has been certified		H	What is the approach to certification: Framework then Scheme. Or Framework via Scheme?

1.6 Who can use the trust framework	explaining how the scheme has been certified		M	Can Schemes issue their own Trustmark in additional to the framework?
1.6 Who can use the trust framework	Whether an organisation uses the trust framework on their own or as part of a scheme, they will need to perform at least one of the following roles, as set out in the paragraphs below:		H	A diagram showing the trust framework, schemes, the other roles in the framework and how they all interrelate would be useful. Also, some example use case journeys. OIX has published diagrams that may help in this area within its Guide to Trust Frameworks. OIX is also working on newer versions of these diagrams to ensure wallet based approaches are clearly supported. OIX would be willing to share these with DCMS.
1.6 Who can use the trust framework	An identity service provider might not need to do all parts of the identity checking process. They can specialise in designing and building components that can be used during a specific part of the process. For example, they could develop software that checks if identity evidence is genuine and valid.		H	When does a component level IdSP need, or qualify, to be accredited to the framework? When they have enough to score something in GPG45? If they provide less, or more basic information, do they sit outside of the trust framework as Evidence Providers?
1.6 Who can use the trust framework	Other identity service providers might choose to create an account associated with a user's identity.		M	When this is done the IdSP must Maintain Trust in the ID when it is reused. The framework should cover this requirement.
1.6 Who can use the trust framework	…. if they have the user's agreement.		M	What is meant by agreement? It would be better to say, "any legal basis under Data Protection Act 2018". This would then be in line with the attribute documents.
1.6 Who can use the trust framework	Attribute service providers must also describe the quality of the attributes they keep. Relying parties and identity service providers will use this information to choose which attribute service provider they request attributes from.	Too Much	H	This is over prescriptive. This should not be in the Framework. Will not help or enable the market. It will create a barrier in what is an existing and successful market. Attribute providers do not do anything like this today. Relying parties select attribute providers without a methodology like the one proposed. The quality and features of attributes are a competitive feature.

				A simpler standardised method of communicating the binding an attribute to an ID would be of use.
1.6 Who can use the trust framework	Orchestration service providers		H	Needs more definition. Brokers and Distributed ledger services are very different. Brokers have multiple options: simple selector hubs Vs trusted ID and Attribute hubs that call attributes of the back of an ID from and IdSP. Where do CIAM solutions fit? Should CIAM solutions be able to get certified as a selling feature to RPs? Where to SSI providers fit (in Attribute Providers we think)? Clear roles are necessary for framework adoption.
1.6 Who can use the trust framework	This means that organisations such as airlines, banks and retailers do not have to check users' identities or attributes themselves.		L	These organisations still have to make sure the users' details are correct and meet their regulatory needs: are the users authorised to undertake the transaction they are trying to undertake. They are relying on a third party (IdSP / ASP) to gather and verify that data for them only.
2.1 Create a digital identity	All identity service providers must follow the guidance		H	OIX would like to see DCMS working more closely with the private sector on the definition of guidance – perhaps through a joint drafting team connected to the future governance body. The rules so far are largely from the Verify programme – which didn't work in government, so why will this work in private sector? They do not align with current private sector rules. Examples are SCA from PSD2, JMLSG Guidelines. Private sector may not want to adopt the GPGs as they stand. More levels in GPG45 may be required to allow for private sector adoption, otherwise inclusion will go backwards, not forwards. Or should the GPG confidence levels be regarded purely as a benchmark for interoperability and a starting point for Schemes to build from to apply sector specific rules? So, a scheme can say any Low is acceptable, but certain overlays must be applied. Or scheme can say some medium profiles are acceptable, but others medium profiles will require an overlay to fill gaps that sector based legislation requires, such as the JMLSG rule that one piece of evidence must contain a name or address.

2.1 Create a digital identity	Create a reusable digital identity		M	If you do not create a re-usable ID, are many of the obligations later in section 5 of the document required?
2.1 Create a digital identity	Create a reusable digital identity		M	Is a Verifiable Credential a Digital ID, as opposed to an Attribute? Should an issuer follow GPG45 and a holder (or their wallet) follow GPG44.
2.1 Create a digital identity	a bank could reuse a user's details from when they signed up to online banking to help them create a digital identity		H	If a bank did this themselves this would make a Bank an IdSP, thus attracting all the obligations that go with this role. As this is currently laid out in the draft framework this will make banks entering the market as IdSPs commercially challenging. Banks are extending the Open Banking API to allow them to share more data about users for ID purposes. This is can be shared with IdSPs and relying parties directly. In this instance the bank is not playing the role of an IdSP, but of an ASP. The bank will use its own non-GPG44 authenticators to release the data into the ecosystem – a mapping of Bank Authenticators to GPG44 Authenticators and GPG45 Verification would be useful. Will a bank comply will all of Section 5 to be an Attribute Provider?
2.1 Create a digital identity	a qualified trust service provider could use an existing electronic signature to create a digital identity for a user		L	Incorrect – TSPs issue certs to users. A better example would be that a QTSP could use a Digital ID as the Qualifier to issue a Qualified Certificate that as user can use to create a Qualified Electronic Signature.
2.1 Create a digital identity	you must manage any digital identity accounts		M	Better definition of "digital identity account" would be useful. Is a wallet a digital identity account, or just somewhere to hold attributes?
2.1 Create a digital identity	You can close an account if the user: has used the account to do something illegal has not followed the terms of use they agreed to wants to close it has died		M	The 1st section asks what if a user wants to close their account, or it has been used for illegal purposes. The 2nd section talks about recovery of accounts that have been stolen.
2.2 Manage digital identity accounts	You must 'suspend' the account before you close it.		M	The requirement to suspend an account before closing is unnecessary.

				This section is mixing user driven processes and reactive processes in the event of fraud. There are several separate scenarios to consider: ○ Known user whose account has been suspended due to lack of use. ○ Known user whose account has been suspended due to contra indicators (e.g., repeated logon attempts, new device). ○ Known user who wants to close their account – no need for suspension. May need a cooling-off period where the user could reopen their account if required. ○ Account taken over by a fraudster – in this instance the IdSP needs to repair the ID (rather than recover).
2.2 Manage digital identity accounts	You must prove and verify the user's identity again. You should aim to get a higher level of confidence than you did when you first set up the digital identity account. This will help you be sure that the user is not an impostor.		M	This is harsh when the user is a victim. The user does need to be re-identified, but by different method not a higher LoA. This may exclude users who are victims.
2.2 Manage digital identity accounts	If the user wants to change their contact details, you must do a 'verification' check to make sure they're the same person who created the digital identity. You will need to get at least the same score you currently have.		M	This seems overkill. The user should be verified, but that is done partly by the user having asserted their authenticators. A lower level of verification would therefore be acceptable. OR the IdSP just needs to validate the new attribute, not reverify the whole user.
2.2 Manage digital identity accounts	You should use a different channel to contact the user if you can, for example by phone, post or email. You should do this using contact details that you know belong to the person who created the digital identity.		M	Channel considerations: If you are using step up, why is another channel necessary?

2.3 Make sure your products and services are inclusive	One of the aims of the trust framework is to make it as easy as possible for users to create and use digital identities (either online or in person).		H	More explanation requested on the objectives. Are all IdPs compelled to be equally inclusive? – if so the market is unlikely to be very competitive; it will be serviced by a few broad IdPs who have deep pockets, or IdPs with monopoly access to certain data. Or can IdPs specialise in particular demographic and still be accepted? How does this flow down to schemes? Certain use cases have specialist user groups, so how does this apply here (e.g. blue badge, high net wealth).
2.3 Make sure your products and services are inclusive	You can also choose to accept a declaration from someone that knows the user (known as a 'vouch') as evidence.		M	Must all IdPs therefore have an offline option for ID creation? i.e. face to face or vouching. This should be specialist IdPs only. Would all IdPs have to implement and support vouching? Or this this a specialist service?
2.3 Make sure your products and services are inclusive	You can also choose to accept a declaration from someone that knows the user (known as a 'vouch') as evidence.		M	Vouching will be vulnerable to fraud. How will this be mitigated against?
2.4 Make sure your products and services are accessible	You must follow the accessibility regulations if you're a public sector organisation that's developing apps or websites.		L	Is the intent of the framework that these regulations must be followed by IdSPs providing services to public sector?
2.4 Retiring your product or service	Retiring your product or service	Too little	M	Needs to be a numbered sub-header. Seems to little. Suggest this is extended: • IdPs should have an appropriate termination plan, including Notice periods and consumer / RP support handover support. • Scheme operator needs obligation to notify governing body.

3.1 Create attributes	Sharing attributes		L	Is this the right word? Would Presenting be a better alternative? Aligns with W3C and OIX.
3.1 Create attributes	Sharing attributes		M	If the user has a Verifiable Credential and shares this, is the user an attribute provider? Or is their wallet an Attribute Provider? Or is the Issuer the Attribute Provider.
3.1 Create attributes	if the person or organisation requesting it has the right to see it		M	Does the attribute provider need to check the person has the right to see it if the organisation requesting it is trusted and has established trust in the user?
3.1 Create attributes	You can then share it in an appropriate way.		M	Consent – how has the user consented for it to be shared? Who is this captured by? It is OK for the organisation requesting the attribute to capture consent, or must the attribute provider capture it?
3.1 Create attributes	You can then share it in an appropriate way.		M	When attributes are presented from an IdSP to an organisation, does the attribute provider need to gather consent again?
3.1 Create attributes	You can then share it in an appropriate way.		L	Are share's timebound? (e.g. 90 day open banking).
3.1 Create attributes	You can then share it in an appropriate way.		L	Is date last updated required to be shared.
3.2 Scoring attributes	Scoring attributes	Too Much	H	A simpler standardised method of communicating the binding an attribute to an ID would be of use. Something along the lines of: The attribute was connected based on • a "matching data set" self-attested by the user • a unique number self-attested by the user. • a matching data set and a unique number self-attested by the user • a verified matching data set (the LoA of the verification might be a factor) • a verified matching data set (the LoA of the verification might be a factor) and a unique number self-attested by the user • by the attribute issuer verifying the user to a low level of confidence. • by the attribute issuer verifying the user to a medium level of confidence.

				• by the attribute issuer verifying the user to a high level of confidence. • by the attribute issuer verifying the user to a very high level of confidence.
3.3 Make sure your products and services are accessible	You should always make sure users have more than one way to use your product or service. For example, a user should have another way to create a digital identity if they're unable to use the online service.		L	Not relevant in this section for attributes?
3.4 Retiring your product or service	Retiring your product or service		M	Similar comments to previous section on retiring a product or service.
3.4 Retiring your product or service	You must also decide how you will manage user's requests for 'data portability', which allows users to obtain and reuse their personal data for their own purposes across different services. Data portability requests may be more likely to occur when a product or service is being retired.		M	Why only on attributes, and not on whole Digital ID Why only on retirement? User can ask for portability at any time. Why referenced here? – it's general data protection law.
4 Rules for orchestration service providers and relying parties	Rules for orchestration service providers and relying parties	Too Little	M	Are there really no specific rules for these parties?
5.0 Rules for all trust framework participants	Rules for all trust framework participants		H	Do all of these rules always apply to all roles in the framework? Will all attribute providers need to comply with Section 5.10 on Fraud Management for instance? Do all of these rules apply to Orchestration providers and in particular RPs? There should be a cross reference to which part of this section applies to each role – per the OIX Trust Framework Guide approach.
5.0 Rules for all trust framework participants	Rules for all trust framework participants		M	Where appropriate a governance process suitable for smaller businesses and start-ups should be considered. For example, IASME as an alternative to ISO27001.

5.1 Making your products and services interoperable with others	Making your products and services interoperable with others	Too Little	H	If users are to be able to use a single ID of their choice across many different sectors, use cases and schemes, then the framework need to make this a clear objective and include rules to ensure this is possible. What are the interoperability goals of the framework? • Cross Sector within UK • International • For the user so the IDs work everywhere. • For the relying party so data delivered is consistent regardless of the IdP This section seems to focus on the last goal only.
5.1 Making your products and services interoperable with others	Future iterations of the trust framework will recommend technical specifications to encourage interoperability between organisations and schemes, in the UK and internationally.	Too Little	H	What would be the contents of these specifications? These should recognise and adopt global and existing UK data and ID standards where possible.
5.1 Making your products and services interoperable with others	Future iterations of the trust framework will recommend technical specifications to **encourage interoperability**		H	This should be “require” not “encourage” if you are going to achieve interoperability in the UK. If interoperability is only encouraged and not ensured and achieved, this will not be a successful framework. For international – international alignment and interoperability need to be considered. **Trust frameworks define rules and requirements, they do not make recommendations.**
5.1 Making your products and services interoperable with others	Future iterations of the trust framework will recommend technical specifications to encourage interoperability		M	A basic need for interoperability is a common agreed and enforced Data dictionary of attributes and attribute values. This should be aligning to international specification/standards (e.g. IANA/OIDF) with local attributes managed by a local governing body. OIX could

				take this role for the UK, working with OIDF for global alignment. This is supported by the OIX members. Certified conformance to tech standards should be required.
5.1 Making your products and services interoperable with others	The specifications should be followed by: all attribute service providers any identity service providers that create reusable digital identities all relying parties		M	Must not Should. Why not orchestration providers? If they manipulate data they must comply with interoperability requirements, and may be enabling interoperability by doing so. Why do RPs need to follow this requirement? RPs benefit from interoperability; they don't need to follow the rules.
5.1 Making your products and services interoperable with others	any identity service providers that create reusable digital identities		M	Why not all IdSPs?
5.1 Making your products and services interoperable with others	You must be able to validate you are receiving messages from an approved organisation or scheme. You could do this by: having a database of approved providers or schemes running public key infrastructure (PKI) using a distributed ledger technology (DLT) model		M	This is a requirement of a Trust Framework but not relevant in this section. This should be a separate section. This is about knowing and trusting who the other actors in the TF are. These are tech solutions, so the how to do this should not be in the trust framework. You might want to say, in a separate section, that a Trust Registry is required. This should be left to schemes to be implement.
5.1 Making your products and services interoperable with others	Each organisation or scheme will need to provide enough information for another to be able to: identify the person decide if the person or business is eligible for something		M	"identify the person" - How does this fit with providing attributes, such as age, without being able to identify who the actual person is? The IdSP can identify the person but just provides their age to the RP, the RP can trust the IdSP will do this correctly without the RP having to know the ID of the person. That should be a feature of the trust framework.
5.1 Making your products and services interoperable with others	How digital identities and attributes will be shared.		M	Example attributes should not be in the framework. They are not exhaustive and are already confusing those wishing to use and be part of the framework.

5.2 Check if a user can act on behalf of someone else	Check if a user can act on behalf of someone else	Too little	M	This section is too high level for what is a very complex area
5.2 Check if a user can act on behalf of someone else	this is known as 'delegated authority'.		M	Delegated Authority implications run through the whole document of this, and other, sections. Same as Vouching.
5.2 Check if a user can act on behalf of someone else	The details of their agreement with the other person might exist as an attribute.		L	On the delegatees or delegators ID?
5.3 Respond to complaints and disputes	You must have a process for dealing with complaints and disputes.	Too little	M	There should be a minimum complaint and disputes process. This is necessary for the credibility of the framework. The framework (governance body) would be, or would have the use of, an ultimate ombudsman for ID matters. Would also expect that Schemes must be aligned to any dispute requirements for their sector. It is necessary to separate Service disputes from ID disputes. Also within ID Disputes specifically, Fraud disputes should be handled separately.
5.4 Staff and resources	Staff and resources	Too much	M	This is not required to be stated separately as it will be in security ISMS required in section 5.7
5.5 Encryption	Encryption	To little	M	Need to define a list of acceptable techniques. These should have expiry dates to move suppliers on to more applicable standards, rather than just stating the latest versions must be followed. There should also be an emergency deprecation process when an accepted standard is breached.
5.5 Encryption	Encryption		M	Should framework state when to sign and when to encrypt? For example, data should be encrypted when in transit and at rest.
5.5 Encryption	Encryption		M	Should call out level of encryption required: 128bit, 256bit etc.

5.5 Encryption	Encryption		M	Are different encryption standards applicable for differently levels of assurance, or is it one size fits all i.e.. the highest bar?
5.5 Encryption	Encryption		M	How do self-sovereign architectures fit in here? There are different flavours of encryption in this space. Which ones are acceptable? A recent paper on SSI ID Encryption Flavours explored this topic: https://identitywoman.net/the-flavors-of-verifiable-credentials/
5.5 Encryption	Encryption		M	How will risk tolerance from a Cyber Security viewpoint be address within the framework (broader that just encryption).
5.6 Quality management	Quality management	Too Much	M	A list of supported standards should be published, rather than giving an example. All other detail needed in this section should be removed at this should be in every standard supported.
5.7 Information management	Information Management	Too Much	M	Similarly, to previous sections, this section should state that what type of standard must be complied with and give a supported list. The rest of requirements listed in this section, Archiving and Disposal, would be part of each supported standard and therefore do not need to be detailed in the Framework.
5.7 Information management	Information Management	Too Much	M	Why is this separate from Information Security? These could be one section.
5.8 Information security	Information Security	Too Much	M	Similarly, to previous sections, this section should state that what type of standard must be complied with and give a supported list. The rest of requirements listed in this section, from Confidentially to User Security Measures…, would be part of each supported standard and therefore do not need to be detailed in the Framework.
5.9 Risk management	Risk Management	Too Much	M	Similarly, to previous sections, this section should state that what type of standard must be complied with and give a supported list.

				The rest of requirements listed in this section would be part of each supported standard and therefore do not need to be detailed in the Framework.
5.9 Risk management	Risk Management - **You must follow the latest version of the standards.**		L	This comment on keeping up to date with prevailing versions of standards should also apply to other section that refers to standards.
5.10 Fraud management	Fraud Management	.	M	The list of best practise guidance is government centric. A reference to the Association of Certified Fraud Examiners (ACFE) might be appropriate
5.10 Fraud management	Fraud monitoring. You must have a way to regularly monitor threats and fraud. This must be assessed during internal audits, fraud audits and exceptional audits conducted by an independent internal auditor or a third party.	Too Little	M	This is very non-prescriptive. Is the detail of this intended to be left to Schemes? Consistent Fraud Controls implemented by all IdSPs at an appropriate level for each use case is really important for interoperability. The upcoming OIX Fraud Controls Guide can provide more detail in this area.
5.11 Respond to incidents	Taking part in an investigation	Just Right	M	When providing information for investigations how does this fit with the Investigation Powers Act 2018?
5.13 Privacy and data protection requirements	Privacy and data protection requirements	Too Much	M	This section reiterates key points to GDPR. Repeating these here is not necessary. Simply state GDPR compliance is a requirement. In trying to summarise GDPR requirements this section the summary has got the Data Protection law wrong. It says agreement must be obtained before making changes, but this is incorrect.
5.15 Things you must not do as part of the trust framework ('prohibited conduct')	Things you must not do as part of the trust framework ('prohibited conduct')	Just Right	L	Does this create responsibility/liability to relying parties who use ID from the Trust Framework? i.e. because accredited to a framework, need to pass on obligations in T&Cs to anyone you are doing business with.