Perceptions and experiences of Verifiable Credentials in Aotearoa

Customer research report

Prepared by Catherine Neal, Service Designer DIA

May 2025

Contents

Background

The Department of Internal Affairs (DIA) is responsible for a range of identity products and services, including birth certificates, passports and RealMe Verified Identities. DIA are also responsible for holding the source identity records for all New Zealanders. DIA have been looking at the future of digital identity, 'Verifiable Credentials', since late 2020. Verifiable Credentials would mean a way for New Zealanders to prove their identity through a digital medium where they might otherwise be required to present a physical document.

A verifiable credential is a trustworthy package of data that contains information. It follows a standard data model, and is digitally signed by the agency that issues it to provide trust that it is accurate and security to prevent tampering. A user would be able to store it in the wallet of their choice and use or share that information as they see fit, and anyone needing them to prove information can trust the credential.

DIA would issue a user with one or more credentials that encompass their identity. These will likely be details such as name, date of birth, place of birth, and a verified photo. They may also be derived credentials such as "Over 18" instead of a birth date. The request for a credential will come from a wallet (or similar service) that is bound to them and can receive the credential from us. We would pass the user through some form of binding and confirmation before we issue the DIA-signed credentials. Signing a credential this way would be similar to how a passport's chip is digitally signed to enable border agencies to trust the data.

A 'Sandbox' environment has been open since **X** to allow interested parties to see how a Verifiable Credential might work for them on a technical level, with opportunities to also understand the social license and any other cultural implications of VCs, and the customer experience customer covering various parties (e.g. wallet providers, getting and using credentials).

As part of the Sandbox, there were two customer objectives to explore:

Objective 1: Understand the social license and any other cultural implications of verifiable credentials.

Objective 2: Understand the full end-to-end journey of a customer covering various parties (e.g. wallet providers, getting and using credentials).

Key findings

Overall, whether people use Verifiable Credentials, and how they use them, will depend on a range of factors including practical need, personal comfort with technology and online services, and how useful or applicable it is in their everyday lives.

We have identified potential opportunities and challenges including:

- Technology and digital services are evolving, and people are evolving with them. Doing things online or digitally is almost becoming an expectation, with people looking to it for ease and convenience.
- New Zealanders have generally high trust in government and there is increasing interest in controlling their own information. Though for some this trust has to be earnt or is more on a 'have to' basis, in order to access the services they need.
- Proving identity via Verifiable Credentials can make things easier and faster; through real-time information sharing, making more services available fully online, and having identity documents on hand on a mobile device, ready to go.
- Digital exclusion impacts a large portion of society, ranging from access, trust, motivation and digital capability. Accessibility issues and the cost of mobile devices, internet connection and obtaining a NZ passport could present barriers to those already left behind.
- With increases in scamming, use of AI and privacy breaches, people's behaviour is shifting. People are becoming more aware and sometimes more cautious of what they are doing in online and with technology.
- We need to keep in mind how easy and practical Verifiable Credentials are in reality, especially when there are other readily available identity documents which may be even easier to use when out and about. The usability and accessibility of the end to end experience is crucial, especially for those that need more support.
- There is potential for the current perceptions of the RealMe service to impact on uptake of Verifiable Credentials as people have mixed views and experiences.
- Piloting Verifiable Credentials with a group where there can be a number of applicable situations e.g. students may help increase uptake.

Approach

To understand how New Zealanders might accept, use and experience Verifiable Credentials a number of high level questions were created linked to the Sandbox customer objectives:

Objective 1:

- How do people prove who they are at the moment?
- What barriers do people face with proving identity and using technology?
- How do people feel about RealMe as a digital identity service?
- What helps to build trust?
- What can we learn from the rest of the world?

Objective 2:

- What are peoples initial thoughts and feelings from the video?
- How would people feel performing an identity check in public or scanning QR codes?
- Do people worry about what information is being shared and how do they feel about the proposed model?
- How would they prefer to provide consent?
- Of their current identity documents, and Verifiable Credentials, which do they think they would prefer or choose?

To start, a range of desk research was completed including published reports from Citizens Advice Bureau, Digital Identity Aotearoa, Digital.govt.nz, NZ Seniors, Te Puni Kōkiri, Research First, as well as previous internal research in the Verifiable Credential, in-person proof of identity and RealMe space. International cases of digital identity were also examined including Singpass (Singapore), mygovID (Australia) and the European Digital Wallet. This research helped to build a picture of the current landscape of digital identity, digital exclusion and other barriers people face when they need to prove who they are or interact with services.

A survey was run in conjunction with Mymahi sent to high school students who are signed up to the service across the country. 500 responses were received covering questions from both objectives. The full set of graphs and summarised free text responses can be found in Appendix 2 and 3.

A series of interviews and group discussions were also undertaken with members from Manawatū SeniorNet, Whaikaha (Ministry for Disabled People), representatives from Horowhenua Youth Council and 8 individuals from across Aotearoa. Each group was asked the same questions, as well as additional focused questions about particular community groups and their needs and experiences.

A full list of references can be found in Appendix 1 at the end of this report.

Our participants...

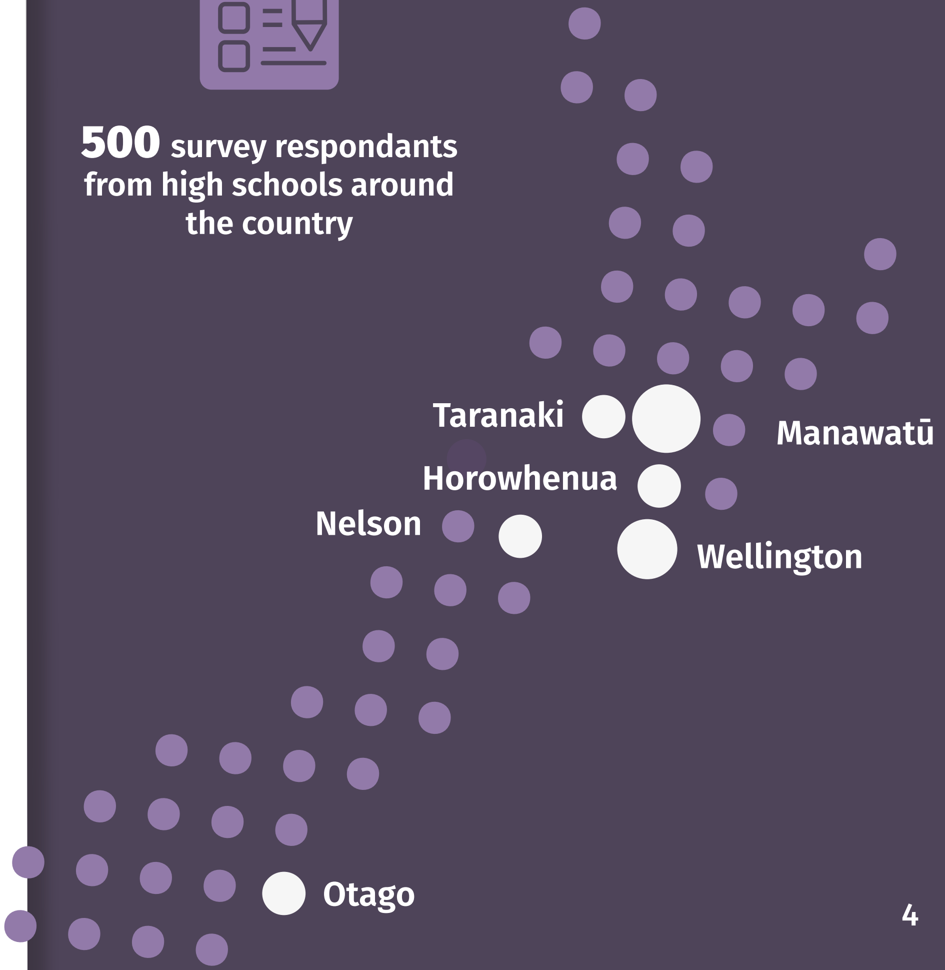
Low - High digital literacy

Med - High trust in government

Low - High online engagement

Aged **16 - 70+**

500 survey respondants from high schools around the country



Limitations

This research, while providing valuable insights into the potential social licence and experience of Verifiable Credentials does have some limitations that should be considered when interpreting the findings. This was an exploratory piece, covering a wide range of topics and does not consist of a full data-based research piece with interview feedback not representative of the whole country. These findings should be used to highlight some high level social and experience opportunities and challenges that could be explored and understood further.

Missed perspectives

During this research some particular focus was given to understanding the perspective of those left behind by digital exclusion. This is because these are the people that could be most impacted by shifts to digital or online services.

Some other key perspectives that were not able to be captured in this research include:

- Māori
- The practicalities of proving identity on behalf using Verifiable Credentials
- Where devices are shared within a home
- Front-line staff receiving the Verifiable Credentials

Engaging with receivers, especially staff on the front line such as cashiers at the supermarket, bottlestore or other public services will provide key insights into how these credentials will be absorbed, trusted and any behaviours it may drive. While there may be an understanding around how it works and the Trust Framework it sits within, the practical application may inhibit or reduce that trust especially if that trust is taken advantage of. With the reduced sharing of personal information, and potentially a simple 'Identity Verified' message, those receiving that verification in order to supply goods or services will need to trust that the person providing that identity is in fact the owner of it. Young people sharing phones or identity documents is a current state issue, and until the technology is used it is hard to know whether that behaviour will change and the flow on effects of that on trust and uptake by receivers.

Usability testing

As this was an exploratory research piece, we focused on high level insights. As we had a demonstration video of Verifiable Credentials in action, we had an understanding of the technology used through the process that we were able to research further both using reports or in our interviews, group sessions and survey. We were able to ask how people would find performing the identity check, scanning a QR code and using the app 'in theory'.

Further work should be done to test the Verifiable Credential app in various scenarios, with customers that have mixed digital capability and usability needs. Testing in different lighting situations, real-life scenarios with customers' own phones and data as well as common pressures or distractions and other factors will help to better understand how credentials will work 'in reality'. This will further build a picture around whether it is easier or more usable than current methods, which scenarios and use cases might be better to pilot with and what potential uptake and perceptions could be.

Objective 1: Understand the social license implications of verifiable credentials

The way we interact with both the digital and physical world, and take up new services or technologies is heavily influenced by our previous experiences, what others are doing and what is going on in the wider ecosystem. Understanding how people think about and interact with identity, digital services and technology today will help us to understand how they might accept and trust Verifiable Credentials in the future.

Like any new technology, whether people use Verifiable Credentials will depend on a range of factors including practical need, personal comfort with technology and online services, and how useful it is in their everyday lives. Young people and students are likely to lead early adoption, as they are they are needing to prove their identity for a range of services including banking, job seeking, university, benefits or loans and proof of age. Others, especially those who don't often need to prove their identity, may not see the value unless it clearly offers a faster, simpler and more accessible way to do things. And for those already facing barriers, such as digital exclusion or not having a NZ passport or other form of ID, Verifiable Credentials may not feel like a solution at all.

Trust in the digital environment and government services will also play a huge role, especially in an ever changing world with new emerging threats to identity security. Those who have experienced identity theft, scamming or data breaches may be less inclined to take up a new digital form of ID, similarly to those who may have had negative experiences with current digital identity products like Realme.

In this report, key insights from both existing research and customer interviews will help provide a snapshot of how people might view Verifiable Credentials and where more work needs to be done to understand the impacts on different facets of society.

90% of New Zealanders find the idea of being more in control of their digital identity appealing[1].

50% of New Zealanders have adapted their online behaviour due to concerns around data privacy [1].

DIA estimates **20%** of New Zealanders experience some form of digital exclusion[2].

64% of seniors prefer to wait until new technology is well established and mainstream before using it themselves[3].

Around **4.3 million** people in New Zealand hold a form of drivers licence[4].

More than **1.5 million** RealMe verified identities exist. RealMe is currently used by 44 agencies and provides access to 148 online services[5].

93% of students surveyed owned a smartphone that could download apps, **94%** owned a smartphone that could take selfies.

1 Digital Identity in Aotearoa, 2023
2 Petition of Citizens Advice Bureau, 2022
3 The New Zealand Seniors Series, 2022
4 Waka Kotahi open data portal, 2022-2023
5. RealMe identify verification service expanded ,2024

What can we learn from the rest of the world?

We aren't the first ones to look into the future of digital identity. Singapore and Australia are just two of the countries who have released their own version of Verifiable Credentials and digital wallets. The European Union is also doing something similar to work across all countries within the Union. These technologies have allowed users to digitally verify themselves with government services and other businesses. We can learn from what other countries are doing and have found in their development of digital identity technology and the common challenges faced.

Singapore

Singapore have a digital identity service called SingPass Mobile which was launched in 2018, with 20,000 active users obtained within two days of launch. SingPass is a digital ID that allows access to over 2,700 services provided by over 800 government agencies[1].

One key learning noted by National Digital Identity (Singapore)[2] during development was the test environment vs real-life scenarios using individual mobiles with different operating systems, preferences and settings and actual user data. It wasn't until they tested the app in real-life conditions that problems surfaced. These included missing notifications during app set up, following more natural directions from others, and buttons being too small. The team also tested QR code scanning with positive responses due to general acceptance and easier functionality for those with limited motor skills.

Other learnings and observations include:

- Maintaining the balance of ease and rigour, sometimes when things are too fast they don't feel as secure.
- Technical errors can cause fear and distrust, what happens if the app is not available when it's needed?
- Digital credentials can improve the experience of interacting with government services, making it less of a chore.

While these findings are generally positive, there have still been concerns raised around accessibility for disabled people and exclusion of those without access to the appropriate technology.

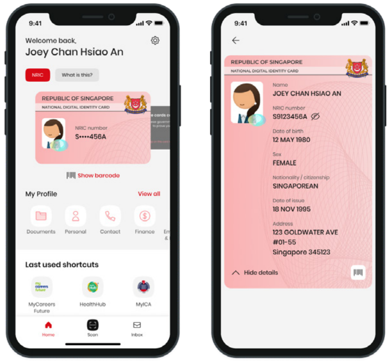
Other key learnings from the Singapore digital identity is it's use across the private sector, boosting it's usability and uptake across the population. The day to day application increases the value addition and interest in the service.

Australia

MyGovID is the Australian Government app which allows citizens to digitally verify themselves across many government services. This service has three different 'strengths' that require different details and verification, and in turn provide different levels of access to services. The strongest identity strength requires verification of an Australian passport and an additional identity document as well as a one-off facial verification check.

Publicis Sapient claim that the 2024 Digital Citizen Report found 73% of Australians have a myGovID login, with 91% of users reporting to have a positive experience using the app and 83% find it trustworthy[4]. Other findings from the Digital Citizen Report include support for expansion, especially from younder demographics, and general concern for how the government keeps identity data safe.

In 2023, the Australian Government commissioned an audit into the user experience, functions and performance of myGov, which includes the ID app. One of the findings of this audit was those needing the most support having the greatest challenge accessing government digital services.



9:41

Welcome back,
Joey Chan Hsiao An

NRIC | What is this?

REPUBLIC OF SINGAPORE
NATIONAL DIGITAL IDENTITY CARD

NRIC number
S••••456A

Show barcode

My Profile — View all

Documents | Personal | Contact | Finance

Last used shortcuts

MyCareers Future | HealthHub | MyICA

Home | Scan | Inbox

9:41

REPUBLIC OF SINGAPORE
NATIONAL DIGITAL IDENTITY CARD

Name
JOEY CHAN HSIAO AN

NRIC number
S9123456A

Date of birth
12 MAY 1980

Sex
FEMALE

Nationality / citizenship
SINGAPOREAN

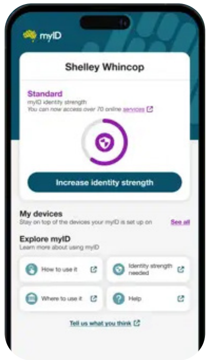
Date of issue
18 NOV 1995

Address
123 GOLDWATER AVE
#01-55
Singapore 345123

Hide details

Left:
Example of Singpass app[1]

Right:
Example of Australian Government myID[5]



myID

Shelley Whincop

Standard
myID identity strength
You can now access over 70 online services

Increase identity strength

My devices
Stay on top of the devices your myID is set up on — See all

Explore myID
Learn more about using myID

How to use it | Identity strength needed
Where to use it | Help

Tell us what you think

[1] SingPass

[2] National Digital Identity (Singapore) - Blog Series, Part 1 - 4

[3] MyID: How to set up myID

[4] Publicis Sapient: The future of digital identity in Australia, 2024

[5] Apple Store: myID - Australian Government

European Union

According to the European Commission, the EU Digital Identity (eID) Wallet is Europe's answer to the challenges of identification with the aim to make wallets available to every citizen, resident and business by the end of 2026[1]. The benefits listed, are similar to benefits found throughout this research including easier access, improved protection and security, reduced information sharing, less admin and reduced cost of authentication.

In 2023, they initiated pilot programmes involving over 350 entities from 26 Member States, Norway, Iceland and Ukraine. These pilots will test the wallet across a range of daily life scenarios and collect feedback. Some of the scenarios include Digital Travel Credentials, accessing government services, opening bank accounts, storing and presenting drivers licences, providing electronic signatures, claiming and dispensing medical prescriptions, education certification, access social security benefits, and payments of products and services[2].

In April and May 2024 an expert survey was conducted across a range of subject matter experts and Linkedin covering specific topics related to the Digital Identity Wallet[3].

Some experience findings from this report include:

- While customers would be able to download the wallet and start using it, it may not be so clear cut and simple for the relying parties as the acceptance of digital wallets is not default today. Existing processes and technology could play a big challenge from adapting customer journeys and back office processes as well as technical integration and cost.
- Ensuring vulnerable groups in society are part of the design and development from the start is key, starting from edge cases such as disabled users.
- Good awareness and education as well as addressing UX and functionality can help with inclusion and equality.

What people around the world think....

More than **9 in 10** Europeans are worried about digital identity theft[4].

74% of Australians support an expansion of the myGovID into businesses, especially younger Australians[5].

56% of Australians are concerned or have doubts about how the government keeps their data safe[5].

A survey of UK residents found that **36%** hold a digital ID and **20%** of people do not know whether they hold one or not. **57%** were not aware of a digital ID[6].

44% of residents surveyed in the UK would prefer a digital ID created by the government rather than a large tech company[6].

> *"Citizens will only adopt digital ID systems if they are "***human-centred***, focusing on* **solving people's problems***'"*
>
> - Miquel Estapé, chief executive of Open Government of Catalonia[7]

[1] European Commission: European Digital Identity
[2] EU Digital Identity Wallet Pilot Implementation
[3] Sonicbee: 2024 Survey Report - Expert Opinions on State of the EU Digital Identity Wallet
[5] Publicis Sapient: The future of digital identity in Australia, 2024
[6] Digital Identity in the UK: A rapid response study, 2024
[7] Digital identity dilemmas – and how governments are working to overcome them

Māori Data Sovereignty and a whānau centred approach

"The Treaty of Waitangi underlines the importance of participation by Māori in government and decisions that affect their rights and interests. The ability of Māori to participate in these matters contributes to both the building of trust and social cohesion, and the effectiveness of government decision-making for improving outcomes and services"[1].

Te mana raraunga Māori Data Sovereignty

Te mana raraunga Māori Data Sovereignty outlines a number of guiding principles to how Māori data is defined, collected, accessed, interpreted, and used.

These principles include:

- Data should live as close as possible to the environment and people the data is about
- The people who know and care about that data should be the ones to look after it
- Decisions about the storage of Māori data should 'enhance control for current and future generations' and reinforce Māori kaitiakitanga, guardianship, of data
- Infrastructures for data relating to Māori must be controlled by Māori
- Storage of Māori data must be within the direct jurisdiction of Aotearoa
- Done in a safe way with the consent of those involved[2].

The location in which data is stored, including identity data and where it has been used, should be considered. If the system allows the data to be stored within the wallet, which could be managed by a third party and held in a cloud or offshore, there is potential for concerns around where this data is stored and who has access to it. Consideration should also be made around potential racial bias or identity match failures and how this might affect the use and uptake of Verifiable Credentials.

Whānau centred approach

Te Puni Kōkiri have released a report 'Understanding whānau-centred approaches' which refers to utilizing a holistic and whānau approach to improving wellbeing rather than focusing on single-issue or individual problems.

Utilizing a whānau centred approach can lead to more connected and coordinated services. These approaches tend to lead to better outcomes for Māori, who tend to have lower trust and confidence in public services, as well as Aotearoa as a whole. More work should be done to understand the impacts on whānau and how this approach could be utilised.

Māori are generally more concerned with privacy, 32% stated that in the past year they had avoided contacting a government department due to privacy concerns[6].

Māori were more likely to express concern about bias in facial recognition (63%) and government organisations combining data (55%).[3]

The cost of technology and internet connection is a significant issue for kaumātua, whānau living in isolated, rural areas and families from a low-socio economic background with school children at home[5].

Citizens Advice Bureau engagement with Māori clients shows the difficulties created for Māori whānau by systems that do not reflect tikanga and whānau life[4].

To be inclusive of Māori, it is essential to establish processes for recognising whakapapa and incorporating Te Ao Māori identities[7].

[1] Public Service Commission: Public Participation in Government in the Future
[2] Te Mana Raraunga: Data Sovereignty
[3] Te Puni Kōkiri: Understanding whānau-centred approaches
[4] CAB Spotlight Report: Māori Engagement with Citizens Advice Bureau
[5] Digital.govt.nz report: Digital inclusion user insights — Māori
[6] Privacy Commissioner: Research on Privacy Concerns and Data Sharing, 2024
[7] PAYMENTS NZ: Digital Identity workshop insights and recommendations 2024

Potential Opportunities

Technology and digital services are an engrained part of life

For many people, they have been born into a world where technology is everywhere. Doing things online is becoming a default, sometimes even an expectation, and technology is used to problem solve and interact with the world. Older generations have had to learn about it or have grown with it, but even for them it is the new normal and education and acceptance is growing with 77% of seniors surveyed by NZ Seniors agreeing that technology has been reasonably easy to embrace[1].

Most people across New Zealand have a smart phone that has a camera and is able to download apps. Those we interviewed all had multiple forms of technology available to them including smartphones, laptops, tablets and computers and 93% of the students surveyed by Mymahi owned a smartphone that could download apps, and 94% owned a smartphone that could take selfies. All of the customers we spoke to had enough data on their phone to access the internet if they needed to, with 80% of the students surveyed advising they had data on their phone.

Technology can also make things more accessible for those that require additional help such as those who are blind or low vision or even learning difficulties like dyslexia. Screen-readers and other audio prompts, the ability to zoom or reformat the size of words or even easily find definitions of words can help people become more self-sufficient in their daily lives. People in the deaf community may also rely on technology to help with communicating with hearing people using functionalities like notepad or even skype calls to utilise NZSL. NZ Seniors found that 64% of seniors surveyed thought that modern technology is more of an assistance in daily life, and 42% would find it a hassle to manage without access to digital devices[1].

More and more services and life activities are moving online including schooling and work building that confidence and capability. This confidence and capability means that new and emerging technologies are more readily accepted, and people are more attuned to just ‘roll with it’.

77% of seniors agreed that technology has been reasonably easy to embrace[1].

93% of students owned a smartphone that could download apps, **94%** owned a smartphone that could take selfies.

“I deal with it on a daily basis with my own job. I’m pretty savvy with the digital space.”

“I have Teams and have to turn stuff in for school. I’ll buy tickets online, or sometimes my parents will.”

“I do everything online. It’s quicker and easier. I’m busy with family and work, so easier online.”

[1] The New Zealand Seniors Series: The Digital Trends Report 2022

Generally high trust in government, interests in controlling their own information and keeping it safe

All of the participants we spoke with indicated they would do most things to everything online with government if they could, and they generally had a high level of trust in government, though for some this trust needed to be earnt. They felt security was generally good, there were low chances or risks of privacy breaches, and that information wouldn't be shared to other agencies. However, some felt they just had to trust government regardless otherwise they wouldn't be able to get the thing they wanted. Where they felt there had been previous data breaches, such as NZ Police, there were lower levels of trust.

90% of NZers find the idea of being more in control of their digital identity appealing[1]. Reasons for wanting more control of their data include being able to check and correct it, control who buys it and for what purpose, deciding what they share and to who, and reducing the risk of fraudulent activity. Of those we spoke to, most would prefer to provide consent with each interaction as well as be able to see a record of where it was shared. When asked how they generally felt about information sharing, most people didn't really think too much about it with some people concerned about how much of their information was actually viewed. However, when we talked through the process further, all of the people we spoke to preferred that their information would not be viewed or stored.

The need to carry and present physical documentation opens up risk for these items to be lost, stolen or damaged. Replacing these documents can be expensive and time consuming, this impact is heightened when the services required are time sensitive. For those in vulnerable situations, it may allow for the ability to replace their identity credentials to access services in a quick, easy and affordable way.

Currently when people present their identity documentation, this consists of a full set of information presented on the document rather than only the subset that is required. What is then done with this information can vary depending on the agency, from photocopying and filing to storing information within a secure system. This can expose this information to privacy breaches and identity theft. With Verifiable Credentials, only the information that the agency needs will be shared, in some cases a simple 'Identity Verified' message would be presented to the receiver. This means that in some cases personal information may neither viewed by a person, nor stored in a system.

90% of New Zealanders find the idea of being more in control of their digital identity appealing[1]

"I trust passports because I assume Passports has very could protocols. I've never heard of duplicate passports."

"They wanted to verify me but they couldn't use my driver's license, they wanted my birth cert, which I didn't have at the time. I had to wait for that to come. "

"Securely gives out information that needs to be given out. There are apps that ask for more information than they need."

[1] Digital Identity in Aotearoa: Identity and Trust in an Increasingly Digital New Zealand, 2023

Proving identity is easier and faster

Among the range of ways that Verifiable Credentials can simplify the process of accessing services, people we spoke to identified the reduction in travel to prove identity in person, keeping identity information in one place and real-time information sharing would make things easier.

For some, the requirement to go in-person to prove identity to obtain services can prove a large barrier. Carting young children around, finding parking close by, mobility issues and living out of town can make it hard for people to prove who they are. Those living in rural areas may need to travel long distances to access services, especially if they are not located in their closest town. Verifiable Credentials could open pathways to allow more services to move fully online, allowing people to prove their identity from their own home in a way that is trusted and secure. Opening bank accounts, applying for university, applying for benefits or jobs from home could help people access these services more easily.

With identity documents stored securely on a phone, users can easily access and share their credentials whenever needed. When asked what their go-to identity document was, almost everyone said a drivers licence. This is because it is widely accepted and easily carried around, often in a wallet or even in their phone case. Along with a wallet, most people will also have a smart phone on them while out and about. Of the 500 students surveyed by Mymahi, 46% of them said they would prefer providing identity via phone (26% prefer having physical cards and 28% answered ‘not sure’). By replicating the on-the-go convenience of a drivers licence Verifiable Credentials should, in theory, be a handy way of having identity documentation on you at all times.

The process of applying for and using verifiable credentials utilises real-time information sharing and matching, without the need for ‘processing time’ in the back office. This potentially enables users to apply for and use verifiable credentials right at the time they need it (provided they have access to the internet). For people in emergency situations, such as victims of theft or those leaving harm, the ability to quickly obtain an alternative identity document in order to access services or replace lost items, could alleviate stress and worry. Although, care needs to be taken to ensure the process feels secure and users know what is happening at the time to build trust. The inclusion of messaging such as ‘checking details against source data’ or processing screens can provide reassurance that the system is robust.

46% of Students surveyed would prefer providing identity via phone, **26%** would prefer physical cards and **28%** were unsure.

64% of seniors think that modern technology is more of an assistance than a hindrance in their daily life[1].

15.7% of New Zealanders live in rural areas[2].

An estimated **17%** of people were disabled in 2023, with **9%** of adults identified as disabled due to physical difficulties[3].

“It looked good, looked like it would simplify sharing information. Makes things easier.”

“It would have been easier if I did it online, I have a 5 year old child that I had to take with me.”

[1] Digital Identity in Aotearoa: Identity and Trust in an Increasingly Digital New Zealand, 2023

[2] EHINZ: Urban-Rural profile, 2024

[3] Stats NZ: 1 in 6 New Zealanders are disabled, 2025

Potential Challenges

Digital exclusion in our communities

One of the biggest challenges to the acceptance of Verifiable Credentials across Aotearoa, is digital exclusion in our communities. Digital.govt.nz research has found that 1 in 5 people in Aotearoa New Zealand lacks at least 1 of the 4 elements needed to be digitally included – motivation, access, skills or trust[1]. Those most at risk of digital exclusion in Aotearoa New Zealand include; Māori, disabled people, Pacific people, those in social housing, seniors, the unemployed and underemployed, and those living in remote communities.

The common barriers to digital inclusion include:

Technology and connection

Unaffordability and access to appropriate devices and internet connection. People may have an older phone that cannot display certain websites, or perform certain functions, they might not have any data and they may not have access to a device that lets them access the internet in an easy, private and safe way.

Some rural areas face significant challenges with consistent and reliable coverage, leading many to rely on community hubs like libraries, schools, and marae for internet access. Some people even move around to find better coverage or use public Wi-Fi.

Face to face interaction

Many communities, especially Māori, Pasifika and elderly, prefer kanohi-ki-te-kanohi (face to face) interactions, speaking to real people. These interactions help to build trust and relationships and allow people to talk through complex issues.

An increasing online environment creates the reliance on remote support for users, often provided through chat-bots, email or over the phone leaving many without the necessary support or information.

Face to face interactions can also help with interpretation in the deaf community, either through lip-reading or where sign-language support is provided as many deaf people prefer NZSL communication.

Confidence and skill

Those who do not regularly utilise, or are new to, online and digital services can lack in skills and confidence to be self-efficient online. This can especially affect those leaving the prison system, seniors, migrants and even young people doing things for themselves for the first time.

Legalese, jargon and technical language can make government services hard to navigate with distrust and confusion around what people are actually doing or signing up to. This can particularly affect those where English is a second language, such as refugees, migrants and Pasifika communities, especially if they are also unfamiliar with government processes or 'how we do things here'.

Accessibility

Individuals with disabilities, like those who are blind or have low vision, often face challenges using technology and services that lack accessible design. Features such as verbal and sensory cues, screen reader compatibility, screen rotation, and alternative text can enhance inclusivity. Additionally, people with autism or motor skill challenges may find it hard to take or have their photo taken so may be impacted by the use of facial recognition technology.

[1] Digital.govt.nz: Report: Digital inclusion user insights — Māori, 2021

Building trust in online identity in a world where awareness and fear of digital safety is increasing

With the rise of AI, scamming, hacking and data breaches peoples awareness and behaviours in how they interact with technology, government services, and their own personal information is changing.

There is a noticeable shift in behaviour, with DINZ reporting that 78% of New Zealanders are concerned about the protection of their identity and the use of it by organisations, and 50% have adapted their online behaviour due to concerns around data privacy[1]. Past data breaches involving government agencies have led to caution around information sharing, reinforced by fears over where data may be stored internationally. Where people have experienced scamming or hacking, either personally or witnessing, it makes them more wary about what they are doing and who they interact with. New Zealand Seniors found in a 2022 survey that 79% of seniors know someone or have been personally targeted by scams, 80% are reasonably concerned about the safety of their private info online, with 19% extremely concerned[2].

When it comes to trust in government, generally New Zealanders have high trust however there is a level of 'trust because you have to'. In order to get the products they need, for example a NZ Passport or drivers licence, or to utilise the services they are required for, you just have to trust that they are safe to get the product or service. Māori and Pasifika can have lower levels of trust in government holding and sharing information about them due to incorrect assumptions, misuse of data and historical events. The Privacy Commissioner also found that Māori were more likely to express concern about bias in facial recognition (63%) and government organisations combining data (55%)[3]. These concerns can include racial or gender biases and misidentification. This bias may not be directly linked to purpose of facial recognition for using Verifiable Credentials, but it will potentially have an impact on the trust of the technology and it's ability to perform and obtain the correct identity.

Overall, people find doing things online easier but some have reservations about moving some sensitive or high-stakes tasks, to digital platforms feeling that paper-based or in-person processes and documents are more secure. If you have your identity documentation physically in your hands, or your wallet, you know no-one else has it.

78% of New Zealanders are concerned about the protection of their identity and the use of it by organisations[1].

79% of Seniors surveyed in 2022 knew someone or had been personally targeted by scams[2].

Māori are generally more concerned with privacy, **32%** stated that in the past year they had avoided contacting a government department due to privacy concerns[3].

> *"Government things should be on paper - hackers are prominent now, people can steal information more easily"*

> *"Have to trust whether you want to or not"*

> *"If you only have it on piece of paper it's the only proper one and no one could get it. Online people can make copies of it digitally. "*

[1] Digital Identity in Aotearoa: Identity and Trust in an Increasingly Digital New Zealand, 2023
[2] The New Zealand Seniors Series: The Digital Trends Report 2022
[3] Privacy Commissioner: Research on Privacy Concerns and Data Sharing, 2024

Competing with other accessible identification documents

All of the people we spoke with already held at least one, mainly multiple, forms of photo or other identity documentation. These included drivers licence, NZ Passport, Student ID card, gun license, Kiwi Access card and birth certificate.

The drivers licence is the most commonly held form of photo ID with around 4.3 million New Zealanders holding some form of drivers licence. It is also one of the most commonly used due to the need to hold and present one when driving, its wide acceptance, and ability to fit easily into a wallet or phone. When it came down to it, most said that for in-person interactions, it would be easier to pull out their existing drivers licence.

While in theory, holding something on your mobile device and simply sharing via QR code seems easier than carrying around physical cards, in reality in-person could be a different story. Success of identity checks in public and the reliance on internet and phone battery, will determine whether Verifiable Credentials are easier to use than physical cards.

Holding identity information on a mobile device poses both benefits and risks. Lost or stolen mobile phones and hacking were concerns raised by those we interviewed, amplified by the fact that everything would then be in one place and accessible to others. Of the 500 students surveyed by Mymahi, just under half (46%) of respondents would prefer providing identity via phone (26% preferring physical cards and 28% were not sure).

Obtaining a Verifiable Credential also relies on the holder already having a NZ Passport, and possibly in future, a drivers license. The cost of a NZ Passport, especially for those on lower incomes or with no means or plans to travel, may pose as a barrier and push them to use other existing identification documents. Around 76% of New Zealanders hold a valid New Zealand passport, this number will be higher including expired passports. To get a Verifiable Credential, people can have an expired passport though how well these might work for photo matching will need to be determined, especially where people may have changed appearance over time.

Around **4.3 million** people in New Zealand hold a form of drivers licence[1].

46% of Students surveyed would prefer providing identity via phone, **26%** would prefer physical cards and **28%** were unsure.

76% of New Zealanders hold a valid passport.

"As a young disabled person gets older and needs to get id it can be tricky. A passport is a luxury thing and hard to justify the cost when the person is often not actually going to ever travel."

"I'd still use the physical driver's licence. It's easier. Your phone might die or there might be problems."

[1] Waka Kotahi open data portal, Drivers licence holders 2022 - 2023
[2] The New Zealand Seniors Series: The Digital Trends Report 2022

Potential accessibility issues in the customer experience

As part of obtaining and using a Verifiable Credential, users have to take a live photo to bind themselves to the identity information. People are becoming increasingly familiar with performing facial biometric testing, such as unlocking their phone or going through SmartGate at the airport. Understanding and acceptance around this technology is increasing, though it does not mean everyone can easily use it. Those with disabilities, especially around vision, sensory processing or motor function, can struggle to use this technology from inability to keep still to not being able to read the instructions.

As well as accessibility issues with the identity check function, not everyone is comfortable with taking a photo of themselves in public. Almost everyone we spoke to, as well as 18% of the students surveyed by Mymahi weren't overly comfortable taking a photo of themselves in public. It was also felt to be an inconvenience or unnecessary step, especially where they might already hold another form of ID. Some did mention that as this became more normal, they might feel more comfortable, or if they had to do it they would. Of the remaining students surveyed by Mymahi, 20% said they would feel very comfortable, 29% would be somewhat comfortable and 28% felt neutral. This is likely due to the culture of taking selfies for social media and instant messaging platforms.

We also do not fully understand how effective the identity check function would be where customers are using it in person such as at supermarkets or public services. Currently, the technology of biometric identity checking is used by Realme where it is only used as part of an application or set-up, not in an as-used function. While the success of the Realme biometric testing sits at around 90%, this is generally where people are in sufficient lighting and in-front of a plain background without environmental pressures of real-time use.

The end to end experience of obtaining and using Verifiable Credentials is highly important. If there is no support or guidance provided during in-person use people may not, in the end, be able to use their Verifiable Credential or get the service they require. We heard of a story around doing a blood test, as there is generally no-one at the reception desk and you are simply required to take a number and wait to be called, people with low or no vision rely on asking others what their number is. This is a good example of where just a single part of the experience can have a significant impact on the overall experience.

18% of students weren't overly comfortable taking a photo of themselves in public.

Currently, the success rates for liveness testing sits around **90%.**

Over **180,000** people in New Zealand are blind, deaf-blind, or have low vision[1].

"It would be an unnecessary inconvenience. I think there would be a slow up take. An elderly person would be fumbling around (taking a photo). It would be easier to pull out their bank card."

"Oh bloody hell, not again!"

"I'd be very cautious out in public, it could screw up with someone else's identity, would be ok at home."

[1] Blind Low Vision: Vision Loss Can Affect Anyone, At Any Time of Life, 2023

The influence and perceptions of Realme, and agency uptake

RealMe is a government-grade login and verified identity service that has been around since 2013. It is a service that allows users to prove who they are online and access many government services online such as applying for a passport, open a bank account, enroll in education, apply for jobs, vote and more. While it can enable access to online services, it also poses as a barrier as it is not always simple. With it's limited use it can, in many cases, only be used a few times a year rather than a system that is used regularly. This leads to varying usability experiences, most commonly around passwords and confusion around what type of Realme identity they hold – login or verified identity. People that we spoke to commented on mixed experiences from arguing and giving up to finding it easy, some hadn't heard of Realme though this was likely due to age and limited experience in proving identity.

Existing views around RealMe may spill over to new digital identity products, even if they are not obviously linked. If RealMe is incorporated into Verifiable Credentials, this could also prove as a barrier.

As found with Realme, agency buy-in could hugely impact the uptake of Verifiable Credentials. Most people who look over 25, for instance, won't be asked to prove their age for more common situations like proof of age. As more agencies and services get onboard with digital identity and verifiable credentials, trust and uptake in the product and process will increase. While a large amount of services are start get on board, and still use physical identity verification, customers may default to known options such as drivers licences and passports as a way to prove who they are.

Singapore, with it's digital identity SingPass, utilises adoption in both the public and private sector allowing users with higer utility in common daily tasks which has in turn boosted the adoption of the service. Through requiring all public services to adopt the identity verification system and integrating it in private sectors such as banking and insurance, they have 90% of citizens and permanent residents using the service[1].

More than **1.5 million** Realme verified identities exist[2].

RealMe is currently used by **44** agencies and provides access to **148** online services[1].

"The RealMe thing I have to work at, it's just not seamless. I didn't know there was more than one RealMe account. I haven't used it a lot because I haven't found it fantastic. "

"I Argued with it and gave up"

"It has made it easier to do things, easy for (me) but my wife found it difficult."

[1] Digital identity dilemmas – and how governments are working to overcome them

[2] RealMe identify verification service expanded

Opportunities for building uptake of Verifiable Credentials

Government-backed and secure

Building trust and visibility of the service is also important. When asked how they adopt new technologies, most people said they are inclined to see how others use it first or see it in action to gain proof that it actually works, before trying something for themselves. Having a government logo, backing from a trusted group, and clear information around how it works and how personal data is kept safe can also help people feel safer using it.

Things like strong passwords, two-factor logins, and face or fingerprint ID were seen as good ways to help people feel secure.

Wide-ranging use cases

Making the technology both useful and visible across a wide range of real-life scenarios is key to driving uptake. Those we spoke to said they'd be more likely to use a digital ID if it worked across lots of services—like government departments (MSD, IRD), banks, universities, and even for things like renting a flat or getting student discounts. Linking Verifiable Credentials to discounts, making it easier to deal with services used regularly, or other incentives or benefits can help boost uptake.

Young people, particularly students, may be a good first pilot group as they are more likely to be asked to prove their identity on a regular basis, with a range of connected services.

Support and education

A lot of people still don't fully understand what digital identity is or how it could be used.

Strategies that would help could include simple, clear information—videos, demos, and support in multiple languages, including NZ Sign Language. This is especially important for disabled communities and people who aren't confident with technology or have limited education. Some said help through public libraries or community groups would make a big difference.

Inclusive design

Accessible and inclusive design is highly important when developing and implementing new services and technologies. Designing for those who might struggle more, will help ensure a product that works for all.

Incorporating a Te Ao Māori worldview and Māori data principles can ensure we are fair Te Tiriti o Waitangi honouring partners.

Including, or allowing compatibility with, accessibility features and technology will allow those who find it harder to access services an easier and more efficient experience. The inclusion of translations (including NZSL), screen-reader technology or sound/vibrational cues will help more people to use Verifiable Credentials in a way that works for them.

"Government stamp is pretty good for me"

"I would probably wait until my friends had used it and I got some feedback. Or a demo from someone. Or some kind of targeted campaign for disabled communities."

"If other people are accepting it as a proof of identity and it was easy and secure, I'd use it. If it was transferrable to other companies"

"References from other people who've used it before. And then going onto the sites to make sure everything they say is true."

Objective 2: Understand the full end-to-end journey of a customer covering various parties

How people view and interact with the world, technology and services will impact their experience with using Verifiable Credentials. This could be influenced by digital literacy and ability, their age, what services they are using, and comfort level with different forms of technology.

As mentioned in Objective 1: Understand the social license implications of verifiable credentials, there are a number of barriers that will exclude, or make it harder for, some people to access and use a Verifiable Credential. These include the cost of a smartphone, access to the internet, confidence with technology and in the digital space, and the requirement of already holding a New Zealand passport. These barriers will prevent, or make it harder for, a number of communities to access this new service. For those that can access this service, there will be varied experiences with obtaining and using Verifiable Credentials based on how they interact with technology and services, and existing perceptions or experiences.

At the highest level, the end-to-end journey needs to be accessible and make things easy, if not easier, than how people do things currently. If the credential itself is easy to get, and the holder app is easy to navigate but the experience of using it across a range of services is not easy or accessible, then the overall experience is affected and uptake will be reduced. Similarly, if there is not a wide range of services that utilise this technology, or where people are not using it on a regular basis then uptake may be affected.

The following pages outline some key insights highlighted by previous research and feedback provided by interview participants who were shown a demonstration video and asked a range of supporting questions. These insights at this stage are primarily ‘in theory’ as opposed to actual experiences which could be gained through scenario testing using a prototype in different situations. The experience is also likely to be very different for in-person proof of identity, versus proving identity for online services. Where these differences exist or where feedback is specific to one of these scenarios, they have been identified through the customer journeys.

> *“It’s ok that the passport has expired, that’s great.”*

> *“If I got this far but don’t have a passport I would go back and see if I could change it to driver’s license.”*

> *“Not going there - trying to do photos in public”*

> *“Worry about a dodgy QR code - will it know if the QR code is legit?”*

> *“I use QR code scanning. Have used it for work. I feel comfortable doing this. ”*

> *“I give consent for them to read my information.”*

Current state journey map - proving identity in New Zealand

	Obtaining ID	Storing / Holding ID	Sharing ID
Actions	• Complete paper or online form • Take photo or perform identity check • Find referee • Pay fee • Provide another form of photo ID or identity document • Go into office or post in application form	• Store documents within a safe or filing cabinet • Keep all family documents in one place • Hold drivers licence in wallet • Scans or photocopies filed away or saved on computers or mobile devices • Lost or stolen documents	• Present in-person • Send scan or photocopy • Enter details into online or paper form • Assert RealMe Verified identity • Copies of documentation taken by service or organisation
Experience insights	• Experiences can range from easy and quick to a hassle and time consuming. • Most people expect or accept that processes will be somewhat difficult, rigorous and take time. • Influences can include time pressures, what identification documents the person already holds and reasons for replacement. • Getting an ID can be expensive, especially a NZ passport which can also take up to 10 working days. • General lack of identification available to seniors, young people, those with disabilities and migrants. • Taking a photo for identification can be difficult for people with vision and motor-skill impairments as well as sensory processing disorders such as autism.	• The most commonly held forms of photo ID include a driver's licence, NZ passport, Student ID card, Kiwi Access Card, and gun licence. • Many use their birth certificate as proof of identity, and for some, it is the only form of identification they hold. • For those unable to drive, holding a NZ gun licence can be an alternative, while young people may rely on a student ID as their only type of photo ID. • Some individuals possess a RealMe account, though many are unsure of the specific type of account they hold. • Vulnerable groups such as those in crisis situations, former prisoners, migrants, refugees, the unemployed or underemployed, elderly, and disabled people often lack sufficient identification.	• How often people need to prove their identity is mostly determined by age, with younger people needing to prove their age most often, as well as people who interact with government services. • The drivers license is the most commonly used form ID, due to the requirement to hold one while driving, convenience to carry around, and it's general acceptance across a range of services. • In most cases, providing ID is relatively easy, straightforward and accepted as practices are similar across services. • The requirement for multiple forms of ID can make the process more complicated. • The requirement to perform identity verification in person can be hard for some, especially those who require support or need to take children.

Future state journey map (page 1)

Key

- 🟢 Positive
- 🟠 Neutral
- 🔴 Negative

Getting a Verifiable Credential

	Set up wallet	Verify identity
Steps	1. Downloads holder app 2. Accept wallet terms of use 3. Allow access to phone camera 4. Performs liveness check for wallet set-up 5. Accept privacy statement and consent to share identity details	1. Enter personal details 2. Enter passport number 3. Take live photo 4. Photo and details matched to DIA source data 5. Credentials displayed in holder app
Experience insights	🟢 Most of the people we spoke to had mobile devices capable of downloading apps and used apps on a daily basis. 🟢 Generally, people are comfortable and familiar with facial recognition or biometric technology. 🟠 Most people we spoke to, would select ‘allow while using this app’ for camera access to their phone. 🟠 Blind or people with low vision may rely on screen-readers or other technology to use their mobile devices. 🟠 Often terms and conditions are not read as they are typically long and hard to understand. Barriers include English as a second language, unfamiliarity with government processes or jargon. 🔴 Terms and conditions are not always accessible to those who are blind or low vision with alternatives not always available. 🔴 Some people will have difficulty taking a photo of themselves e.g. lack of motor skills, vision impairment or sensory processing disorders. 🔴 People may have an older phone that cannot download the app, have a suitable camera or not have access to the internet. 🔴 Parental or school controls may mean young people cannot access or download the app during certain times, or access the service.	🟢 Some people were relieved that the passport could be expired. 🟢 The interfaced seemed standard and easy to use. 🟢 People generally knew where to find their passport number. 🟢 The green ticks on the credentials made people feel that they were valid and ready to use. 🟠 Those who have recently changed name will need obtain a new passport with the updated details to reflect in the credential. 🔴 The requirement for a NZ Passport will be a barrier due to it’s cost. 🔴 Some concern around whether the identity check would work where the photos may be different due to age or other factors. 🔴 Usability issues with the live photo and reading the instructions if they have vision issues or need to take off glasses. 🔴 Repeated liveness checks could create a cumulative difficult experience for those who struggle to perform this task.

Future state journey map (page 2)

Key

- 🟢 Positive
- 🟠 Neutral
- 🔴 Negative
- 🖥 Online specific
- 🧍 In-person specific

Using a Verifiable Credential

	Presented with QR code	Scan and share
Steps	1. Presented with a QR code 2. If required, user logs on to holder app and performs identity check	1. Opens 'scan' function 2. Scans QR code 3. Consent to share information with provider
Experience insights	🟢 Some people were relatively comfortable with QR codes as they saw or used them frequently. 🟠 Some people were wary of QR codes due to potential scamming or hacking risks. 🟠 Most people would feel safer with QR codes presented on a website or app, rather than being sent via email. 🧍 Visually impaired individuals may struggle with locating or viewing QR codes and those in wheelchairs might find it difficult to reach QR codes. 🧍 Many people find taking photos in public uncomfortable and inconvenient, with concern around potential failures, especially if it is repeated. 🧍 Personal preferences and practicality may drive people to use existing identity documentation such as drivers licence.	🟢 Most people we spoke to would have no issues scanning a QR code with their mobile device 🟢 Everyone we spoke to would prefer to consent to share their information each time, giving greater control. 🟢 The process seemed straightforward, quick and easy to use. 🖥 Fully on-line services would make it easier for those with little time or ability to leave the house. 🟢 A simple verification 'pass' or tick is preferred to sharing of identity information with services, though most felt that larger and trusted organisations could see more information. 🔴 Those with disabilities may find it difficult to scan a QR code or follow the instructions. 🔴 There is a general concern about who sees and has access to their identity information and where this is stored.

Manage Credential

- Keeping a record of where and when information has been shared is important. This should be easily visible within the app.
- Notifications sent directly from the holder app, rather than via text or email are more trusted. Seniors and deaf people can be more wary of scam messages.
- If there were any issues with the credentials, for example no longer valid, people would prefer to be notified.
- A red 'X' or other message on an invalid credential could prompt people to investigate further or rectify the issue.
- Most people we spoke to would expect the owner of the app or information to provide support if required.
- Many people prefer multi-channel support including face-to-face, phone, video call or chat.
- Some people are wary of automated tools such as chat-bots or AI and would prefer to talk to a real person.

High level requirements

Accessibility and usability

People with disabilities and seniors can struggle to use technology to it's full advantage. This can be either through insufficient accessibility available in apps or websites, or through lack of knowledge and confidence. To ensure Verifiable Credentials are more usable and accessible to all, the following requirements should be considered:

- Plain English and clear instructions
- Accessibility standards applied to the holder app and affiliate websites or documentation, including WCAG 2.1 Level AA and/or PDF/UA accessible
- The holder app needs to have in-built voice, sound or vibration functionality options and be compatible with different screen readers
- Ability to zoom in and scale the screen without losing functionality or visuals
- Use of colour and messaging to identify issues or missing information
- QR codes adhere to accessibility standards with in-built QR code finder options
- Abilty to access digital ID without internet access
- Verifiable Credentials should not be the only option for proving identity available to access services
- Verifiable Credentials should be able to replace the need for customers to provide multiple forms of ID to access services.

Build trust, awareness and understanding

As mentioned in the opportunities for uptake, building awareness and understanding through education pieces will be vital to build trust and uptake in the service. While people are becoming increasingly familiar with these technologies, there may be concerns around how it works behind the scenes.

Targetted education and resourcing in a range of media can help alleviate concerns in a way that is accessible to a wide range of people. Some things that could be considered include:

- Video demonstrations including NZSL
- Education around process, privacy and security
- Translations in different languages.

Other things that can help build trust include:

- The inclusion of government logos and known branding to help demonstrate government-backing and known and trusted services
- Where possible, any data should be held within locally owned servers
- Clear guidance should be provided to users outlining exactly where there information is held, who has access and where to go if they have concerns.

Appendices

Appendix 1 - References

New Zealand:

- Digital Identity in Aotearoa: Identity and Trust in an Increasingly Digital New Zealand
- Petition of Citizens Advice Bureau New Zealand: Leave noone behind—Campaign to address digital exclusion
- The New Zealand Seniors Series: The Digital Trends Report 2022
- Waka Kotahi open data portal, Driver licence holders dataset & API
- Beehive.govt.nz: Streamlining identity verification online
- Public Service Commission: Public Participation in Government in the Future
- Te Mana Raraunga: Data Sovereignty
- Te Puni Kōkiri: Understanding whānau-centred approaches
- CAB Spotlight Report: Māori Engagement with Citizens Advice Bureau
- Digital.govt.nz report: Digital inclusion user insights — Māori
- Privacy Commissioner: Research on Privacy Concerns and Data Sharing
- PAYMENTS NZ: Digital Identity workshop insights and recommendations 2024
- Blind Low Vision: Vision Loss Can Affect Anyone, At Any Time of Life
- EHINZ: Urban-Rural profile
- Stats NZ: 1 in 6 New Zealanders are disabled

Singapore:

- Towards Inclusive Digital Transactions: Disability and The Case of Singapore's Singpass App
- SingPass
- National Digital Identity (Singapore): Making digital services more accessible for all - Part 1
- National Digital Identity (Singapore): Making digital services more accessible for all - Part 2
- National Digital Identity (Singapore): Making digital services more accessible for all - Part 3
- National Digital Identity (Singapore): Making digital services more accessible for all - Part 4

Australia:

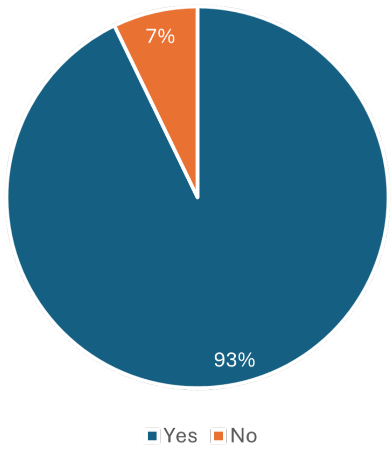
- Publicis Sapient: The future of digital identity in Australia

Other:

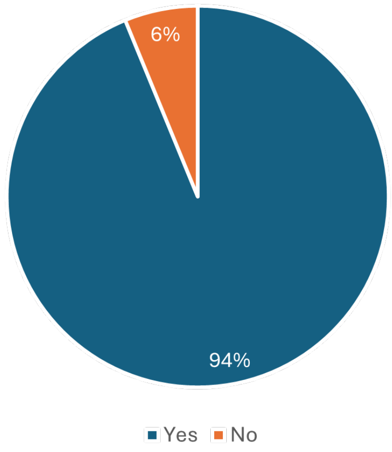
- European Commission: European Digital Identity
- EU Digital Identity Wallet Pilot Implementation
- Sonicbee: 2024 Survey Report - Expert Opinions on State of the EU Digital Identity Wallet
- Publicis Sapient: The future of digital identity in Australia
- Digital Identity in the UK: A rapid response study
- Digital identity dilemmas – and how governments are working to overcome them

Appendix 2 - My Mahi survey survey graphs

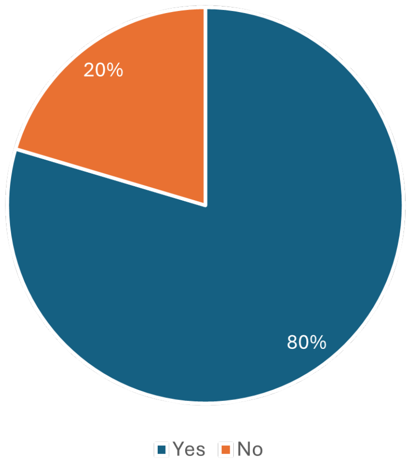
Q1: Do you own a smartphone that can download apps?



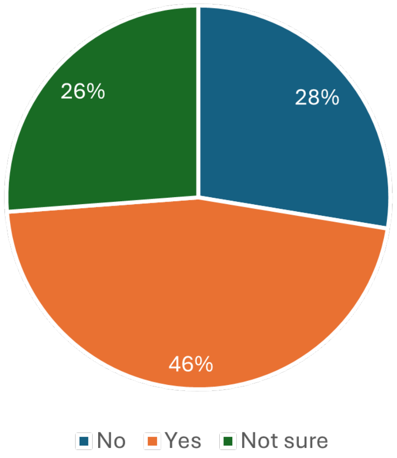
Q2: Does your phone have a front-facing (selfie) camera?



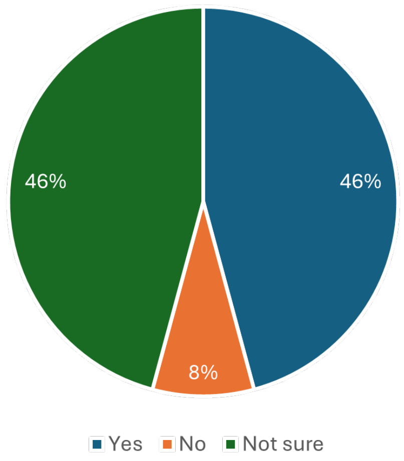
Q3: Do you currently have mobile data on your phone to access the internet?

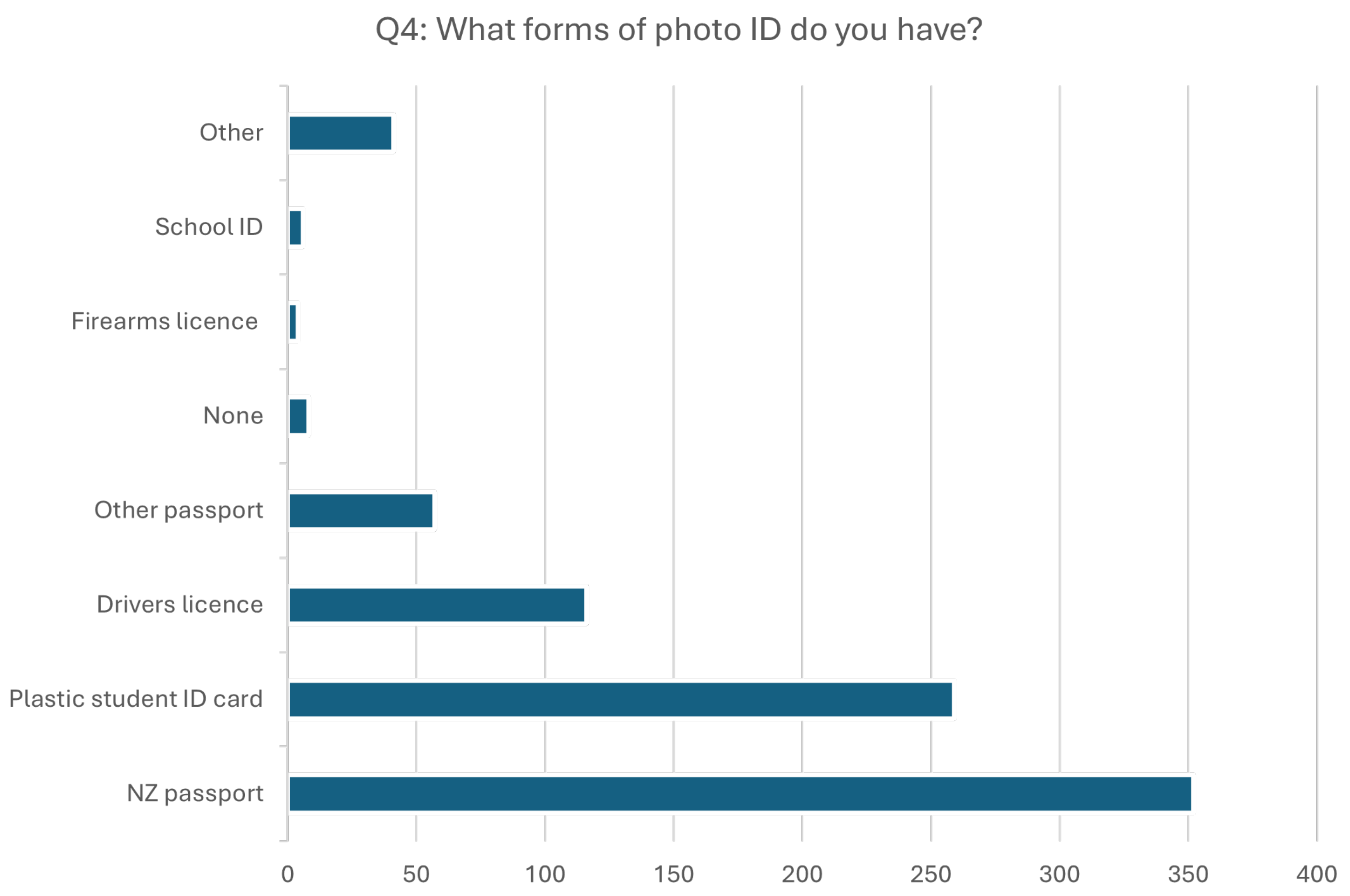


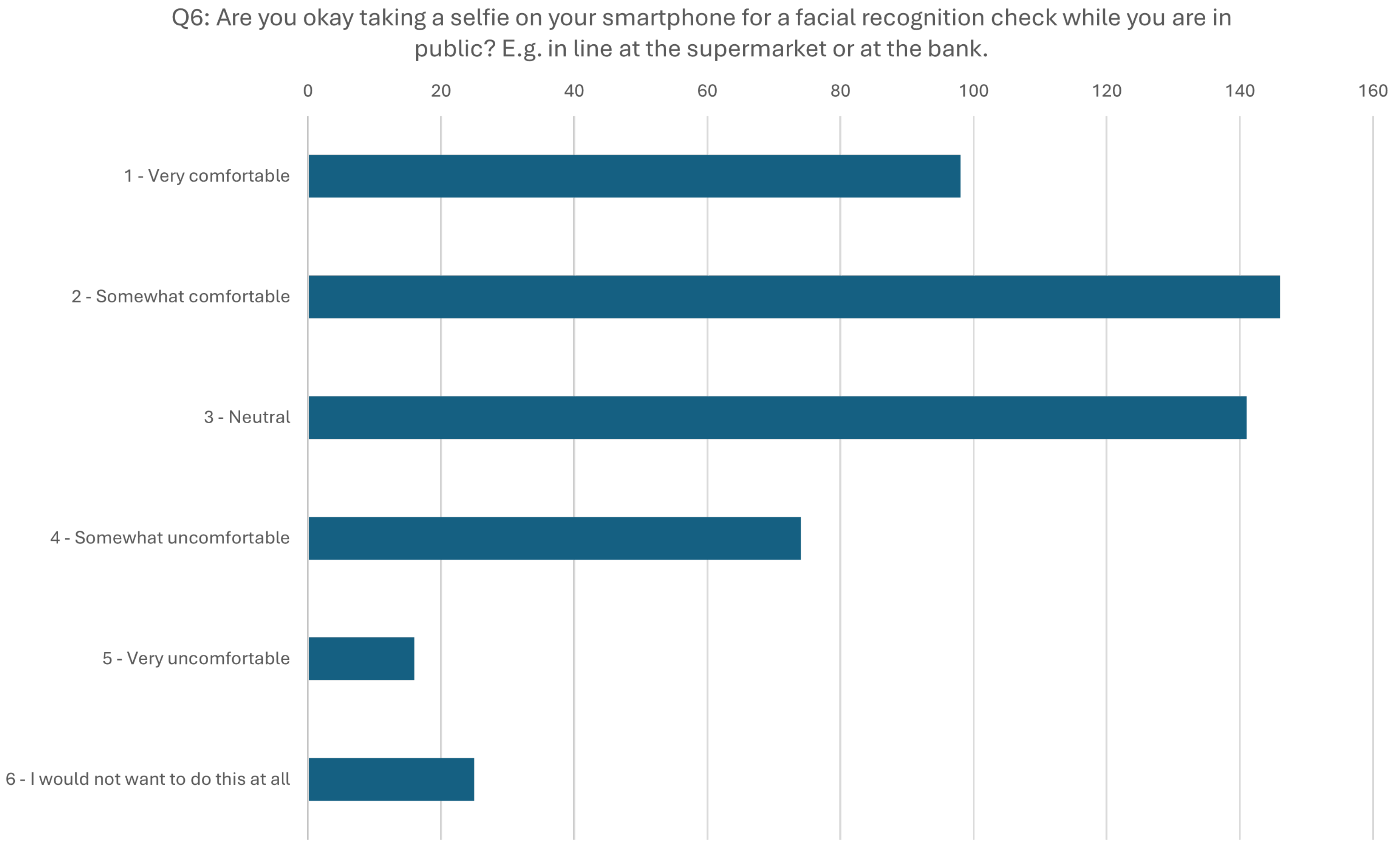
Q5: Would you prefer proving your identity using your phone over carrying physical ID cards?



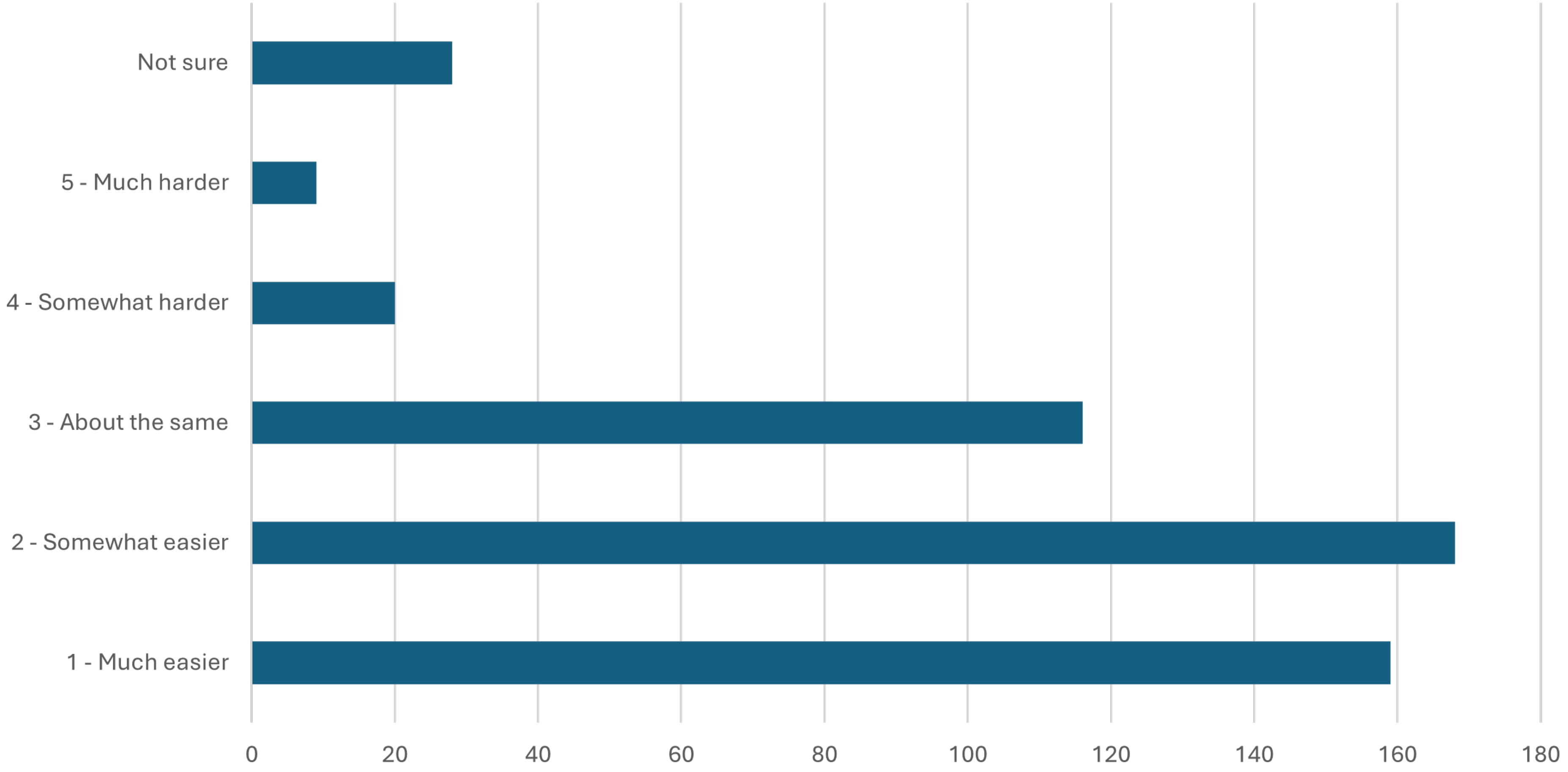
Q8: Would sharing only a 'Pass/Fail' or 'Verified' status rather than your full digital ID make you feel more comfortable?




Q4: What forms of photo ID do you have?
Other
School ID
Firearms licence
None
Other passport
Drivers licence
Plastic student ID card
NZ passport
0
50
100
150
200
250
300
350
400


Q6: Are you okay taking a selfie on your smartphone for a facial recognition check while you are in public? E.g. in line at the supermarket or at the bank.
0
20
40
60
80
100
120
140
160
1 - Very comfortable
2 - Somewhat comfortable
3 - Neutral
4 - Somewhat uncomfortable
5 - Very uncomfortable
6 - I would not want to do this at all

Q9: Would having an official digital ID on your phone make proving your identity easier or harder for you?



Appendix 3 - My Mahi survey survey free text summaries

Question 7: What features would help you feel more confident that your information is secure within an app?

- Many respondents emphasized the importance of strong passwords
- Two-Factor Authentication (2FA)was a common suggestion for enhancing security
- Biometric Authentication like Face ID and fingerprint recognition
- End-to-end encryption
- Secure data storage
- Only collecting necessary data
- Allowing users to control specific permissions and access to their data
- Alerts for unusual login activities or changes to account security settings
- Multiple forms of verification, such as email, phone, or passport verification
- Clear and transparent privacy policies
- Government-approved or open-source.

Question 10: Is there anything we should be thinking about when designing a digital ID? e.g. how it could be used, what it could be able to do.

- Security and Privacy
- Encryption, preventing forgery, and ensuring data protection
- Easily accessible, even offline
- Usable on multiple devices and platforms
- There was concern around the use of a digital ID when their phone dies
- Customizable, including adding photos, barcodes, and QR codes
- Features like multi-factor authentication, face ID, and passcodes
- Should be usable for various purposes, such as student discounts, age verification, and as a valid form of ID for different services
- There were comments on making the digital ID visually appealing and ensuring it contains all necessary information in a readable format.