Digital Identity and Verifiable Credentials in Centralised, Decentralised and Hybrid Systems

DGX Digital Identity Working Group - 2022

DIGITAL GOV EXCHANGE

Digital Transformation Agency

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 website@dta.gov.au.

Version: 1.5

1. Overview

About the DGX-DIWG

The Digital Government Exchange (DGX) Digital Identity Working Group (DIWG) was established in 2020 by representatives of the DGX international group. The purpose of the DIWG is to share experiences and opportunities for the use of digital identity initiatives, initially 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 current membership for the DIWG was formalised in February 2022 and is chaired by the Australian Government's Digital Transformation Agency (DTA), with members from Australia, Canada, Estonia, Germany, Israel, Japan, New Zealand, Singapore, the United Kingdom and the New South Wales government (as an observer). It is representative of many of the leading 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, supporting the opening of domestic and international borders for travel and trade.

Working Group Approach

In 2022, the objectives of the working group have been structured around: seeking to understand how digital identity in centralised, decentralised and hybrid systems are being used to support trustworthy, high-value verifiable credentials; and to understand what is required to enable mutual recognition and/or interoperability of these verifiable credentials between DIWG member countries.

These objectives recognise that the opportunity for mutual recognition and/or interoperability between DIWG member countries may have broader application across non-member countries and non-government digital identities, infrastructure and verifiable credential standards.

The working group recognises the opportunity to explore the various models of designing, governing and operating digital identity systems, combining these models with other international standards to enable new capabilities including digital wallets and trustworthy, verifiable credentials for use within and across economies. These are captured through the use cases and experiences of DIWG member countries.

Limiting the working group's scope to verifiable credentials has allowed this topic to be explored in greater depth, building on the findings and prior discussions from 2021.

Increasing adoption of government-led digital identity services during COVID-19 lockdowns amongst DIWG member countries has triggered a corresponding increase in the demand for digitisation (including low- or no-contact transactional activities) throughout respective economies.

Opportunities for adoption and reuse of existing digital identities for identity-adjacent activities are increasing, with various non-government sectors seeking to build on established standards, systems and frameworks created through prior investments in policy, legislation and digital infrastructure.

DIWG member countries are examining how existing policies, legislation and standards used for their digital identity systems may also need to evolve to align to, or support emerging international standards (for example ISO, W3C and new proposed changes to eIDAS).

Separate to this working group, bi- and multi-lateral engagements have been established and are underway to enable mutual recognition and/or interoperability of digital identities and digitally issued credentials, including between DIWG member countries. The language and principles in this report aim to assist these engagements.

What is a verifiable credential?

Credentials in the physical world might consist of:

- Information related to identifying the subject of the credential (for example, a photo, name, or identification number)
- Information related to the issuing authority (for example, a city government, national agency, or certification body)
- Information related to the type of credential (for example, a Dutch passport, an American driving license, or a health insurance card)
- Information related to specific attributes or properties being asserted by the issuing authority about the subject (for example, nationality, the classes of vehicle entitled to drive, or date of birth)
- Evidence related to how the credential was derived
- Information related to constraints on the credential (for example, expiration date, or terms of use).

Examples include education qualifications, healthcare data, immunisation records and driver licences.

A verifiable credential can represent all of the same information that a physical credential represents. The addition of technologies such as digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts.[1] Both verifiable credentials and their presentation can be transmitted rapidly, making them more convenient than their physical counterparts when trying to establish trust at a distance.

[1] Verifiable Credentials Data Model v1.1. 2022. Verifiable Credentials Data Model v1.1. [ONLINE] Available at: https://www.w3.org/TR/vc-data-model/. [Accessed 23 August 2022].

Findings

Digital identity continues to be a critical enabler for DIWG member countries and approaches to verifiable credentials are rapidly evolving. An international scan of working group member countries identified findings which can be grouped into three distinct themes:

Design

1. Existing government-led digital identity systems are increasingly drawing on elements of decentralised architectures to support the issuance, storage, and presentation of verifiable credentials across economies.
2. The role of digital wallet providers in the digital identity system is essential. Wallet proliferation is emerging as a potential usability and security risk, irrespective of the accreditation and standardisation approaches adopted at a country level.
3. The market for distributed and decentralised technologies used for storage and integration of these cryptographically-signed materials is maturing – common patterns for implementation at a national scale have not yet been established.

Policy

4. High-value, high-volume use cases for verifiable credentials anchored to digital identities are primarily clustered around the employment, healthcare, finance and professional sectors.
5. EU directives and regulations requiring the availability of digital identity wallets for all citizens who want one by 2023 have increased the expectations of scalable digital identity systems for verification and authentication activities used during issuance of credentials to be stored in digital wallets.
6. COVID-19 proof of vaccination certificates have altered the expectations of individuals' and businesses' acceptance and use of digitally presented permissions and credentials.

Standards and interoperability

7. Broad alignment with digital identity standards and levels of assurance within and between member countries has been a foundational pre-requisite for progressing international interoperability pilots using verifiable credentials.
8. Technical standards of verifiable credentials at a whole-of-economy or global level are still maturing but are generally being developed 'in the open'.

Digital identity models

In 2022, 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. Member countries reported (Table 1) that they aligned with either a centralised government-led digital identity approach, or a hybrid approach in partnership between the private sector and government.

Other than the United Kingdom, who have established 'One login for Government' to replace 'GOV.UK Verify', no countries had reported a significant shift in their existing models over the last 12 months.

Table 1 - DGX DIWG country digital identity models.

DGX DIWG country	Digital identity approach
Australia	Hybrid digital identity approach, led by national government with participation by private sector identity and credential providers. State governments progressing parallel, compatible systems with expectation to federate for interoperability.
Canada	Hybrid approach, that includes federal, provincial and territorial governments and private sector as identity and credential providers. Exploring the verifiable credentials model to enable digital services across government and the economy.
Estonia	Centralised identity management approach, led by government running for public services supported by multiple private sector eID providers.
Finland	Hybrid approach, led by government running for public services supported by multiple private sector eID providers.
Israel	Centralised Identity approach led by government. Adoption of eID-compatible and e-authentication standards and frameworks. Objective of becoming a full national system as local government joins the central scheme. Piloting with Distributed Identity and Verifiable Credentials.

New Zealand	Hybrid approach, led by central government with additional private sector identity providers.
Singapore	Centralised approach led by government.
United Kingdom	Hybrid approach, led by central government, building ‘One Login for Government’, an in-house identity service, with support from the private sector. This is underpinned by the UK digital identity and attributes trust framework, a set of rules and standards to govern digital identity and attribute solutions for identity service providers in the wider economy.

1.1 Verifiable credential governance models

The international scan identified that DIWG member countries have varying levels of adoption and employment of verifiable credentials with similar variance in levels of governance models.

Most established systems are operating within existing governing structures, with those nations within the European Union soon to enjoy the benefits of the European Digital Identity Framework.

Member countries all recognised that any work within the verifiable credentials space is moving at speed and is inherently broad in scope with governance needing to maintain pace with policy developments.

1.2 Technical settings

Previous international scans across DIWG member countries indicate that the technical settings of digital identity systems theoretically support domestic and cross-border interoperability.

Consistent use of international, open and interoperable standards for digital identity (including the use of comparable identity proofing standards) are well established – these standards enjoy high levels of visibility, adoption and currency, with generally mature approaches to international standards governance and they present a strong opportunity for technically-interoperable digital identities.

However, best practice approaches to implementation and example scalable architectures are not yet widespread for verifiable credentials – the ‘general purpose’ nature of verifiable credentials has few tightly-defined implementations for credentials outside the driver licence scenario. Countries may recognise the validity of an individual’s digital identity but may not have technically bridged the gap necessary to recognise, understand, and trust a digital credential being presented to them by that individual.

2. Current digital identity and verifiable credentials landscape

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

Prior international scans in 2021 found that DIWG member countries had primarily deployed centralised and/or hybrid models whilst drawing on self-sovereign or decentralised identity models as appropriate.

Having established foundational digital identity systems for their respective countries, DIWG members had begun exploring how best to use those capabilities to underpin sectors and use cases where verifiable credentials were seen as desirable and feasible, capitalising on existing investments in, and adoption of, policy, legislation, trust frameworks and infrastructure.

Building on these foundations, domestic interoperability of verifiable credentials for some member countries has begun to appear as a realistic milestone.

Whilst some well-established standards exist for individual use cases (for example, ISO/IEC 18013-5 mobile Driver's License), consistent technical implementations of general use cases (for example, those using the W3C-VC approach) relying on trustworthy digital identity service providers during issuance is yet to become standardised, widespread, or well documented.

For example, verifiers in one country relying on the presentation of a credential by an individual from another country not only need to be able to consume and process that presentation within their technical systems, but they also need to know that:

1. the individual presenting that credential is who they say they are (using a level of identity proofing appropriate for the service / product being requested)
2. the credential has been issued by an appropriate and trustworthy organisation within that country (it is suitable for the service / product being requested)
3. an acceptable level of evidence was provided by the holder prior to it being issued

Driver's Licenses are one such example where approaches to mutual recognition are well-established. However, the digital presentation of that licence may not be suitable or acceptable when accessing products or services unrelated to a holder's ability to drive and/or rent a car in other international jurisdictions.

Outside the public sector, the willingness and ability of verifying parties to process and accept digitally identity-anchored verifiable credentials from other jurisdictions remains inconsistent. Beyond government service use cases, larger, multinational companies (for example, hotel and car rental chains) may be better equipped to initially support VC-based use cases geared around digital driver licences, with digitally mature tertiary institutions and larger employers positioned to follow, leveraging trustworthy academic qualifications and professional licences.

2.1 Australia - Federal

The Australian Government's existing Digital Identity system uses a federated model, supporting several levels of identity proofing when accessing government services and payments online. Whilst Digital Identity uptake is comparatively high (approximately 30% of eligible population), reuse of these Digital Identities for government service delivery is low (average 1.2 usages annually).

Current policy settings permit relying parties to leverage a user's digital identity attributes to issue credentials. A variety of projects are in development or are being proposed to store government issued credentials in device native or state-government wallets and applications (for example, a COVID-19 vaccination certificate issued by the Department of Health). Other digital versions of presentable documents may reside in dedicated applications (for example, a digital Medicare card presented in a standalone Medicare app).

Some Australian jurisdictions (for example, New South Wales, Victoria) are conducting public pilots using existing state-based government apps as digital wallets for credentials. Use cases have been focused on employment and education sectors (for example, applying for new jobs, working with vulnerable people).

Cross-jurisdictional use cases are emerging where citizens may need to present credentials issued by the Commonwealth government (for example, a Tax File Number, Medicare number and tertiary qualifications) alongside credentials issued by one or more state-level jurisdictions (for example, driver's licence, working with vulnerable people, professional qualifications). Multi-jurisdiction consistency is expected to better support worker and student mobility, both domestically and internationally.

No single wallet is currently capable of holding all these credentials simultaneously, potentially negatively impacting the user experience and the cost imposed on verifying entities.

Australia's Trusted Digital Identity Framework is updated regularly – the responsible agency is considering including revised roles, functions and vocabulary to better align with those used by the W3C-VC standard and better support potential Verifiable Credential constructs. Related legislation focuses on the protection of users' privacy and ensuring appropriate oversight of the national system but does not preclude the establishment of hybrid architectures combining the existing federated model with a decentralised approach to verifiable credentials.

Within Australian jurisdictions, there is a broad recognition and support of the Commonwealth's central digital agency in coordinating changes to accreditation, technical and governance standards to support domestic interoperability of digital identity systems and associated touchpoints when issuing verifiable credentials, with the expectation that these approaches will position Australia for international interoperability.

Australia – New South Wales

New South Wales (NSW) is Australia's most populous jurisdiction, and currently enjoys a near-total penetration rate of their government app, ServiceNSW. Adoption spikes were observed with the availability of COVID-safe check-in functionality and the availability of Digital Driver Licences within the app. Users can also choose to create a digital identity at varying strengths with their MyServiceNSW Account, relying on existing government-issued physical documents for verification.

Once a strong digital identity has been established, users can add the digital equivalents of these documents, including other verified profile details (for example, mobile number, date of birth, email address) as foundational steps to adding further verifiable credentials issued by trusted institutions like the Registry of Births Deaths & Marriages. Credentials can then be presented via the ServiceNSW app, or a dedicated Births Deaths & Marriages app.

Future opportunities being considered by NSW feature a set of primary verifiable credentials used to establish a digital identity (including those issued by the Commonwealth government), underpinning cohort-specific use cases for customers (change of circumstances, education), businesses (liquor licences, trade licences) and government priorities (assisting cost of living through seniors' cards, student cards, disability permits).

Pilot implementations of these credentials within the private sector are anticipated. For example, car rental companies rely on both government-issued identity evidence, combined with evidence of a suitability to drive. Signatures and photographs may be available on these credentials, but do not need to be presented to the rental company, prioritising a data minimisation and consent-led approach to information sharing, pivoting away from relying on a 1:1 digital representation of physical documents.

NSW is undertaking planning for verifiable credential platform integration into existing systems within the next few years, including to achieve National interoperability.

2.2 Canada

In late 2021, Canada’s Prime Ministerial mandate letter to the President of the Treasury Board expanded to specifically include work to progress a national trusted digital identity platform to support seamless service delivery for Canadians.

Historically, some Canadian provinces have actively rejected (or deferred) provincial-level digital identity programs.

To mitigate the risk of a national digital identity program being rejected, Canada is prioritising further consultation and communication activities with the public, academia and Federal provincial and territorial partners. Clarification of the roles of government and private sectors in the delivery of trusted digital identity infrastructure will also be required.

Expanding on existing digital identity initiatives, the Canadian government is looking to build out opportunities to strengthen digital trust by supporting clients who want to create and hold their digital identities, and choose the information that they share about themselves, with whom and for what purpose. All levels of Canadian government can issue documents proving who individuals or businesses *are*, and both the private and public sectors issue documents proving what those individuals or businesses can *do*.

A proposed model of the ‘National Digital Trust Service’ includes a blockchain-based verifiable data registry underpinning Digital Issuing and Verification services for individuals and businesses seeking to obtain both public and private sector services.

Decentralized approaches, such as digital credentials and wallets, that allow clients to hold their information reduce the risk of data breaches as compared to centralized approaches. Additional legislative and regulatory measures to ensure privacy and consumer protections are anticipated in this maturing space. Canadian authorities are also seeking to avoid a proliferation of potentially incompatible ‘digital wallets’ in the market being used to store government-issued verifiable credentials.

2.3 Estonia

The digital identity system, as the vital cornerstone of Estonian e-state, has been around for 20 years (since 2002). Estonia’s long-established digital identity system supports multiple methods of authentication for citizens interacting with public and private sector service providers. Estonian government issues ID cards, mobile IDs and digital IDs based as part of a multi-channel ecosystem. Moreover, all Estonian national eID schemes are notified at the EU level for cross-border use on the assurance level “high.” Every person using their eID can safely identify themselves, use digital services and give qualified digital signatures. The identity data (i.e. name and date of birth) and unique identifier are stored directly in the electronic certificate and disclosed at each authentication session. The term “digital signature” in Estonia refers only to a signature that is legally valid and legally equivalent to a handwritten signature. All Estonian public institutions are obliged to accept digitally signed documents and most private sector companies prefer to conduct business via electronic means.

In Estonia the identity management policy is closely related to identity documents policy. The Ministry of the Interior is responsible for policy in both areas and the Ministry of Economic Affairs and Communications is responsible for the political decisions on eID. At the heart of the Estonian identity management and identity documents policy are the following principles:

- state monopoly and responsibility to identify a person,
- centralized identity management,
- principle of "one person = one identity",
- unambiguous relationship of digital authentication and digital signing certificates with the user of the document,
- public verification of digital authentication and digital signing certificates via the personal identification code.

Estonian government is continuously developing the existing eID ecosystem with emerging technologies and evolving user expectations – for example, the Estonian ID cards have been moving towards to launch the contactless interface (NFC interface) function where the capacity of the new chip has been increased, enabling to add new applications such as electronic tickets in public transportation or other electronically issued certifications. The Estonian eID software has an open-source code, so that all interested parties can see the source code and take part in its development via GitHub. This also facilitates the adoption of an eID in countries that do not have strong identity systems in place yet.

The Estonian market of trust services is dominated by SK ID Solutions AS, qualified provider of certificates for e-signatures and e-seals and timestamps. SK ID Solutions also operates the SIM card based mobile ID identity and the app-based Smart ID solution, both of which are certified as qualified signature creation devices. Estonian government funds development and operation of two identity carriers capable of both qualified electronic signature and authentication: the ID-card and SIM-based mobile ID with SK ID Solutions acting as the CA in both cases and as the operator for mobile ID.

Policy, regulatory, governance and technical investments in Estonia’s X-Road data exchange layer has already established a strong foundation for verifiable credentials anchored to trusted digital identities.

The Estonian government anticipates being an early adopter of the emerging European Digital Identity framework. The framework, proposed by the European Commission, aims to offer citizens and companies in the EU Member States, among other things, so-called digital wallets, with which national digital identity can be linked to other personal documents, e.g., driving license, diplomas, bank account. Such digital wallets would allow paper documents (such as driving licenses) to be digitalized across Europe and conveniently carried and presented across borders. According to the proposal, such digital wallets will be built based on digital identities issued by the member states, i.e., the Estonian ID card and other eID solutions. These solutions will not disappear, but all countries will have an obligation to provide their people with a reliable digital identity. The eID-s and similar systems in the EU Member States will remain intact. However, national systems will become the basis for this digital wallet, such as Estonian PKI based eID ecosystem. Each Member State will develop a separate digital wallet app for its citizens according to the current plan. As for many other EU countries, Estonia will be participating in the EU digital identity wallet pilot focusing firsthand on the mobile driving license use-case. More details about the pilot and concept of the Estonian digital wallet solution will most likely be available during the first half of 2023.

2.4 Israel

Israel's centralized Secure Identity Authentication System (SIAS), deployed since 2016, enjoys a fairly high level of adoption, given its long-term digital identity program and based on a central Population Registry, a unique ID number for each citizen/ resident and a mandatory ID-card, which has been upgraded into chip-card based commencing in 2013. The card issuance is under the responsibility of the Population, Immigration and Border-control Authority (PIBA) in the Ministry of the interior. The digital certificates and the PKI scheme are under the responsibility of the National Digital Agency (NDA) in the Ministry of Economy and Industry.

Regular revision and alignment of standards with international patterns has been an ongoing focus of the NDA adhering to the ISO/IEC 29115 standard for Identity and Service Providers since 2016 and adopting the included risk evaluation model adapted to the Israeli concept when determining levels of assurance (LoA) required to access digital services and the IdP services and issued credentials.

A separate online government services portal (MyGov) dedicated to citizens and to legal entities (e.g., businesses, NGOs in the future) have allowed for rapid uptake of the Gov.iD issued by the SIAS by end-users. Over 80 services from 19 ministries have joined the MyGov citizen portal, further increasing the value of creating a digital identity for end users through the SIAS. Since December 2021, local government authorities (for example - Tel Aviv, and Jerusalem in the near future) have also commenced onboarding their services. The SIAS includes also a Mobile application 2nd factor authentication (2FA) named Gov.id.

Israel is addressing digital accessibility and inclusion issues through the provision of more than 281 self-service digital kiosks (adopted by 45 services across 12 ministries), providing citizen identification services, payments and official formal document printing, for those without digital devices or who prefer physical documentation.

Support for multiple established technical standards (SAML, OAuth, OIDC) has been considered from the outset. The vision is to include in the future a national eIDAS node, following supporting and informing discussions with EU-based members planning for future mutual recognition and interoperability pilots.

When building out their 'secured information avenue' for trusted information transactions between citizens, institutions, companies and governments, Israel has aimed for a data minimization approach and implementing the "ask-once" concept.

Israel is currently piloting and testing the concept of Distributed Identity, verifiable credentials, e-wallet and blockchain. The pilot is undergoing and will be finalized with conclusions and recommendations for a future roadmap. The concept will support individuals managing their credentials in their own digital wallets. The current pilot is leveraging off-the-shelf distributed ledger technologies like Bitcoin, Ethereum and Hyperledger, whilst the e-wallet and the credentials are based on the Blockcerts open standard.

Primary use cases in the current pilot for combining digital identity with verifiable credentials in Israel include - support for issuing blind persons' certificates, land surveyors' credentials, foreign volunteers, foreign workers stay permit and government employee cards.

2.5 New Zealand

New Zealand has taken a broad collaborative approach to the development of a new digital identity system. The Digital Identity Services Trust Framework (DISTF) Bill is currently progressing through Parliament. The legislation is anticipated to be passed by the end of 2022. Associated regulations and rules are also in development.

The Bill aims to promote the provision of secure and trusted digital identity services that meet essential minimum requirements for security, privacy, identification management and interoperability. It also aims to support community resilience and realise the wider benefits of digital identity.

The legislation will be technology agnostic and people-centred, offering New Zealanders great control over their identity related data. The framework will support the use of a range of identity systems, such as the government provided RealMe service, while also encouraging the development, and safe and secure use, of identity services provided by the private sector, including verifiable credentials from both the public and private sectors. The Department of Internal Affairs partners with Māori through regular engagement with iwi[2] leaders and has specific workstreams around Māori identity needs. It also works closely with industry through Digital Identity New Zealand.

New Zealand is developing two key consent-based services designed to support the new digital identity approach: Identity Check and a Verifiable Identity Credential (VIC) based on authoritative data held by government.

Identity Check is a government-operated confirmation service that provides individuals and organisations with a common approach to verifying user identity. A controlled pilot study is the first step in the implementation process.

New Zealand is also exploring the development of a VIC which can be stored by individuals on their personal device via an app or in an online account and can be shared directly with organisations or agencies to prove their identity.

[2] An iwi, or Māori tribe, is the largest socio-political unit in traditional Māori society. It is generally made up of several hapū that are all descended from a common ancestor. Hapū are clusters of whānau where the whānau is usually an extended family grouping consisting of children, parents, often grandparents, and other closely related kin. Iwi, hapū and whānau are now commonly used in New Zealand policy documents.

2.6 Singapore

Singapore's strong uptake of its national digital identity, Singpass (serves approximately 97% of Singapore Citizens and Permanent Residents) has enabled the country to achieve the vision of improving the lives of citizens, creating opportunities for businesses, and transforming the capabilities of government agencies. The Singpass suite of services includes the

a) Singpass app, a mobile user interface, allowing users to access their digital identity, and provide a convenient and secure access to government and private sector services, online and in person
b) Login enables easy authentication access to digital services using the Singpass app, doing away the need for users to remember additional set of credentials
c) Face Verification for enabling access to digital services using a face scan which is then compared against the government's biometric database
d) Myinfo enables electronic Know-Your-Customer (eKYC) via consent-based data sharing
e) Sign to support digital signing of documents, providing convenience and increases productivity and business efficiency
f) Verify to digitalise face-to-face identity verification transactions
g) Myinfo business for pre-filling of digital forms with entity data from government sources upon consent

There are more than 2000 services and 700 organisations using Singpass. By integrating with Singpass, businesses have shared that they enjoy up to 80% reduction in transaction time and $50 savings per transaction.

Everyday transactions performed with non-government entities (for example, healthcare, insurance, HR and employee services) have seen those sectors leverage on Singpass in lieu of creating or maintaining their own digital identity credential services.

Future enhancements to the Singpass infrastructure include moving towards a hybrid model where instead of a centralised model, there are plans to federate parts of Singpass (e.g. federating with foreign trust anchor to allow more foreigners to use Singapore's digital identity offerings). The plan includes extending Singpass Digital Identity Wallet powered by GovTech by implementing privacy-enhancing features to support Verifiable Credentials that could be issued by public and private sectors.

This approach will enable mutual recognition of digital credentials for proof of identity use cases, e.g. vaccination status, driving license and education qualification.

2.7 United Kingdom

The UK government is delivering a number of ambitious and interlinked policy initiatives to prepare the UK for the digital world, and to improve the lives of businesses and citizens. These initiatives, alongside enabling legislation, will help ensure that the UK is able to take full advantage of the opportunities that digital identities and the wider digital economy have to offer.

Two departments that are supporting the delivery of this are: the Government Digital Service (GDS) and the Department for Digital, Culture, Media and Sport (DCMS).

The ‘One Login for Government’ programme, led by GDS, will provide a single account for citizens to login, prove their identity and access all central government services more efficiently. It will replace several existing systems, including ‘GOV.UK Verify’ which relied on identity providers in the private sector. ‘One Login for Government’ is being designed to strike a better balance between inclusivity, accessibility and privacy. It will simplify and accelerate application processes for users, while reducing duplication and costs across government, including by lowering levels of identity fraud.

‘One Login for Government’ relies on a number of credential issuers to perform checks on a user’s identity, backed by both commercially available and government services. Each system that performs a check issues a verifiable credential, which helps provide an audit trail of the check that was done. This means it can be stored and reused in the future. At the same time, ‘One Login for Government’ adheres to the principle of data minimisation, as contained within the General Data Protection Regulation (GDPR), minimising the amount of data that is stored and shared around government. The collected verifiable credentials show what checks were done, without including any unnecessary identity data.

DCMS meanwhile is focused on helping the UK economy to realise the benefits of digital identity. To do this, DCMS has developed the ‘UK digital identity and attributes trust framework’: a set of rules and standards to govern the use of digital identity. This is in addition to legislation being introduced through the ‘Data Protection and Digital Information Bill’, which will give people and businesses confidence that they can trust the framework. The legislation will do the following:

- Establish a new certification scheme so that users can have the confidence that organisations have been independently assessed to prove they follow the rules.
- Set up a governance function to oversee the certified, ‘trust-marked’ organisations.

- Enable a data-checking gateway which will allow accredited private sector organisations to check against government held attributes for the purpose of identity or eligibility verification.

The framework will help organisations to check identities and share attributes in a trusted and consistent way and will facilitate domestic and international interoperability. The Office for Digital Identities and Attributes (OfDIA) will be responsible for maintaining the framework, leading both accreditation and certification processes for private sector entities.

3. Priority Digital Identity + Verifiable Credentials Use Cases

The Working Group looked at the use cases that were being explored or were being used by member countries. It was apparent that there is a broad array of applications for verifiable credentials, as well as different stages of development.

Country	Prioritised Use Cases	Approach
Australia	• Digital Driver Licence • Medicare Card • Concession Cards	National Verifiable Credentials Working Group established, spanning Commonwealth and State and Territory jurisdictions.
Canada	• Individual or business opening a bank account • Cross-border acceptance of diplomas • Proof of address to support municipal services	Federal leadership involving the National Standards and Digital Trust Infrastructure to support domestic and international interoperability of digital identity documents. Partnership between Canada and UK to explore digital credentials established.
Estonia	• Mobile Driving Licence • e-Health and it's sub use cases (e.g. e-prescriptions)	Participation in the European Digital Identity Wallet pilot project for early adoption of the renewed eIDAS regulation and for enabling the cross-border use of digital credentials.
Israel	• Land surveyors (with the Survey of Israel) • Blind person certificates (with the Ministry of Welfare) • Foreign volunteers (with the Ministry of welfare) • Foreign Workers Stay Permit (with the Population and Immigration Agency) • Employee Card (with the Ministry of Economy) • Air Crew Certificate (with the Israeli Civil Aviation Authority) • Vehicle inspector / garage certification (with the Ministry of Transportation)	The different use-cases are part of a pilot/ POC undertaken by the Israeli National Digital Agency, looking at the concept of VC, e-wallets and blockchain. The results will determine how to proceed. The pilot was initiated to actually try practical use cases that can be studied from end-to-end, instead of just a theoretical discussion, but with definite constraints of such a pilot/POC. The e-Wallet standard will eventually be used to support Digital Wallet for citizens, alongside existing central authentication system, self-service kiosks and other identity credentials.
New Zealand	• Identity Check • VIC Development	Both will be driven by DIA in collaboration with a number of other government agencies
United Kingdom	• COVID-19 vaccination status	The UK Government Digital Service is focused on developing the MVP for 'One Login for Government' before prioritising some further use cases for verifiable credentials: enabling for

		the use of digital identity across multiple government services.
Singapore	For cross border use cases: • Individual / business user opening individual / corporate bank account • Individual applying for work permit • Passports • Driving licence • COVID-19 vaccination status • Education qualifications	Explore potential collaboration opportunities with interested partners. Start with issuing government data as verifiable credentials but the future plan is determined based on use case needs, while keeping abreast and alignment to international standards where relevant.

4. Aligning existing digital identity frameworks with verifiable credentials language and concepts

The Working Group were asked to identify where their existing frameworks and standards were being updated to accommodate verifiable credentials.

Country	Approach	Timeframes
Australia	Considering replacing ‘Credential Service Provider’ role (and associated language) with ‘Authenticator’ to prevent concept clashes. Credential issuer concepts may be split into ‘Identity Provider’ roles and ‘Credential Provider’ role, to denote sensitivity, accreditation and assurance levels and credential type. Current version at: https://www.digitalidentity.gov.au/tdif	Update likely in 2023.
Canada	Transitioning away from the concept of Digital Identity to Digital Credentials that enable the delivery of services across the economy. Digital identity means many things to many people, and it is unclear as to what it means. Digital credentials are the digital equivalent of largely government-issued documents, such as driver licenses and business registration documents, provided to individuals and businesses. Digital credential not only enable access to government services, but they also enable individuals and businesses to obtain services and conduct transactions across the economy.’	Canada to consult on the digital credentials model, publicly and with key stakeholders across the economy, in early 2023.’
United Kingdom	The UK digital identity and attributes trust framework contains a data schema written to be consistent and not in conflict with different industry approaches for data exchange and technical standards, such as OpenID Connect and W3C’s Verifiable Credentials data models.	The UK framework is currently in its beta phase.

5. Further Reading

- **OpenID for Verifiable Credentials**
  - (https://openid.net/wordpress-content/uploads/2022/05/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials_FINAL_2022-05-12.pdf)
- **White Paper: Verifiable Credentials and ISO/IEC 18013-5 Based Credentials**
  - (https://www.ul.com/insights/verifiable-credentials-and-isoiec-18013-5-based-credentials)
- **Verifiable Credentials Data Model v1.1**
  - https://www.w3.org/TR/vc-data-model/
- **Verifiable Credentials Data Model Implementation Report 1.0**
  - https://w3c.github.io/vc-test-suite/implementations/
- **Verifiable Credentials Use Cases**
  - https://www.w3.org/TR/vc-use-cases/
- **Decentralized Identifiers (DIDs) v1.0**
  - https://www.w3.org/TR/did-core/