

# Digital Identity in response to COVID-19

DGX Digital Identity Working Group



DIGITAL GOV EXCHANGE



# Contents

Contents.....	2
1. Overview .....	3
2. Current digital identity landscape (FA1) .....	6
2.1 Digital identity models .....	6
2.2 Policy and legal settings .....	9
2.3 Technical settings.....	10
3. DIWG experiences and COVID-19 use cases (FA2) .....	11
3.1 Australia .....	11
3.2 Singapore .....	12
3.3 United Kingdom .....	13
3.4 Canada .....	14
3.5 Finland.....	14
3.6 New Zealand .....	15
3.7 The Netherlands.....	15
3.8 Israel.....	16
4. Future mutual recognition and interoperability (FA3) .....	16
4.1 Interoperability principles.....	18
4.2 Common definitions and digital identity taxonomy .....	21

Digital Transformation Agency

© Commonwealth of Australia (Digital Transformation Agency) 2022

With the exception of the Australian Commonwealth Coat of Arms and where otherwise noted, this product is provided under a Creative Commons Attribution 4.0 International Licence. (<http://creativecommons.org/licenses/by/4.0/legalcode>)

The Digital Transformation Agency has tried to make the information in this product as accurate as possible. However, it does not guarantee that the information is totally accurate or complete. Therefore, you should not solely rely on this information when making a commercial decision.

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you are having difficulties with accessing this document, please email [digitalidentity@dta.gov.au](mailto:digitalidentity@dta.gov.au).

Version: 04

## 1. Overview

The Digital Government Exchange (DGX) Digital Identity Working Group (DIWG) was established to share experiences and opportunities for the use of digital identity initiatives, with a focus on the response to and recovery from the impacts of COVID-19 on governments and people. It also provides an opportunity to collaborate and drive progress on mutual recognition and interoperability of digital identities between member countries.

The DIWG was established in 2020 by representatives of the broader DGX international group. The current membership for this group was established in February 2021. The working group is chaired by the Australian Government's Digital Transformation Agency (DTA), with members from Australia, Canada, Finland, Israel, New Zealand, Singapore, the Netherlands, the United Kingdom, and the World Bank (as an observer). It is representative of many of the leading digital governments with digital identity initiatives globally.

The working group aims to develop pathways to enable mutually recognised and/or interoperable digital identities and infrastructure, to enhance trade opportunities in the context of a Free Trade Agreement or similar bi- or multi-lateral agreement. It also recognises that similar pathways may be part of solutions to facilitate economic recovery from COVID-19, for example to support the opening of domestic and international borders.

### Approach

The objectives of the working group have been structured around three focus areas; to understand how digital identity is being used and the models that might enable mutual recognition and/or interoperability, to share respective governments' experiences with digital identity including in the COVID-19 response, and to understand what is required to enable mutual recognition and/or interoperability between DIWG member countries. These objectives recognise that the opportunity for mutual recognition and interoperability between DIWG member countries may have broader application across non-member countries and non-government digital identities and infrastructure.

The working group recognises the opportunity to explore the various centralised, decentralised and self-sovereign identity models of digital identity as well as the capabilities that identities enable, such as digital wallets and certificates. These are captured through the use cases and experiences of DIWG member countries.

The findings of each of these objectives, outlined in Table 1 below, form the basis of the approach and structure of this report.

Table 1 – DGX Digital Identity Working Group focus areas.

Focus Area	Approach	Deliverable
<b>FA1:</b> Understand how digital identity is being used, including where free trade or similar agreements exist, and how these might enable mutual recognition and/or interoperability.	International scan of DGX DIWG member countries to understand how digital identity is being used.  Scan and alignment of DIWG digital identity definitions and taxonomies.	Description of DIWG member country digital identities and infrastructure and use cases.  Definition of a common digital identity language and set of definitions.
<b>FA2:</b> Share governments' experiences with digital identity through use cases, research findings and benefits, with a focus on the COVID-19 response and recovery.	Capture digital identity experiences and use cases with a focus on the COVID-19 response and recovery and alignment with free-trade or similar agreements.	Description of supporting use cases across DIWG member countries in COVID-19 response and recovery.
<b>FA3:</b> Understand what is required to enable future mutual recognition and/or interoperability between member countries.	Collaboration on work already underway around interoperability/mutual recognition.	Definition of a set of principles which guide interoperability and mutual recognition.

## Findings

Digital identity continues to be a critical enabler for DIWG member countries. An international scan of working group member countries found that:

- Digital identity continues to demonstrate significant benefit, with increased uptake, new and valuable use cases emerging in response to and recovery from COVID-19,
- Government-led digital identity systems are mostly aligned to a centralised or hybrid identity model whilst also drawing on elements of self-sovereign and decentralised identity models where appropriate,
- Most systems are underpinned by existing and new policy, legislation and trust frameworks,
- Interoperability is a key consideration of most systems and enabled by design, and
- For many systems, the technical settings are in place to support mutual recognition of digital identities and broader interoperability.

DIWG member countries each have relevant policies and/or legislation which cover their respective approaches towards digital identity, captured through policy, legislative and trust frameworks governing the digital identity systems. For most, trust frameworks and digital identity systems were implemented using existing government policies and legislation as a foundation, for example existing privacy legislation, and broadly align to ISO standards (as defined by the International Organisation for Standardisation), European Union (EU) standards (as defined through the eIDAS regulation) or industry best practice. A similar model was found for technical settings across digital identity systems.

In most cases, government led initiatives have been designed with mutual recognition and interoperability in mind, even where international interoperability has not been considered as an immediate use case.

Digital identity has enabled member countries to respond to and recover from COVID-19, including to rapidly develop and deliver government information, services and support to verified people and businesses. In some countries Digital identity has also supported the rollout of COVID-19 vaccinations, enabling the secure sharing of information and verification of status across the population.

These benefits appear largely independent of the digital identity model used. Generally, they appear to be more dependent on the maturity and uptake of the respective digital identity system pre and during pandemic. In many cases, COVID-19 has in fact accelerated the use of digital identity, with access to digital services becoming critical as countries managed their response to the pandemic.

In the future, digital identity initiatives could also feasibly enable broader recovery, such as a strong, mutually recognised and interoperable COVID-19 vaccination certificate to enable greater international movement, including for trade and travel. Digital identity could also enable the international interoperability of digital wallets so people can use their various identity attributes and credentials across borders, such as their digital driver's license, education and qualifications and health information.

DGX presents a great opportunity to enable mutual recognition and interoperability between digital identities and infrastructure to support cross-border use cases and benefits. This requires several foundational activities, including:

- The agreement of a common language and definitions across digital identities,
- Assessment and alignment of respective legal and policy frameworks, supported by appropriate consensus on identity standards and cross-border application, and
- Interoperable technical models and infrastructure.

This report provides an initial alignment of digital identity definitions across DIWG member countries. It also proposes a set of principles to enable future mutual recognition and/or interoperability of digital identities. These are intended to inform the basis of a consistent taxonomy to support formal and information international collaboration around broader mutual recognition and interoperability of digital identity systems and infrastructure. These principles can be considered and applied whether mutual recognition is approached from a formal or informal perspective.

In parallel to this working group, this report recognises that a range of bi- and multi-lateral engagement is underway to enable mutual recognition and interoperability, including between DIWG member countries. The language and principles in this report aim to assist these engagements.

## 2. Current digital identity landscape (FA1)

Focus Area	Approach	Deliverable
<b>FA1:</b> Understand how digital identity is being used, including where free trade or similar agreements exist, and how these might enable mutual recognition and/or interoperability.	International scan of DGX DIWG member countries to understand how digital identity is being used.  Scan and alignment of DIWG digital identity definitions and taxonomies.	Description of DIWG member country digital identities and infrastructure and use cases.  Definition of a common digital identity language and set of definitions.

An international scan was used to understand the current digital identity landscape and how it is being used across DIWG member countries.

This was achieved through the distribution of a survey to representatives of working group member countries. The survey aimed to capture information on the respective country's digital identity model and approach, policy and legal settings, technical settings and any other relevant considerations in the delivery and use of digital identities.

The international scan identified that there are two main digital identity approaches taken by DIWG member countries using centralised and/or hybrid models, whilst also drawing on elements of self-sovereign and decentralised identity models where appropriate. The different approaches recognise the different contexts, social settings, and requirements of the countries. In most cases, these models are underpinned by the policy, legislation, trust frameworks and technical settings required to operate the systems.

Though there are differences between the approaches and digital identity systems, most have been designed with mutual recognition and interoperability in mind and are based on comparable standards. While this should enable progress on interoperability, there will likely be policy, legislation, trust and technical considerations that need to be worked through. Similar challenges are likely to be encountered when broadening interoperability to other government and private sector-led digital identity initiatives.

### 2.1 Digital identity models

The working group considered three recognised digital identity models that form the basis of most digital identity systems: centralised, self-sovereign and decentralised digital identity models. While these models may appear conceptually distinct, in application they exist along a continuum of centralisation of identity authority in the trust framework and digital identity system, visualised in Figure 1 below. This leads to a range of hybrid digital identity approaches which draw on the principles and components of one or more of these three models.

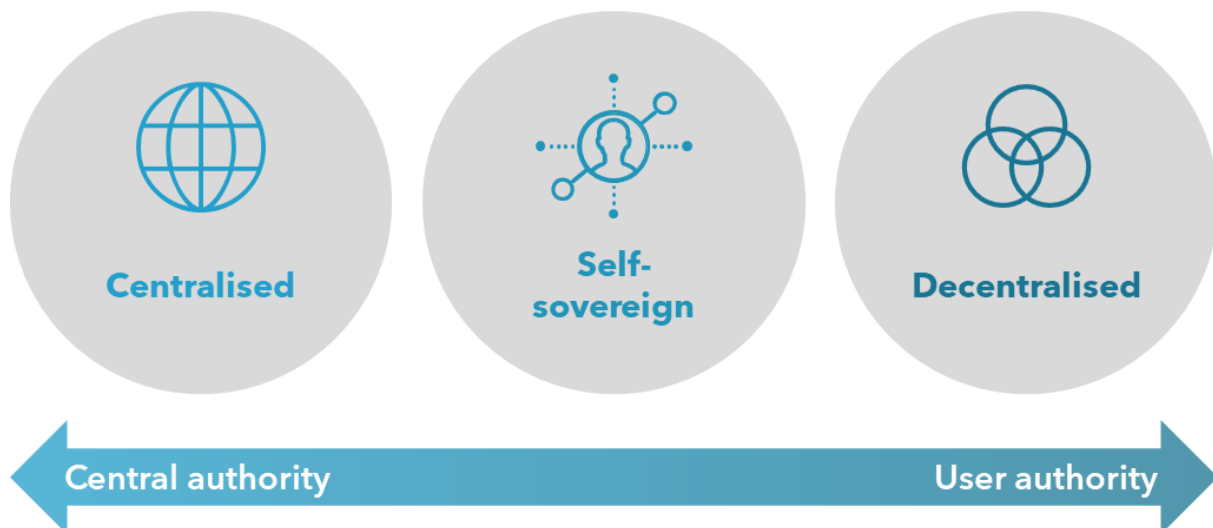


Figure 1 - Digital identity models.

The international scan identified that DGX DIWG member countries primarily align to two digital identity approaches: a centralised government-led digital identity approach, and a hybrid approach in partnership between the private sector and government. These approaches used by member countries are summarised in Table 2 below.

Table 2 - DGX DIWG country digital identity models.

DGX DIWG country	Digital identity approach
Australia	Hybrid digital identity approach, led by government with participation by private sector identity and credential providers.
Canada	Centralised approach, led by government with individual programs between federal and provincial governments.
Finland	Hybrid approach, led by government running for public services supported by multiple private sector eID providers.
Israel	Centralised approach led by government.
New Zealand	Hybrid approach, led by central government with additional private sector identity providers.
Singapore	Centralised approach led by government.
The Netherlands	Centralised approach led by government for citizens, hybrid approach in partnership with the private sector for businesses.
United Kingdom	Hybrid approach, led by central government with additional private sector identity providers.

The approaches differ most significantly in the participation of identity providers in the respective trust framework and digital identity systems:

- The centralised government approach generally offers only one identity provider, authorised and delivered by the central government.

- The hybrid approach allows people and businesses a choice in identity provider, generally between a central government provider and private sector identity providers, with identity information validated and shared between requesting parties and identity providers through an identity exchange.

Within both approaches, the international scan identified that digital identity systems and infrastructure is developed using principles of centralised and self-sovereign identity model. Most member countries drew on elements of each of these models.

A centralised identity model generally provides a single identity provider which is authorised and delivered by the central government. This centralised government provider can then provide parties confirmation of a valid identity when requested by the user to share with other parties.

A self-sovereign identity model generally provides multiple identity providers across the central government and non-government providers, allowing people and businesses to store and manage their identities and data on their own devices. When required to validate their identity the user is then able to provide this data instantly, also achievable through other, hybrid models.

The self-sovereign identity model allows users to have greater control of their identities and personal data and reduces the instances of unintended sharing of personal data, achieved without relying on a centralised database. The self-sovereign identity model is one way to achieve these objectives, alongside other hybrid and decentralised models.

The working group recognised there are international examples of a decentralised identity models, elements of which are also used through hybrid approaches. This is generally delivered through multiple identity providers and increases people's individual control over their digital identities so that people can use different parts of their identity and attributes as they need.

The European Digital Identity framework, which will be required by all member countries, will use a decentralised approach to offer people and businesses a digital identity wallet containing their national digital identities and other personal attributes. While this will take a decentralised approach to connect digital identities across member countries, each member country itself may follow a centralised, self-sovereign, decentralised or hybrid digital identity approach as described above. At this stage, this proposes new legislation to be set by EU Commission that needs the support of both EU member state national governments and the EU Parliament. It also requires each of the EU member state initiatives to be made technically interoperable through national coordination points. Once implemented, this model could, for example, form the basis of the European Commission's Digital COVID Certificate framework, a decentralised approach to connect the issuance and use of certificates across all EU member states, as well as other digital wallet uses.

While the international scan identified the approaches of government-led digital identity initiatives, the working group recognised there are other non-government-led approaches and initiatives across the economy, such as the private sector through banks and financial institutions. This report focuses on government-led digital identity initiatives, however many of the findings and work towards mutual recognition and interoperability may be applicable across other initiatives.



## 2.2 Policy and legal settings

The scan identified that DIWG member countries each have relevant policies which cover their respective approaches towards identity management standards, requirements, and specifications, as well as standards for privacy, data and security, and system oversight. These are often captured through the various trust frameworks governing the digital identity systems.

Most trust frameworks and digital identity systems were implemented using existing government policies and legislation as a foundation, including existing requirements to ensure:

- privacy of people and their personal information, such as the Personal Data Protection Act (Singapore) and various Privacy Acts (including Australia and New Zealand),
- the identity management standards and requirements for government services, such as the Standard on Identity and Credential Assurance (Canada), National Plan for Safe Identification policy (Israel) and ISO29115 standards,
- sovereignty and security of data, such as Public Sector Governance Act (Singapore), General Data Protection Regulation (EU and UK) and ISO27001 standards, and
- regulation, oversight and operation of digital identity systems, across various audit and oversight functions, including EU eIDAS Regulation (EU).

While specific to the respective government requirements, these policies and legislation were generally based on ISO standards, EU standards or industry best practice, which are broadly aligned. Therefore, there are many consistencies across the various trust frameworks and digital identity policies between the working group member countries. Across most member countries, trust frameworks, policy and legislation have been developed with future mutual recognition and interoperability in mind, opening up the broad opportunity to achieve interoperability between the digital identity systems and infrastructure.

However, differences in legislation and specific government requirements may also impact mutual recognition and interoperability. This includes issues such as differing views on or misalignment between privacy and personal data legislation, security and data sovereignty across borders, and the role of government and the private sector in digital identity systems. These appear to be generally dependant on individual countries and their domestic context; some countries are more able to share data between countries, such as member states of the EU, while others are less able. In many cases, additional legislation was created and passed to support the initiatives and digital transformation or is currently being developed and consulted on. This was increased further during the COVID-19 pandemic, with the expedited introduction of legislation and temporary legislation to allow governments to respond to the pandemic. The new legislation supported the transition to digital government services, which were underpinned by the requirements of having digital identities for citizens.

In addition to supportive policy settings and legislation for digital identity, each member country had set up external oversight and auditing functions to oversee the digital identity initiatives, which continue to review and ensure the policies continue to be robust and meet requirements. These also support compliant participation in the system.

## 2.3 Technical settings

The international scan identifies that DIWG member countries have broadly implemented digital identity systems which, at least in theory, provide the technical settings required to support domestic and cross-border interoperability.

The working group recognised that a common understanding of the technical landscape is required to determine how digital identities could be used and recognised freely across countries. A universal set of definitions and taxonomies for digital identity will foster interoperability and allow for seamless collaboration between governments, private enterprise, and citizens.

Beyond definitions and taxonomies, a common set of technical standards, architectural models and authentication must be developed and agreed upon. This will lay the foundation of a global digital identity system, allowing countries, businesses, and citizens to realise the benefits of seamless verification and authentication of people across borders.

Three separate approaches have been detailed in the responses from member countries towards creating a common and interoperable technical landscape:

- Consistently using the ISO standards developed around digital identity and digital services. These standards are used as the foundation to develop services and ensure consideration of the security, usability, and architecture requirements. The scan identified that ISO standards are in use across many member countries.
- Maintaining a digital first and open standards approach. This involves the countries being as open as possible surrounding data, definitions, and technology. It allows all potential collaborators to identify relevant standards and practices to enable efficient integration and cross board application of future solutions. An example of this can be seen through Singapore's cloud first approach and open API product database.
- Modelling the regulations and technical settings outlined by the European Union. This allows countries the opportunity to adopt technical setting used by the 27 member states to integrate and create interoperability of digital identity with multiple countries immediately. To achieve this a model following the eID and eIDAS is required, however this is not fully mature and requires alignment internationally.

Member countries also recognised that identity assurance and proofing requirements referencing open standards are important to enable mutual recognitions and establish a uniform baseline to support interoperability of digital identity systems. The survey identified that many DIWG members used broadly consistent identity assurance and proofing levels, including those based on ISO standards, National Institute of Standards and Technology (NIST) Electronic Authentication Guidelines and Identity Assurance Levels and Canadian Standards on Identity and Credential Assurance,

These approaches and technical settings align to the draft digital identity interoperability principles proposed in this report.

### 3. DIWG experiences and COVID-19 use cases (FA2)

Focus Area	Approach	Deliverable
<b>FA2:</b> Share governments' experiences with digital identity through use cases, research findings and benefits, with a focus on the COVID-19 response and recovery.	Capture digital identity experiences and use cases with a focus on the COVID-19 response and recovery and alignment with free-trade or similar agreements.	Description of supporting use cases across DIWG member countries in COVID-19 response and recovery.

The working group recognised that digital identity was, and continues to be, a critical enabler for DIWG member countries to respond to and recover from COVID-19. Digital identities and infrastructure enabled governments to rapidly develop and deliver government information and services with confidence to verified people and businesses, support the rollout of COVID-19 vaccinations, and manage vaccination status across the population.

Experiences and use cases were captured through this report to share relevant insights and benefits of digital identity systems, with a focus on the COVID-19 response and recovery. These complement the current digital identity landscape in Focus Area 1.

#### 3.1 Australia

The Australian Government's Digital Identity system is transforming the way that Australians and Australian businesses engage with the government services they use every day.<sup>1</sup>

Digital Identity is supported by the Trusted Digital Identity Framework (TDIF), which details the rules and requirements for governance, accreditation and operation of all parts of the system. This ensures a safe and secure digital identity system for the Australian economy. The TDIF has been developed to be interoperable both domestically and at the international level and is based on international and industry best practice and standards and builds on layers of existing policy and legislation, including privacy related rules applying to data entering the digital identity system.

As of December 2021, the Australian Government's Digital Identity system is used by over 6 million individuals, saving them time and money, and helping almost 1.3 million businesses to access over 80 Government services, improving their efficiency and productivity. The system was used by most Australian businesses to access services and support during the COVID-19 pandemic. It was also integrated with the Australian Government's primary individual portal, myGov, to support individuals to access government services and support.

The system provides a way for people to log in to myGov, the primary portal for individuals to access Australian Government digital services, using their government-led myGovID digital identity. myGov also provides access to people's COVID-19 Vaccination Certificates, which supports Australia's recovery from the COVID-19 pandemic and may become essential for reopening international borders. Strong authentication and verification methods like the digital identity system guard against fraud and ensures the person applying for the certificate is who they say they are. In the future, this could feasibly enable a strong, internationally

---

<sup>1</sup> For more information on the Australian Government's Digital Identity system see [digitalidentity.gov.au](https://digitalidentity.gov.au).

recognised and interoperable COVID-19 vaccination certificate to support international travel through integration of a person's Digital Identity and digital wallet.

The Australian Government has also recognised that Digital Identity can also provide essential support in the case of other national and international disasters, demonstrated during the 2019-2020 Australian bushfires. Once a Digital Identity has been created, it removes the need to find identity documents which may have been lost, such as birth certificates or passports, allowing for faster access to government services and relief payments.

As Australia's digital economy expands, an interoperable digital identity system will unlock more and more services and allow the system to be used across government and private sector services. Once people have created a digital identity, they will be able to reuse it across any government and commercial services that are connected to the Digital Identity system. The Australian Government is developing legislation to support a broader rollout of Digital Identity to additional states and territories, and the private sector.

## 3.2 Singapore

Singpass, Singapore's National Digital Identity (NDI), is one of the Smart Nation strategic national projects.<sup>2</sup> As a foundational digital infrastructure, the NDI is critical to achieving Singapore's vision of improving lives of citizens, creating opportunities for businesses, and transforming the capabilities of government agencies. Singpass offers Singapore residents greater confidence, convenience and accessibility when transacting with the Government and private sector, online and in person.

Singpass was introduced in October 2018 and enhanced with more recent features such as Digital IC, facial verification and digital signing. It enables access to more than 1,400 services offered by over 340 public and private sector organisations. Of the 4 million Singapore residents on Singpass, over two-thirds (over 2.7 million) are on the Singpass app with over 90% of them using the app at least once a month, making this everyday app one of the most downloaded digital applications launched by the Singapore Government.

NDI enables Businesses and agencies to create new value-added services for Singapore residents through Singpass' application programming interfaces (APIs).<sup>3</sup> This currently includes the Singpass app, Authorise, Myinfo, Myinfo Business, Login, Verify, Face Verification, Sign and Notify. Residents can now access digital services, retrieve their personal information, digitally sign documents and remotely authorise transactions on their Singpass app without using passwords or manually filling forms.

Digitalising everyday transactions saves time for both residents and businesses. People can transact securely and safely online, without submitting hardcopy documents. These streamlined processes result in quicker approvals for applications. The digital capabilities built in the NDI ecosystem offer an exciting glimpse into the possibilities and future of Singapore's Smart Nation initiative – one enabled by the trusted national digital identity.

Singapore's NDI supported the digitisation of COVID-19 contact tracing processes, including through SafeEntry to enable authorised contact tracers to quickly obtain identity information of visitors to a physical location. This information is used as a credible reference to uncover locations visited by confirmed cases, identify possible clusters and, identify locations for

---

<sup>2</sup> For more information on the Singapore Government's Singpass see [singpass.gov.au](https://singpass.gov.au).

<sup>3</sup> APIs are listed in the Singpass API Developer and Partner Portal [api.singpass.gov.sg](https://api.singpass.gov.sg).

deep cleaning. To use SafeEntry, users give their consent to the transfer of personal information upon scanning a SafeEntry QR code to check in whenever they visit a location.

By using technology and digital contact tracing tools, the time taken to identify, and quarantine close contacts reduced from an average of 4 days to less than 1.5 days.

COVID-19 has reinforced the urgency for digital literacy and accelerated Singapore's broader digital transformation. Despite having disrupted physical interactions, Singaporean residents continued to use their Digital Identity to have seamless and secure access to government and private sector services.

Digital readiness has enabled Singapore to minimise disruptions and respond quickly to the pandemic. There were over 170 million transactions facilitated by Singpass in 2020, which is more than a 60% jump from the previous year as residents conducted more of their transactions digitally during the pandemic.

The increased adoption presents an opportunity to extend NDI's suite of services beyond its current individual and business offering. NDI is progressively building a mobile version of the Corporate Digital Identity for businesses. With the increasing volume of electronic corporate transactions, we aim to offer a wider range of services through the mobile application like enabling corporations to leverage our Sign products to conduct secure digital signature transactions.

Moving forward, a wider variety of transactions will be conducted digitally, from verifying identity and health certificates to cross-border data transfers. The National Digital Identity is expected to support a growing range of use cases for digital identity. NDI is exploring new initiatives that build on the principle of adopting open standards which support interoperability with different digital services and international partners.

### **3.3 United Kingdom**

The UK Government's GOV.UK Verify is a government-led federated digital identity solution, supported by certified private sector companies as Identity Providers (IDPs). The scheme has been in operation since 2016; however, it is due to be retired in April 2023. In the UK, the use of digital identities is not mandated, as well as what digital technologies or delivery models should be used.

The UK Government is in the process of building a single sign-on and identity checking system that will replace GOV.UK Verify and other government digital identity schemes over time. The UK Government is also in the process of developing a Trust Framework for digital identities and attributes, which provides high level guidance on what standards schemes sitting under it should be using; however, it is not prescriptive on how these schemes are delivered. This is in line with the Government's commitment to realising the benefits of digital technologies without creating ID cards.

GOV.UK Verify saw a significant increase in sign-ups during the COVID-19 pandemic as more people looked to use government services online. It has played a critical role in providing access to key services, such as Universal Credit – a welfare payment made to people on a low income, out of work or unable to work.

The UK Government is building on the lessons learned from GOV.UK Verify, as well as multiple external reviews of the service, to develop the new login and identity assurance system. This is an ambitious cross-government programme that provides an opportunity for genuine co-design and co-development. The programme will seek to reuse or repurpose

assets created by GOV.UK Verify where doing so is more efficient or effective than starting from scratch.

The Government Digital Service (GDS) in the UK has also published the Good Practice Guide (GPG) 45, which serves as the UK standard for checking someone's identity. The guidance aligns with certain international standards and regulations, including the Pan Canadian Trust Framework Model and the EU electronic identification and trust services (eIDAS).

### 3.4 Canada

The Canadian Federal Government is fostering the Canadian digital identity ecosystem and supporting a pan-Canadian approach which accepts trusted digital identities issued by the sub-national jurisdictions (e.g. Provinces and Territories who have jurisdiction and the authoritative data sources). This approach aims to enable access to federal programs and the services offered to Canadians and businesses (e.g. social benefits and tax). This is supported by the Public Sector Profile of the Pan-Canadian Trust Framework.

Currently, there is no federal digital identity program, and sub-national programs are not ubiquitous and are at varying levels of maturity, ranging from very mature to non-existent. Where in place, the federal government is leveraging trusted digital identity programs from the provinces and territories to enable access to online federal programs.

The current approach in Canada is leveraging existing centralized systems (supported by federal government), with federated approaches (relying on provinces and territories for trusted digital identities). Canada also continues to foster innovation by exploring the emergence of newer decentralized approaches to digital identity, so that they approaches can be applied in Canada, as appropriate.

### 3.5 Finland

All public sector e-services in Finland which require strong authentication are connected to the public sector eID portal.<sup>4</sup> Through this, eID can be used to access around 900 e-services. Use of the common public sector eID portal, provided by the Agency of Digitalisation, is mandated by law for public sector e-services in Finland.

In a country of 5.5 million people, the public sector eID portal has around 18 million authentications per month, growing from 13 million per month in the previous year. Almost all adults in Finland have at least one government accepted eID (such as a bankID, SIM card-based certificate issued by mobile operators, or ID card).

COVID-19 triggered a reduction in physical services provided by government agencies and municipalities, with most service delivery staff also working from home. This significantly accelerated the uptake of e-services. While it was an early adopter of digital identity in Finland, the pandemic also expanded the use of eID in the Finnish health sector. This included registration through a COVID-19 mobile app, getting a COVID-19 test time, booking a vaccination, and accessing COVID-19 vaccination certificates.

Finland is moving towards self-sovereign identity frameworks, aligning with the EU Commission. Nationally, Finland is pursuing an ambitious schedule to introduce self-

---

<sup>4</sup> For more information on the Finland Government's eID see [kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/electronic-identification](https://kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/electronic-identification).



sovereign identity wallets, to be available for people to provide various attributes, such as vaccination certificates, by 2023.

### 3.6 New Zealand

People's identities are currently digitally verified and/or authenticated in different ways in New Zealand (NZ). The government operates RealMe services, which include a single login for citizens to access government services, and a verified identity for citizens to prove who they are digitally.<sup>5</sup> Additionally, local, and international identity providers offer bespoke digital identity solutions, though New Zealand does not have dedicated regulation of these private sector digital identity solutions.

The RealMe services currently enables people to access a number of public and private services with their RealMe verified identities, such as access to student loans and allowances.

COVID-19 highlighted the importance of digital identity for ensuring access to essential services. This increased demand of digital identity services, for example some agencies were unable to provide in-person services during lockdowns. The experience responding to COVID-19 has provided an opportunity to accelerate creating a strong digital identity system. For example, some agencies are incorporating the need for better digital identity solutions in their service transformation plans.

To support the growth of trusted digital services, New Zealand is currently developing an opt-in Digital Identity Trust Framework. As part of this work, NZ has made international commitments to mutual recognition and the development of the Digital Identity Services Trust Framework in line with trust frameworks being developed in Australia, the UK and Canada. Additionally, under the Digital Economy Partnership Agreement (DEPA) with Singapore and Chile, New Zealand will endeavour to promote interoperability between their respective regimes. NZ is looking to introduce legislation later this year and is developing the trust framework rules in parallel.

### 3.7 The Netherlands

The Netherlands' DigiID is a centralised, government-led digital identity initiative which supports citizens to access government and public services digitally.<sup>6</sup> DigiID has one of the highest uptakes of a government-led digital identity initiative globally, used by over 80% of Dutch citizens. The Netherlands also provides eRecognition for businesses to access public services, a hybrid initiative in partnership with the private sector.<sup>7</sup>

DigiID currently supports Dutch citizens to access over 650 public and semi-public services digitally and is practically required by citizens to access the services they need. COVID-19 increased the use of DigiID and accelerated the uptake of stronger levels of identity verification as people needed to access more services digitally. DigiID has also been used for people to access COVID-19 tests and vaccinations throughout the pandemic, and more recently to provide a health credential for people to prove their vaccination status.

The Netherlands intends to expand the DigiID system across more services and extend its use to the private sector, using the concept of a 'digital base identity' as the authoritative

---

<sup>5</sup> For more information on the New Zealand Government's RealMe see [realme.govt.nz](https://realme.govt.nz).

<sup>6</sup> For more information on the Netherlands' Government's DigiID see [digid.nl](https://digid.nl).

<sup>7</sup> For more information on the Netherlands' Government's eRecognition see [eherkenning.nl](https://eherkenning.nl).

source and issued by the government. This digital base identity will include the minimum data that people need to prove who they are in societal transactions.

The Netherlands is also looking to broaden the use of DigID across more applications, including providing verified attributes and e-signing of documents. This will be enabled through legislation which will see the establishment of a digital base authority, led by the government, which supports the sharing of information across public and private sectors. By establishing the base digital identity, the government will create an authoritative source of reliable identifying data for individuals, thus creating the foundations for trust in the digital world.

The Netherlands has also been active in the development and participation in the eIDAS regulation to create interoperable digital identity initiatives across the EU and is progressing trials with Germany to establish mutual recognition and interoperability of digital identities and digital wallets.

### 3.8 Israel

Israel's National Identification System provides a way for 2 million registered Israeli citizens and residents to securely access the digital government services they need, including through the Government's MyGov portal.<sup>8</sup> The system, based on Israel's National Secure Identity Policy introduced in 2017, is anticipated to be expanded to all 6.5 million adult citizens and residents in the coming years.

The National Identification System currently supports people to register for an identity and access most government services digitally through the MyGov portal. It provides the levels of identity assurance people and Government need, including providing options for people to use their biometric passport or mobile application to prove who they are. The system is based on internationally recognised ISO standards and is anticipated to support future mutual recognition and interoperability. Currently, Israel is exploring compatibility with EU eIDAS standards and other international partners.

The COVID-19 pandemic significantly increased the uptake and use of Israel's National Identification System and digital government services through MyGov as more people moved to access services online. Registrations have doubled and the number of people using the system have increased from around 600 thousand to 2 million throughout the pandemic. Usage of the National Identification System and MyGov has increased threefold to 1.5 million per month.

The National Identification System extends Israel's previous Government Identification System, which was expanded in 2020 to more organisations across the economy including the health sector and local authorities. In the future, Israel is considering transitioning to a distributed digital identity through a digital wallet using blockchain technology, with a proof of concept currently underway.

## 4. Future mutual recognition and interoperability (FA3)

Focus Area	Approach	Deliverable
------------	----------	-------------

---

<sup>8</sup> For more information on the Israel Government's National Identification System see [login.gov.il](https://login.gov.il).



<b>FA3:</b> Understand what is required to enable future mutual recognition and/or interoperability between member countries.	Collaboration on work already underway around interoperability/mutual recognition.	Definition of a set of principles which guide interoperability and mutual recognition.
---	--	--

There is a great opportunity to enable both mutual recognition and interoperability between digital identity systems and infrastructure, both domestically and across borders. This will enable a range of use cases and unlock additional benefit from digital identity initiatives for governments, people, and businesses. This will also enable other use cases, including the use of trusted digital wallets internationally.

However, the working group recognised that both mutual recognition and interoperability are complex challenges that will take several years to achieve. They require policy, legal and technical alignment between government trust frameworks, digital identities, and infrastructure. Efforts to enable interoperability, such as the EU's eIDAS, show these challenges are significant to overcome.

The DIWG identified foundational activities required to enable both mutual recognition and interoperability of digital identities, including:

- The definition of a common language and definitions across digital identities,
- Assessment and alignment of respective legal and policy frameworks, supported by appropriate consensus on identity standards and cross-border application, and
- Interoperable technical models and infrastructure.

These activities, and interoperability more broadly, require agreements between member countries to make progress. These can take the form of free-trade agreements (FTA), memoranda of understanding (MoU), or similar structured agreements. These agreements can formalise the intent and achieve the outcomes required for mutual recognition of digital identities across borders, and interoperability of digital identity systems.

Ultimately, when applied this enables the benefits unlocked by both mutual recognition and interoperability to be realised, including more efficient government interactions, increased support for businesses operating across borders and simple, streamlined experiences for people travelling internationally. In the future, this could also feasibly enable broader recovery from COVID-19, such as strong, mutually recognised and trusted vaccination certificates to enable safer cross-border movement.

Various formal agreements currently exist or are being developed which involve DIWG member countries, such as:

- A digital economy agreement between Australia and Singapore, with a specific MoU for digital identity. This has the direct purpose of developing mutual recognition between participants by exchanging policies, technologies, information and human resources related to digital identity. A similar agreement exists between Australia and New Zealand.
- The Digital Economy Partnership Agreement between Singapore, New Zealand and Chile, a free trade agreement to work towards mutual recognition and making digital identity systems interoperable.
- The European Union (EU) Single Digital Gateway Act and agreement, which requires a range e-services including digital identity to be accessible for cross-border use by 2023. The eIDAS Act is also to be renewed across the EU to regulate a variety of e-

services including the verification of individuals and businesses online. In addition, Israel is assessing the potential to cooperate with this agreement.

- The 2021 free trade agreement between Australia and UK aims to promote compatibility between their respective digital identity regimes.
- An MoU between Israel and Estonia to progress mutual recognition and interoperability of digital identities.
- Nordic-Baltic Co-operation on eID, led by the Nordic Ministerial Council, aimed at improving eID mutual recognition and interoperability between Finland, Sweden, Norway, Iceland, Estonia, Latvia and Lithuania.

Beyond these formal agreements, the DIWG recognised there are a range of other initiatives intended to progress both mutual recognition and interoperability of digital identities and infrastructure and which member countries have contributed to. This includes:

- Targeted working groups, such as the European Self Sovereign Identity Group and Digital Nations ID Group,
- Enduring forums, including the DGX, OECD, ID4Good and the World Economic Forum, and
- Established frameworks, including the EU Interoperability Framework and World Bank's Digital Identity Practitioners Guide.

Many countries are also undertaking discovery and pilot activities on use cases to enable interoperability between digital identity initiatives.

Most countries are currently taking a risk-based and phased approach to mutual recognition and interoperability. The working group recognised the value of a common set of principles to guide mutual recognition and interoperability of digital identities and infrastructure. These would give regard to alignment of policy and legal frameworks, technical interoperability and standards. These principles could help to accelerate interoperability and realise potential benefits, including opening international borders for trade and travel in recovery from COVID-19.

Close attention needs to be considered for data management and the protection of personal information by considering existing internationally recognised principles or guidelines, including to consider privacy, transparency, fairness, and person-centred values. Other policy and legal frameworks will need to align between countries to enable sustainable interoperability of trust frameworks and digital identity systems, including global digital identity standards, identity assurance levels and liability frameworks. Interoperability also needs to consider the role of the private sector in digital identity systems, including a common understanding of the underlying business models and frameworks for liability between countries and the public and private sector.

## 4.1 Interoperability principles

An initial common set of interoperability principles were defined to describe the context in which mutually recognised digital identities can be designed and implemented. These have been adapted from the European Union Interoperability Framework<sup>9</sup>.

---

<sup>9</sup> European Union, 2017, 'New European Interoperability Framework: Promoting seamless services and data flows for European public administrations', Publications Office of the European Union, Belgium.

The principles aim to allow for a common understanding to guide future discussions on both mutual recognition and interoperability of digital identities and infrastructure. These initial high-level principles, outlined in Figure 2 and described below, are proposed to be adopted to drive collaboration and progress.

## Interoperability principles












-  **1 Openness**
-  **2 Transparency**
-  **3 Reusability**
-  **4 User-centricity**
-  **5 Inclusion and accessibility**
-  **6 Multilingualism**
-  **7 Security and privacy**
-  **8 Technology neutrality and data portability**
-  **9 Administrative simplicity**
-  **10 Preservation of information**
-  **11 Effectiveness and efficiency**

Figure 2 - Digital identity interoperability principles.

### Principle 1: Openness

All data should be freely available for use and reuse by others by default as relevant to trust frameworks and digital identity systems, unless restrictions apply such as for the protection of personal data, confidentiality or intellectual property rights.

### Principle 2: Transparency

Aligned public administrations, citizens and businesses can view and understand the administrative rules, processes, data, services and decision-making across digital identity systems.

This includes interfaces with internal information systems which facilitate the reuse of systems and data and securing the right to protection of personal data by respecting the applicable policy and legal frameworks for the large volumes of personal data of citizens held and managed by public administrations, including in digital identity systems.

### Principle 3: Reusability

Public administrations confronted with a specific problem seek to benefit from the work of others by default, assessing what is available and its usefulness or relevance to the problem

at hand and adopting solutions that have proven their value elsewhere, where this is appropriate.

This requires the public administration to be open to sharing and interoperability of trust frameworks and digital identity solutions, concepts, frameworks, specifications, tools and components with others, as aligned to Principles 1 and 2.

#### Principle 4: User-centricity

User needs are considered when determining which public services should be provided and how they should be delivered, and therefore user needs and requirements guide the design and development of public services and use of digital identity, aligned to the following expectations:

- A multi-channel service delivery approach, meaning the availability of alternative channels, physical and digital, to access a service, is an important part of public service design, as users may prefer different channels depending on their circumstances and their needs.
- A single point of contact should be made available to users, to hide internal administrative complexity and facilitate access to public services.
- User feedback should be systematically collected, assessed and used to design new public services and to improve existing ones.

#### Principle 5: Inclusion and accessibility

Inclusive delivery enables everyone to take full advantage of the opportunities offered by new technologies to access and make use of digital services enabled through mutually recognised digital identity, overcoming social and economic divides and exclusion. Accessibility ensures that people with disabilities, the elderly and other disadvantaged groups can use public services at service levels comparable to those provided to other citizens.

Inclusion and accessibility usually involve multi-channel delivery. Traditional paper-based or face-to-face service delivery may need to co-exist with electronic delivery. Inclusion and accessibility can also be improved by an information system's ability to allow third parties to act on behalf of citizens who are unable, either permanently or temporarily, to make direct use of public services, which may be enabled through digital identities.

#### Principle 6: Multilingualism

Public services should be available in the languages of the expected end-users. The number and type of languages is decided by users' needs and as required for the service to be inclusive and accessible. Interoperability of digital identities will need to consider languages across borders.

#### Principle 7: Security and privacy

Citizens and businesses must be confident that when they interact with public authorities, they are doing so in a secure and trustworthy environment and in full compliance with relevant standards and regulations.

Public administrations must guarantee the confidentiality, authenticity, integrity and non-repudiation of information provided by citizens and businesses, including through the creation and use of digital identities.

#### Principle 8: Technology neutrality and data portability

Public administrations should focus on functional needs and minimize technology dependencies, to avoid imposing specific technical limitations and remain agile to adapt to the rapidly evolving technology environment. Public administrations should provide for access and reuse of their public services and data irrespective of specific technologies or products.

Data must also be able to move and reused across different systems, which becomes even more challenging with cross-border interoperability.

#### Principle 9: Administrative simplification

Streamlining of administrative processes by improving them or eliminating any that do not provide public value. The implementation of digital identity systems and services should be supported by electronic means, including their interactions with other public administrations, citizens and businesses. Digitisation of public services should take place in accordance with the following concepts:

- Digital-by-default, whenever appropriate, so that there is at least one digital channel available for accessing and using a given public service.
- Digital-first, which means that priority is given to using public services via digital channels while applying the multi-channel delivery concept and the no-wrong-door policy, such as co-existing physical and digital channels.

#### Principle 10: Preservation of information

Legislation requires that decisions and data are stored and can be accessed for a specific time. This means that records and information in electronic form held by public administrations for the purpose of documenting procedures and decisions must be preserved and be converted, where necessary, to new media when old media becomes obsolete. The goal is to ensure that records and other forms of information keep their legibility, reliability and integrity and can be accessed as long as needed subject to security and privacy provisions.

#### Principle 11: Assessment of effectiveness and efficiency

There are many ways to take stock of the value of interoperable digital identity services, including considerations such as return on investment, total cost of ownership, level of flexibility and adaptability, reduced administrative burden, efficiency, reduced risk, transparency, simplification, improved working methods, and level of user satisfaction.

Technical solutions (e.g. cloud computing, internet of things, big data, software-as-a-service) should be evaluated when striving to ensure the effectiveness and efficiency of mutually recognised digital identities.

## 4.2 Common definitions and digital identity taxonomy

A common set of definitions and universal taxonomy for digital identity is critical to enable mutual recognition of digital identities and interoperability of digital identity systems.

An initial alignment of digital identity definitions was developed by referencing the definitions provided by DIWG member countries. A version of this alignment is attached to this report (Common Terms), intended to support ongoing discussions and collaboration through the working group.

The alignment found that while there appears to be substantial differences in the terms used across member countries and digital identity systems, most terms were able to be aligned to

common definitions. This forms a basis to allow for a common understanding to enable future discussions and alignment of digital identities and infrastructure.

This set of common definitions will evolve as trust frameworks and digital identities are further developed. In theory, this can be used to develop a universal digital identity taxonomy to support further collaboration and progress towards mutual recognition and interoperability.