OIX GUIDE TO PRINCIPLES IMPLEMENTATION

February 2021

Version 1.1

Authors: ID Crowd

TABLE OF CONTENTS

1. OIX USER CENTRIC PRINCIPLES FOR TRUST FRAMEWORKS

Principles should be accessible for end users, written in plain English and where possible not use jargon.

In the first iteration of the principles, created by previous OIX working groups, it was unclear whether ID referred to an identity, a credential or both. In this latest iteration, the word ID has been replaced with digital identity. The OIX glossary defines this as: A Digital Identity allows a user to provide trust in their identity to any organization.

The latest user centric principles to reflect this wording change along with some minor amendments to ensure that the guidance is not too prescriptive.

They have also been extended ensure inclusivity for users.

CONVENIENCE
A digital identity I set up can be used in lots of different places – I don't need different digital identities to access different kinds of services, unless I choose to do so
I need to know where I can use my digital identity
I need to understand why I am sometimes asked for further evidence to prove my identity
CHOICE
I can choose who manages my digital identity for me and change this at any time
I can have more than one digital identity
My digital identities are free.
I can create a digital identity directly for myself, or find assistance to help me create and manage it
I can choose an alternative to a digital identity, if I am unable or unwilling
CONTROL
It's my digital identity and data.
I need to agree who my data is shared with
I can see a record of this, and request for it to be returned and removed if I want.
I can change my data at any time and choose who is informed of that change.
My data will only be used in ways that I have agreed to, at the point of need
CONFIDENCE
I need to know my digital identity and data is protected from fraud and those who might use it illegitimately.
If something goes wrong, I need to know how I can seek help, support or independent redress from a trusted governance body
If I choose to, I can create a digital identity, whoever I am, whatever my background.

2. CONSIDERATIONS FOR ECOSYSTEM PARTICIPANTS

To help those creating and using trust frameworks ensure the principles are embedded in a trust framework implementation, the following tables have been created that highlight what each role in the ecosystem must do to ensure each principle is adopted.

The role of the Trustmark in communicating principles to users his also highlighted.

2.1 Convenience

Principle	Relying Party (RP)	Trustmark (on behalf of framework or scheme)	Broker	Identity provider (IdP)	Evidence Verifier
CONVENIENCE					
A digital identity I set up can be used in lots of different places – I don't need different digital identities to access different kinds of services, unless I choose to do so	An RP could display one or more Trustmarks so users know their digital identity will be accepted	Trustmarks provide details of how to find more information about a scheme - it's purpose, participants and services; how to get help, assistance and support and how to seek redress	Trustmarks are displayed so users know their digital identity will be accepted List available services based on any RPs, participating in a scheme, the broker has contracts with	Trustmarks are displayed so users know they can create a digital identity List available services based on any RPs, participating in a scheme, the IdP has contracts with	Trustmarks are displayed so the user knows that an organisation is participating in a scheme and can verify evidence Any evidence presented will be checked with authoritative sources such as issuing bodies
I need to know where I can use my digital identity	One or more Trustmarks are required in order to confirm that the RP is part of specific digital identity schemes and will accept the digital identity	Could list RPs and available services that are part of specific schemes Provide guidance for users if they want to access services that their current digital identity does not cover.	Could list RPs and available services that are part of specific schemes Provide guidance for users if they want to access services that their current digital identity does not cover.	List sectors, RPs and services the digital identity can be used with This should include any relevant Trustmarks.	Trustmarks could be shown to indicate participation in a scheme.

I need to understand why I am sometimes asked for further evidence to prove my identity	If a service requires a higher level of assurance, than the user currently has, it will be necessary for a user to provide additional evidence that will need to be validated and bound to the individual in order for the user to access the service Explain why some services might need greater confidence in a user Provide help and assistance through the process	If a service requires a higher level of assurance, than the user currently has, it will be necessary for a user to provide additional evidence that will need to be validated and bound to the individual in order for the user to access the service Explain why some services might need greater confidence in a user Provide help and assistance through the process	If a service requires a higher level of assurance, than the user currently has, it will be necessary for a user to provide additional evidence that will need to be validated and bound to the individual in order for the user to access the service Explain why some services might need greater confidence in a user Provide help and assistance through the process	If a service requires a higher level of assurance, than the user currently has, it will be necessary for a user to provide additional evidence that will need to be validated and bound to the individual in order for the user to access the service Explain why some services might need greater confidence in a user Provide help and assistance through the process	Should explain why data is processed and how the user's data and privacy is protected.

2.2 Choice

Principle	Relying Party (RP)	Trustmark (on behalf of framework or scheme)	Broker	Identity provider (IdP)	Evidence Verifier
CHOICE					
I can choose who manages my digital identity for me and change this at any time	RP should show which IdPs are preferred / accepted for new registration when a user wants to change.	Lists the different digital identity providers. Should also include summary information of the services offered.	Shows who the alternative digital identity providers are. Should allow users to transfer data (and potentially attributes) from one IdP another, subject to digital identity proofing. This may be an automated process or may require re-registration depending on the scheme rules.	If the scheme supports it, a user may be able to request transfer of some digital identity Information but not transfer of digital identity itself. Equally, users should be able to close an IDP account at any time and request removal of their data as necessary.	N/A
I can have more than one digital identity	RP should ensure that users are able to use multiple digital identities without a noticeable change in user experience or access to services.	Explains that users can have more than one digital identity, if there are any additional costs, and why they might consider having more than one digital identity.	The broker should not be affected by the choice of digital identity or if the user has multiple digital identities.	Users should be able to request their digital identity is removed at any time	N/A
My digital identities are free.	The commercial model of the scheme will determine whether there is an end user cost for a digital identity. In the public sector these are likely to be free An RP could choose to subsidise the cost of a digital identity or provide another means of incentivising the user to create a digital identity	The commercial model of the scheme will determine whether there is an end user cost for a digital identity. In the public sector these are likely to be free.	Digital identities may be free but brokers may also provide access to other attribute data that could have a commercial model different to that of identity. The commercial model of the scheme should consider such possibilities.	The commercial model of the scheme will determine whether there is an end user cost for a digital identity. In the public sector these are likely to be free	N/A

I can create a digital identity directly for myself, or find assistance to help me create and manage it	The RP should clearly signpost the user to either further information provided by the framework (Trustmark) or to the range of IDPs the RP accepts. Ideally a brief explanation of why digital identity is required and how it can be easily obtained should be available to the user.	Provide information about why digital identities are necessary, how they can be used and how a user can obtain one The scheme may permit different methods for identity proofing and verification. e.g. How to accept a vouch as evidence of someone's identity (https://www.gov.uk/government/publications/how-to-accept-a-vouch-as-evidence-of-someones-identity) .Explains how to create an ID and how to get assistance if the user requires this.	Provide information about why digital identities are necessary, how they can be used and how a user can obtain one Implements the trust scheme requirements to enable users to select assistance if required.	Provide clear instructions and guidance on how to create a digital identity are necessary, how they can be used and how a user can obtain one Implements the trust scheme requirements to enable users to select assistance if required.	N/A
I can choose an alternative to a digital identity, if I am unable or unwilling	RPs are likely to be the first point of contact for users so must make it clear what the alternatives to digital identity there are and how they can be accessed. If there are restrictions on use (or access) as a result this should be stated without infringing on the rights of the individual.	Should highlight the capability of RPs with respect to alternative methods of identification and if there are any restrictions on use as this may affect the choices made by users. Equally if IDPs are able to offer alternative means of verification or authentication more acceptable to the user (e.g. in person verification) then these should also be highlighted to the user.	The broker should not be affected by the user deciding to use an alternative to digital identity.	IDPs may wish to provide alternative methods of verification to users or to provide assistance to users unable to complete the normal process for registration of a digital identity. This may go beyond the norm for IDP services in the ecosystem. IDPs should explain before registration starts exactly what is required of users and provide reassurance that their data will be protected and where multiple routes to verification are available describe what these options are (e.g. alternative forms of evidence).	N/A

2.3 Control

Principle	Relying Party (RP)	Trustmark (on behalf of framework or scheme)	Broker	Identity provider (IdP)	Evidence Verifier
CONTROL					
It's my digital identity and data.	The RP should provide an explanation of how the users identity data will be used when accessing the service and how their rights are protected.	Explain how the users identity data will be used when accessing a service and how their rights are protected.	Explain how the users identity data will be used when accessing a service and how their rights are protected.	Explain how the users identity data will be used when accessing a service and how their rights are protected.	Explains that a users PII belongs to them, but that any evidence belongs to the issuer
I need to agree who my data is shared with	RP must explain clearly what data is needed and for what purpose so the user can provide informed consent Audit requirements to record data and purpose and gather informed consent from a user RP may have time limited use of data (per open banking 90-day rule) but user must be informed.	Should explain how and why data is shared within the scheme or framework and who is responsible for data storage and processing. Should make it clear to the user where agreements are required and how (and with who) the user may view or amend existing agreements.	Audit Trail of which IdP shared data with whom, but not the detail. Should provide a statement of how data is shared via the broker and an assurance that no user data is retained or shared with other parties outside the ecosystem by the broker. My also provide the user with audit facilities showing who has asked for data, when, and how it passed through the broker to another ecosystem party.	Gathers and records consent to share with RPs and Evidence Verifiers. IDPs should make it clear prior to registration what data will be processed and what data will be retained by the IDP. Alongside this the user should be made aware of who data may be shared with and where consent will be required and control afforded to the user. Users should have the opportunity to review and amend consent at any time following a successful registration. This should be made clear to users before they complete the registration process.	Should make clear to users how data is processed and what will be shared with the IDP (or other requesting parties) following an evidence verification (either positive or negative in nature). Depending on the service provided, users may be able to control what is shared with the requesting party e.g. a simple confirmation (Y/N) or perhaps more detailed information such as an identifier or data value (e.g. profession, age, nationality).

I can see a record of this, and request for it to be returned and removed if I want.	Removes user data on request, informing the user of the consequences of doing so. Minimal audit data will be retained	Should explain how the rights of users are supported such as requesting the removal of data. This should be accompanied by an explanation of the consequences of these actions and how it will affect access to services (or not). There should be the ability for a user to report errors, or potential fraud based on the records they are able to view. It may be that the scheme manages this on behalf of the ecosystem as users may not understand where an issue has occurred.	Should provide an audit trail for users showing how data has been requested and delivered via the broker to other ecosystem parties. Brokers may provide a mechanism for altering other ecosystem parties to the need for removal of data (if requested by the user).	Shows historic RP consents and allows user to request removal. IdP sends a request to the RP to remove data? OR IdP presents the user a link to the RP site where the RP tells the user how to delete their account.	Should provide an audit trail of previous requests for verification of evidence. Users should also be able to report potential errors or erroneous results provided by the evidence verifier either as a complaint or as an update to their information. The evidence has a responsibility to the user in this respect as well as to the ecosystem.
I can change my data at any time and choose who is informed of that change.	RP must subscribe to accept change of data and update their records accordingly. RPs must make it clear that users wanting to change their data must do so with their IDP as part of their identity account. Signposting should be provided to help the user complete this task.	The scheme should explain how a user can update personal information about themselves and how a user notifies scheme participants of this change	Brokers should not hold personal data so should be unaffected by changes to data elsewhere. Information should be provided to users or signposting provided if they wish to make such changes.	Allows user to change and choose who to alert, from ss list of RPs who subscribe to this service.	The EV will confirm changes asserted by a user
My data will only be used in ways that I have agreed to, at the point of need	Prohibited from selling data. The RP should make it clear what data is required to access the service and if any data is subsequently required to complete transactions requested by the user.	The scheme should make clear the need for any data required by a user to access an RP service will be clearly explained	Brokers should enforce the rules of the scheme/framework but should also make it clear to users that their data will not be used for additional purposes without user consent.	Gathers permission if relevant. The IDP should make it clear that only necessary and relevant data about the user will be shared and only with user consent. data minimisation to reflect that only relevant, necessary data should be shared when	The EV should record consent as well as a history of transactions for later review by the user or other authorised parties.

				needed to adhere with privacy laws and ensure that it is not out date when it is used	

2.4 Confidence

Principle	Relying Party (RP)	Trustmark (on behalf of framework or scheme)	Broker	Identity provider (IdP)	Evidence Verifier
CONFIDENCE					
I need to know my digital identity and data is protected from ID fraud and those who might use it illegitimately.	Put operational controls in place to monitor system usage, security controls to protect data and mitigate against risks and threats Implements Fraud Controls	Should explain how the ecosystem provides protection from fraud or misuse and who is responsible for data and processing. Users should be provided with a means of reporting potential fraud or misuse either centrally (at the scheme/framework level) or with individual ecosystem parties.	Should implements fraud controls and make it clear to users what those controls are and how they ensure the protection of the users and their data. The ability to report fraud or misuse should be provided (even if signposted to a central service) and signposting to a means of redress or support where applicable.	Should implement fraud controls and make it clear to users what those controls are and how they ensure the protection of the users and their data. The ability to report fraud or misuse should be provided (even if signposted to a central service) and signposting to a means of redress or support where applicable.	Should implement fraud controls and make it clear to users what those controls are and how they ensure the protection of the users and their data.
If something goes wrong, I need to know how I can seek help, support or independent redress	Provide clear information on how to get help, assistance or support Provides details on how to make and escalate complaints and to seek redress with an independent body	Provide clear information on how to get help, assistance or support Provides details on how to make and escalate complaints and to seek redress with an independent body	Provide clear information on how to get help, assistance or support Provides details on how to make and escalate complaints and to seek redress with an independent body	Provide clear information on how to get help, assistance or support Provides details on how to make and escalate complaints and to seek redress with an independent body	Provide clear information on how to get help, assistance or support Provides details on how to make and escalate complaints and to seek redress with an independent body
If I choose to, I can create a digital identity, whoever I am, whatever my background.	Only engages with Schemes, Brokers and IdPs that meet their inclusion needs.	Informs the user about inclusion aims and options supported by the scheme.	Implements inclusion rules and targets set by the scheme.	Implements inclusion rules and targets set by the scheme. Might have to implement a rolling inclusion improvement plan to make sure more and	Provide access to diverse data and alternative proofing techniques (such as issue of letters with QR codes) to ensure

				more users are included over time.	inclusion across the ID Ecosystem is maximised.