DINZ Inclusive and Ethical Uses of Digital Identity (IEUDI) Working Group

Overview and plan – June 2023

Background

Working group purpose & objectives:

- Address the need for clarity about those New Zealanders who may be disadvantaged regarding benefitting from digital identity in a post-DISTF world. The need to understand the types of disadvantages, both digital and otherwise, that these New Zealanders either directly experience or perceive.
- Propose strategies and actions to address those challenges. For example, would there be merit in developing a voluntary "Code of Practice for Inclusive and Ethical uses of Digital Identity" centered on the DISTF design principles, as a supplement to the regulatory arrangements that will be put in place?

Initial research findings:

- New Zealand's DISTF Act 2023 is built on eight principles including inclusion. Ethical use of digital identity is only mentioned once.
- Internationally, frameworks for development of digital identity services do focus on inclusion but are also relatively silent on ethics.

Why is this important?

Digital identity is increasingly part of the very fabric of people's lives and is now an established priority for the New Zealand Government and industry, with a nascent ecosystem emerging. The Digital Identity Services Trust Framework (DISTF) Act 2023 is anticipated to provide an accessible and effective digital identity ecosystem that has the potential to unlock a range of opportunities across all parts of society. But can this potential be realised?

This question has clearly been considered in development of the DISTF, which has been based around the following eight principles:

- People-centred
- Inclusive
- Secure
- Privacy-enabling Enabling
- Te Ao Māori approaches to identity
- Sustainable
- Interoperable
- Open and transparent

These principles are of vital importance and welcome. However, as New Zealand's recent experience of digital solutions developed to respond to COVID-19 (e.g., the MoH's COVID Tracer, My Health Account (health digital ID) and COVID-19 Vaccination Certificate applications) illustrate, there remains a digital divide in NZ that, left unaddressed, will continue to preclude some New Zealanders from benefitting from digital identity.

And, as use of the COVID Vaccination Certificates demonstrates, some New Zealanders now have first-hand experience of digital identity enabling a mechanism that can deprive people of their legal rights and freedoms. This illustrates the potential for digital identity to open or exacerbate a "trust divide" that is contrary to the intent of the DISTF and should not be ignored. Unless participants in the identity ecosystem that the DISTF seeks to foster and regulate behave in inclusive and ethical ways, in line with the design principles of the DISTF, then its objectives may be frustrated, and New Zealanders may be harmed.

Defining terms

It is important to define ethics and inclusion for the purposes of this working group. The following is proposed:

- **Ethics**: the branch of philosophy that involves systematizing, defending, and recommending concepts of right and wrong behaviour. In the context of this working group, this translates to a focus on understanding 'right' and 'wrong' ways to develop digital identity systems and use digital identities in Aotearoa New Zealand.

  To stimulate thinking about this, ChatGPT states that ethics related to digital identity services "involves respecting privacy, being transparent, inclusive, and accountable, obtaining consent, ensuring accuracy, and using data responsibly while complying with relevant laws and regulations" (see annex).

- **Inclusion**: The government's Digital Inclusion Blueprint states that its vision for digital inclusion is "that all of us have what we need to participate in, contribute to, and benefit from the digital world". In its explanation of the principle of inclusion that informed design of the DISTF Act, the DIA states that that key measures of an inclusive digital identity system are:

  - The digital identity system can reflect the needs and requirements of a broad range of stakeholders.
  - Barriers to participation in the digital identity system, whether they be social, financial or technical, are minimised without compromising security or privacy.
  - Everyone is able to use digital identity services without risk of discrimination or exclusion.

Scope

The terms of reference for this working group specify that its scope of work is:

- To help ensure inclusive and ethical and responsible use of digital identity technologies to help ensure equitable digital identity outcomes for all New Zealanders.
- To build an understanding of the views and roles of relevant advocacy groups (for example but not limited to NZ Council for Civil Liberties) in the successful adoption of digital identity technologies.
- Providing constructive forums for discourse with groups that are either clearly disadvantaged in relation to digital identity or have concerns about the potential future uses of digital identity.

Deliverables

- A summary of working group views on what inclusive and ethical use of digital identity means in a New Zealand context.
- A draft paper covering an outline of a **Code of Practice** for both policy makers and digital identity service providers to consider when designing public facing digital identity services
- Draft recommendations to the DiNZ Executive Council on next steps, including investment required, stakeholder groups (agencies, private/public/NGO's) that would need to collaborate to achieve outcomes, measures and targets to drive action.

Working group composition

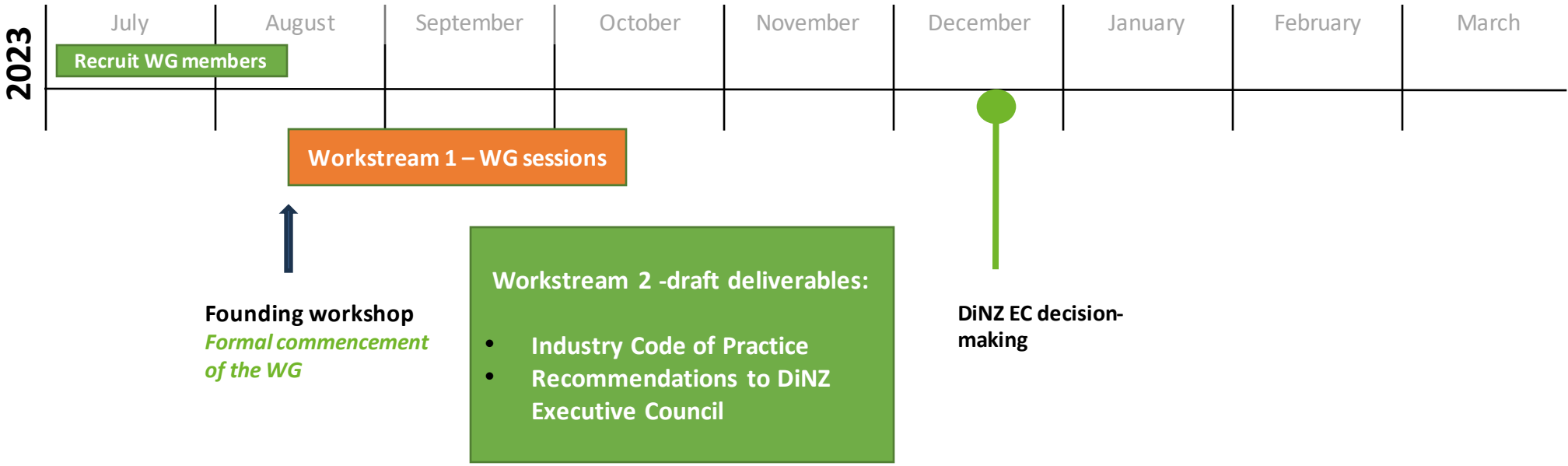
We need broad & diverse participation in the working group. Ideally, this will include specialists in digital ethics and inclusion (both government and non-government), DiNZ members, and representatives from the following "communities of interest":

- Iwi/Māori
- Pasifika
- Civil liberties & human rights
- Community advisory/advocacy groups (e.g. CAB)
- ????

From government, we would ideally have participation from:

- DIA – both those working on implementing the DISTF regulatory framework, and the Digital Public Service team focussed on digital inclusion.
- Stats NZ – representation from the Centre for Data Ethics and Innovation
- (MBIE - potential connection here to the team working on the Customer and Data Product Bill?)

IEUDI Working group timetable



Why participate in this WG?

- This is an opportunity to create meaningful long-term social impact for all New Zealanders.
- Play a part in doing the right thing for disadvantaged groups in Aotearoa.
- Help take the fear out of technology change.
- Be part of filling a significant vacuum and bring life to what ethical use of digital identity (as mentioned in the DISTF Act 2023) might mean in New Zealand.

Annex

ChatGPT on the ethics of digital identity:

“Ethics in the world of digital identity services refers to the principles and standards that guide the responsible and ethical use of personal information and the management of digital identities. It involves ensuring that individuals' privacy, security, and rights are respected throughout the entire lifecycle of their digital identities.

Here are some key aspects that define ethics in the realm of digital identity services:

Privacy: Respecting individuals' privacy rights by collecting, storing, and using personal information only for legitimate purposes and with explicit consent. Implementing robust security measures to protect personal data from unauthorized access or misuse.

Transparency: Providing clear and understandable information to individuals about how their digital identities are managed, including the purposes for which data is collected, how it is processed, and who has access to it. Being transparent about any potential risks or implications of using digital identity services.

Inclusivity: Ensuring that digital identity services are accessible and inclusive for all individuals, regardless of their demographic characteristics or technological capabilities. Avoiding discrimination and biases in the design and implementation of identity systems.

Consent and Control: Giving individuals control over their digital identities by providing mechanisms for them to give informed consent, manage their personal information, and control the sharing of their data with third parties. Allowing individuals to easily revoke consent and delete their personal data when desired.

Accuracy and Accountability: Striving for accuracy and integrity of personal information stored in digital identity systems, taking steps to correct any inaccuracies promptly. Holding organizations accountable for the responsible use and protection of digital identities and providing channels for individuals to address concerns or file complaints.

Ethical Use of Data: Ensuring that personal data collected for digital identity services is used only for the intended purposes and not exploited for unethical or harmful activities such as identity theft, surveillance, or profiling. Avoiding the aggregation and use of personal data for purposes beyond what individuals have consented to.

Legal Compliance: Adhering to relevant laws, regulations, and industry standards governing the collection, processing, and storage of personal data in the jurisdiction where the digital identity services are provided. Being proactive in adopting privacy and security best practices beyond mere legal compliance.

It's important for organizations providing digital identity services to prioritize ethics and adopt practices that safeguard individuals' privacy, security, and rights. This helps build trust, maintain user confidence, and ensure responsible and beneficial use of digital identity technologies in society.”