OIX – PRINCIPAL PRINCIPLES

February 2021

Version 1.1

Authors: ID Crowd

TABLE OF CONTENTS

1. SUMMARY

A guiding set of basic principles is imperative to ensure an inclusive approach to the development of policy, technical frameworks and systems for identity. These principles should be user centric, allowing individuals to control and consent when to reveal their own identifying information. Only with this focus will it be possible to create compelling identity enabled ecosystems that will be both trustworthy for and attractive to citizens and consumers alike.

This paper explores some existing international work on principles for identification to identify common themes, considers work from previous OIX working groups and recommends a revised set of basic principles.

2. PRINCIPAL PRINCIPLES

A clear set of basic principles, agreed and enforced by all stakeholders, must underpin an identity trust framework in order to maximise the benefits, minimise any risks and ensure effective and available access to all end-users.

While the principal principle must be to adapt and build on existing work, rather than try to reinvent or embellish what in its very nature should be inclusive, transparent and open, all principles should recognise that they must adapt over time to reflect new stakeholders, emerging technology and lessons learned in the real world.

With this in mind, probably the second most important principle, that underpins the World Bank's Identity for development (ID4D) principles on identification for sustainability, is the mantra: *No one should be left behind.*

This means both providers (government and the private sector) and individuals must align on a set of common principles to ensure inclusivity for all. While inclusion remains a challenge in the developing world inclusion is rapidly becoming a pressing issue everywhere, not least due to the Covid-19 pandemic which is kick-starting an acceleration of digital transformation globally.

Without the opportunity to meet in-person or perform face to face transactions there is increased demand for remote identity proofing and digital means to both access services and make them available. This is no less evident in the UK, one of the world's advanced economies, where 1.4 million self-employed people had no prior digital identity credentials required to use HMRC's identity verification service and make a claim for benefits.

That said, while putting the individual front and centre, principles should cover all aspects of delivering an identity assurance ecosystem. But also recognise that while principles are generally universal, the principles for a specific identity trust framework must be fit for the purpose intended and should be applied appropriately. For example, while international or sector specific interoperability must be a clear aspiration it is important to ensure that a specific identity trust framework works for the actual stakeholders involved first.

The wording of all principles must be carefully chosen, discussed and agreed with all stakeholder groups, and reviewed over time to cater for inevitable change. And principles should be drafted to allow for some flexibility rather than be too prescriptive, while it must also be noted that there may also be special interests (e.g. law enforcement) that might need exemptions.

3. EXISTING INTERNATIONAL WORK ON PRINCIPLES

Following our principal principles, we examine some of the international initiatives that have created principles for identity as we look to establish a common set of principles that build on existing work.

3.1 Principles on identification (ID4D, World Bank)

The Identity for development programme (ID4D) focus is often on creating foundational identification systems for the developing world, to meet the United Nations sustainable development goals. However, as these principles have been designed for all, building on existing international work and lessons learned from real-world implementations, the same principles apply everywhere.

ID4D has identified ten core principles that have been categorised into three main groups (see figure 1).

Figure 1: World Bank's ID4D - Principles on Identification for Sustainable Development

The key themes from these principles can be loosely summarised as follows:

- inclusivity - everyone has a right to participate fully in their society and economy
- design - systems must be robust, accurate, secure, accessible, interoperable, sustainable, adopting open standards whilst enabling user privacy and control
- governance - ensuring support, accountability and oversight

ID4D recognises that these principles will need to be adapted over time to include other stakeholders, technologies and further lessons learned.

3.2 Identity Assurance principles (PCAG, UK)

The Privacy and Consumer Advisory Group (PCAG) was established to provide independent review, analysis, guidance and feedback on UK Government initiatives relating to the use of individuals' personal data and their privacy.

In this capacity PCAG created a set of nine identity assurance principles to advise on how the UK government should provide users with a simple, trusted and secure means of accessing public services whilst ensuring user consent and maintaining user privacy.

Identity Assurance Principle	Summary of the control afforded to an individual
1. User Control	Identity assurance activities can only take place if I consent or approve them
2. Transparency	Identity assurance can only take place in ways I understand and when I am fully informed
3. Multiplicity	I can use and choose as many different identifiers or identity providers as I want to
4. Data Minimisation	My request or transaction only uses the minimum data that is necessary to meet my needs
5. Data Quality	I choose when to update my records
6. Service-User Access and Portability	I have to be provided with copies of all of my data on request; I can move/remove my data whenever I want
7. Governance/Certification	I can have confidence in any Identity Assurance System because all the participants have to be accredited
8. Problem Resolution	If there is a problem I know there is an independent arbiter who can find a solution
9. Exceptional Circumstances	Any exception has to be approved by Parliament and is subject to independent scrutiny

Figure 2: PCAG's Identity Assurance Principles

The key themes from these principles are about user control focusing on privacy and consent:

- processes can only occur with informed consent, relevant and necessary data
- choice of how an individual chooses to transact
- ability to request copies of personal data and the right to be forgotten
- evidence that systems and stakeholders have been through robust processes to participate
- ability to seek, help support and redress

3.3 Principles for digital identity (Digital Identity Strategy Board, UK)

The UK Government's digital identity strategy is being driven by DCMS and GDS via a new government Digital Identity Strategy Board that has developed six principles to inform how the government develops policy and law to enable secure digital identities and safeguard citizens.

1. **Privacy** – When personal data is accessed citizens will have confidence that there are measures in place to ensure their confidentiality and privacy. Where possible, citizens select what personal data is shared. Organisations will have privacy standards to uphold and will need to prove their ongoing compliance.
2. **Transparency** – Citizens must be able to understand by who, why and when their identity data is used [when using digital identity products].
3. **Inclusivity** – This means those who want or need a digital identity should be able to obtain one. We will look at how citizens could use different attributes (e.g. name, date of birth etc.) held across government and by other parties to support identity proofing.
4. **Interoperability** – Setting technical and operating standards for use across the UK's economy to enable international and domestic interoperability.
5. **Proportionality** – User needs and other considerations such as privacy and security will be balanced so digital identity can be used with confidence across the economy.
6. **Good governance** – Digital identity standards will be linked to government policy and law. Any future regulation will be clear, coherent and align with the government's wider strategic approach to digital regulation.

Figure 3: Digital Identity Strategy Board's principles for digital identity

The key themes from these new principles are similar to those developed by PCAG, however seem to omit the need for independent oversight, certification, assurance and audit or the ability to seek, help, support or redress.

3.4 Guiding principles for the Pan Canadian Trust Framework (PCTF)

The Digital ID & Authentication Council of Canada (DIACC) is committed to developing a Canadian framework for digital identification and authentication. DIACC is a non-profit coalition of public and private sector organisations that aim to enable Canadians to completely and securely participate in the global digital economy by establishing a robust, secure, scalable, inclusive and privacy-enhancing digital ecosystem. DIACC's PCTF is based on a set of guiding principles.

2.5 Guiding Principles

The PCTF achieves its goals and objectives in part through standards and guidelines that reflect the following guiding principles:

1. **Support robust, secure, scalable solutions** – Canada's digital identity ecosystem must be sufficiently robust to ensure security, availability, and accessibility at all times.
2. **Implement, protect, and enhance privacy by design** – Privacy enhancing tools enable an individual to manage their information and what specified purpose(s) it is used for. These tools may include support for a user's "right to be forgotten" (when appropriate in the legislative context of the trust framework participant).
3. **Be inclusive, open, and meet broad stakeholder needs** – Digital identity ecosystem services and tools must be affordable, standardized, and create value for users in the interest of broad adoption and benefit to all Canadians.
4. **Be transparent in governance and operation** – Canadians need to trust that services offered in the Canadian digital identity ecosystem will respect and meet their needs and expectations.
5. **Provide Canadians choice, control, and convenience** – Services are based on the principle that individuals can choose what information to share, what services to use and from which countries, and are informed about the potential benefits and consequences of digital identities.
6. **Build on open standards-based protocols** – Use of open standards and applicable best practices for Canada's digital identity ecosystem helps protect against obsolescence, ensure interoperability, and foster a dynamic and competitive solutions marketplace.
7. **Maintain international interoperability** – Interoperability and global technology and policy standardizations are foundational to todays connected world. Much like standardized railway gauges enable travel and the movement of goods across countries, technology and policy interoperability and standardization allows digital services to communicate and lower costs while increasing innovation opportunities.
8. **Be cost effective and open to competitive forces** – It is essential that the digital identity ecosystem respects the budgetary constraints of the present and the future. Ensuring the ecosystem is open to competition, representing multiple economic sectors, each playing different roles, will lead to decreased costs for all stakeholders and increased innovation.
9. **Support independent assessment, audit, and enforcement** – For Canadians to trust a digital identity ecosystem, governing controls must be put in place. On-going, functionally independent, and third-party assessments provide one way to ensure that ecosystem stakeholders adhere to the trust framework requirements.
10. **Minimize data transfer between sources and avoid creation of new identity information repositories** – Users of digital identity ecosystem services should be asked to provide only the minimum amount of personal information needed in a given interaction.

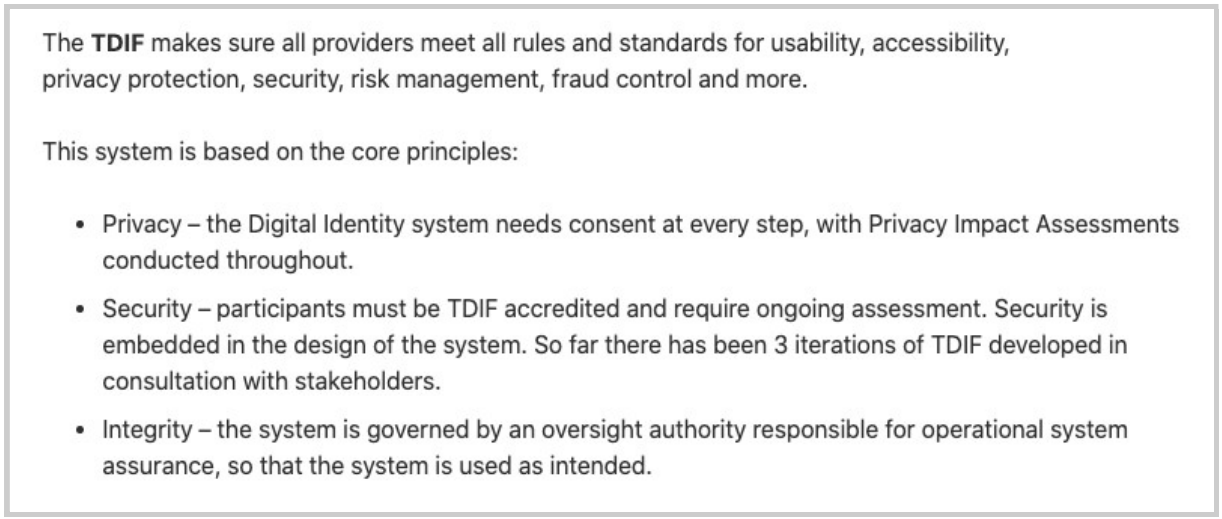
Figure 4: PCTF's guiding principles for digital identity

The focus is to create a nationwide identity ecosystem for the individual:

- Inclusivity with individual choice, control and convenience
- Privacy by design minimising data
- Transparent and auditable
- International interoperability facilitated through open standards
- Robust, secure, and scalable systems that are cost-effective and competitive

3.5 Principles for the Trusted Digital Identity Framework (TDIF)

The Australian Government Digital Transformation Agency (DTA) has taken an innovative and transparent approach to identity by developing and publishing it's Trusted Digital Identity Framework (TDIF) with all the information for new entrants to onboard in their own time.


The **TDIF** makes sure all providers meet all rules and standards for usability, accessibility, privacy protection, security, risk management, fraud control and more.

This system is based on the core principles:

- Privacy – the Digital Identity system needs consent at every step, with Privacy Impact Assessments conducted throughout.
- Security – participants must be TDIF accredited and require ongoing assessment. Security is embedded in the design of the system. So far there has been 3 iterations of TDIF developed in consultation with stakeholders.
- Integrity – the system is governed by an oversight authority responsible for operational system assurance, so that the system is used as intended.

Figure 5: TDIF's principles for digital identity

The TDIF defines requirements for the proper operation; roles and operating responsibilities of the participants which are based on core principles covering these key themes:

- privacy and consent
- security - all participants must undergo ongoing assurance
- integrity - oversight to ensure the system can be used as intended

3.6 Common themes

Not unsurprisingly there are common themes across and throughout the principles we have explored:

- Inclusion for all covering accessibility, usability and availability
- User centric ensuring privacy and facilitating informed consent
- Robust, secure, scalable ensuring end to end integrity while mitigating risks and threats
- Transparent governance with independent oversight, audit, certification /assurance
- Ability to seek help, support and redress

4. CONSIDERATIONS

The OIX principles need to cover all the common themes identified and provide guidance without being too prescriptive. Individual trust frameworks or schemes will include detailed requirements on how guidance will be delivered.

As we have seen some existing identity implementations have put forward groupings of principles to aid with understanding but in essence the objective should be to ensure that any principles proposed cover all aspects of identity assurance. So, while it may appear convenient to group principles across a number of categories, this must not be at the expense of the principles themselves.

While a digital first approach is highly likely to be the aspiration, especially given the challenges accelerated and amplified by the Covid-19 pandemic, we must also be mindful of the ID4D mantra: No one must be left behind. Principles should also consider non-digital channels and must clearly distinguish between intent and implementation. For example, the proofing process to identify an individual to a level of assurance is one part of a digital identity and the credential and authenticators are another. Only together can an individual actively make use of their digital identity. We must be careful not to conflate the two. For this reason, we have recommended that we replace the use of ID with identity or digital identity as appropriate.

Using the common themes let's consider why and which principles are essential.

User Principle	User Principle Element	Who?
CONVENIENCE	An ID I set up can be used in lots of different places – I don't need different IDs to access different kinds of services, unless I choose to do so	Bkr, IdP, Sch, Fwk
	I need to know where I can and cannot use my ID.	Bkr, IdP, Sch, Fwk
	I need to understand why I am sometimes asked for further verification of my ID.	IdP
CHOICE	I can choose who manages my ID for me and change this at any time.	Bkr, Sch, Fwk
	I can have more than one ID.	Bkr, IdP, Sch, Fwk
	My IDs are free.	Sch, Fwk
CONTROL	It's my ID and data.	Bkr, IdP, Sch, Fwk
	I need to agree who my data is shared with.	IdP
	I can see a record of this, and request for it to be returned and removed if I want.	Bkr, IdP, RP
	I can change my data at any time and choose who is informed of that change.	IdP, Bkr, RP
	My data will only be used in ways that I have agreed to	IdP, RP
CONFIDENCE	I need to know my ID and data is safe from ID fraud and those who might use it illegitimately.	Bkr, IdP, Sch, Fwk
	If something goes wrong, I need to know I will be OK, and the problem will be resolved.	Bkr, IdP, Sch, Fwk

Figure 6: OIX principles for digital identity

4.1 Inclusion for all covering accessibility, usability and availability

It is highly likely that, in the short and medium term, digital identities will be tied to individual trust frameworks or schemes. So, while it should be made as obvious as possible where a digital identity can be used there is no need to specify where it can't. The way individuals are informed will be down to the organisations operating the scheme or trust framework. Principles should be more broad and less specific.

As per the World Bank's first principle on inclusion - everyone has a right to participate fully in their society and economy. However, this may well be through various means and may require specific digital identities for different purposes. For example, the public sector may offer low cost means to access public services including benefits. While this may even be free access in some instances there is a general acceptance that government issued documents such as passports and driving licences may incur a costs especially if they include more secure ways of identification or protection. And in the private sector, as we see today with many freemium services, the provision of a "free" digital identity or credential may well be in return for targeted advertising or some similar means for a commercial entity to recoup their costs.

The means of participation must also consider what available access or how different demographic groups choose to access different services. Usability, access to technology must be considered across all stakeholder groups.

4.2 User centric ensuring privacy and facilitating informed consent

Consumers of identity (relying parties) will have established risk profiles that will require levels of confidence and certainty in an individual which will vary depending on the organisation. And providers of identity may choose to only cater for specific demographic groups. But all participants must ensure that individual's personal information is kept private and that the intended purpose and processing is clearly articulated before consent for use is requested from an individual. Data minimisation must be at the heart of all transactions to ensure data processing and privacy laws are upheld but this will be specific again to each trust framework or scheme.

User control is an interesting concept that should be considered. While your identity - the biographical, biometric and even behavioural traits may well be yours, the credentials probably belong to the provider that issued them e.g. a passport belongs to the state. So, there is an implicit "right to use" but no ownership per se. So, data about you may well not be in your control for example the licence to drive is typically issued by a government organisation e.g. the DVLA following a series of competency tests and is a binary decision - a licence to drive is issued or not.

4.3 Robust, secure, scalable ensuring end to end integrity while mitigating risks and threats

Once an accurate identity has been established it must be robustly and securely protected for its lifetime. This means proactive protection from both existing and new risks and threats such as identity fraud. There must be considerations made to ensure that individuals understand that this protection is dynamic and starts from the initial proofing processes to

establish that an individual is who they claim to be, the ongoing use of any digital identity and across any and all transactions.

4.4 Transparent governance with independent oversight, audit, certification /assurance

The purpose for which any information is gathered and used must be clear to individuals including the ability to ask for copies of all data to be provided or removed as per the “right to be forgotten” as part of EU’s GDPR regulations.

4.5 Ability to seek help, support and redress

To ensure confidence it must be straightforward for individuals to get help or assistance when creating a digital identity, to get support if something goes wrong and to know how to seek redress from an independent arbiter when all other routes have failed to provide resolution.

5. RECOMMENDED REVISED OIX PRINCIPLES

- Principles should be accessible for end users, written in plain English and where possible not use jargon. In the current iteration of the principles, created by previous OIX WGs, it was unclear whether ID referred to an identity, a credential or both, It 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.
- We have revised the principles to reflect this wording change along with some minor amendments to ensure that the guidance is not too prescriptive.

Revised Principles
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.