



**Citizen Digital Identity and Digital Credentials for Re-Opening Borders, Travel, and Economies, to Return to “Normal” Life**

---

# COVID-19 has changed most everything

In an effort to contain the COVID-19 pandemic, many countries around the world closed their borders and businesses and **are only recently looking to reopen.** To do this, many governments and organizations are evaluating methods to effectively **convey critical health and identity information** to help revive economies, resume travel, and enable a more “normal” return to work and life.



# Challenges with Traditional Credentials

Traditional identity and health credentials, such as passports and vaccine yellow cards, are often paper-based which creates inherent security risks and fails to meet most modern citizen preferences.

- 1** Fraudulent actors are evolving to exploit document security vulnerabilities
- 2** Many stakeholders play a role in the credentialing process, increasing unnecessary exposure of data on paper
- 3** Customers expect a seamless and secure user experience with reduced physical touchpoints
- 4** Manual verification of paper credentials is timely and costly for many organizations
- 5** Physical credentials lack biometric privacy protection and are susceptible to forgery
- 6** Physical credentials are unable to capture the complexity of changing requirements and fraud advancements

\* A paper-based credential may still be used as an alternative to accommodate people who do not have digital access and as fall back or redundancy mechanism.

# Solution: Citizen Digital Identity & Digital Credentials

Citizen Digital identity and digital credentials are the **next frontier**.



## OVERVIEW

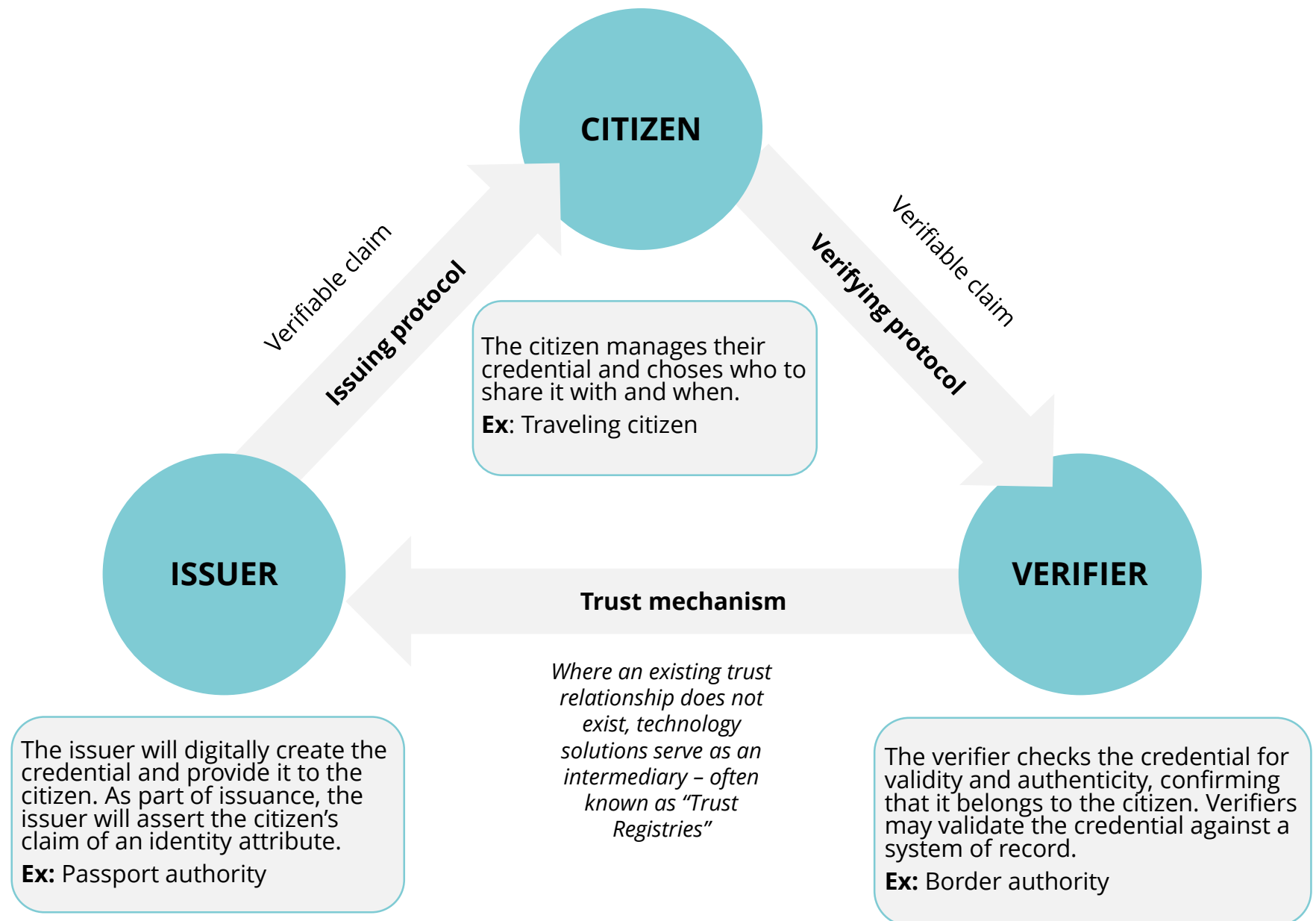
Many digital identity and digital credential solutions allow stakeholders to **certify, communicate, and authenticate** the identity and health status of individuals, while **increasing privacy** and putting control of personal data in the hands of citizens.

Digital IDs and credentials offer citizens **control over their data**, and **flexibility** to choose what information to share, when, and with whom. Digital credentials are also simpler to **issue and verify**, helping to streamline processes and **protecting against fraud**.

**Note:** Paper counterparts can still exist alongside digital credentials, especially for those who do not have access to necessary digital ID technology, such as smart phones. However, paper credentials associated with a digital solution remain more secure than traditional paper IDs as they can leverage one-time codes and other techniques.

## KEY PLAYERS

Citizen digital identity has **three key players**: the **issuer, the citizen, and the verifier**. Each stakeholder plays a significant role in enabling the digital identity ecosystem. With the citizen at the center, this model enables the individual to have flexibility and provide their credentials without ongoing touchpoints with the issuing authority.



# Potential Benefits of Citizen Digital Identity & Digital Credentials

Citizen digital identity and digital credentials offer numerous benefits for individuals, governments, and corporations in **detering fraudulent actors, improving accessibility** and **enhancing security** for citizens.



## For Individuals

---

- Improved access and speed of access to public, financial, or health services
- Improved security and control of personal data by limiting ownership
- Decreased risk of identity or data theft
- Eased travel across borders



## For Government + Regulators

---

- Decreased cost and time of document issuance and data collection
- Decreased possibility of government corruption and increased trust
- Eased process of cross border diligence and visa processing in terms of cost and time



## For Corporations

---

- Reduced losses due to fraud and other illicit activities
- Expanded customer base including new markets of the unbanked, and faster corporate registration

# Mitigating Challenges by Adhering to Core Principles and Frameworks

Because citizen digital identity and digital credentials are a new frontier, several challenges should be fully understood and mitigated before solutioning occurs at scale. These challenges are surmountable with the right strategies, principles, and frameworks.

## Challenges

### TECHNOLOGY

between interoperability of systems and assuring privacy of citizens and security of their data

### ECOSYSTEM

between designing digital identity ecosystems while maintaining flexibility, and security, and reconciling different legal frameworks across jurisdictions

### SOCIAL

between creating a transformative capability and maintaining equity, or preventing the emergence of an elite class of digital identity and credential users

### SCALING

between making digital identity and credential solutions widely available, acknowledging a potential lack of initial customer interest or willingness to embrace the technology early on, and the increase in the volume of credentials to be verified

## Core Principles



### SOCIAL GOOD

Digital credentials should serve citizen interests and be open to all who wish to participate. Digital and paper credentials will need to co-exist. Plan for both.



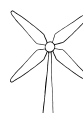
### PRIVACY, SECURITY, & ETHICS

Adopting leading privacy, security and ethical approaches will be critical to building trust and confidence in the credentials.



### CITIZEN-CENTRIC

Put the citizen at the center, provide the credential to the citizen and enable them to use it in the context that makes sense for them.



### SUSTAINABLE

As we saw during COVID-19, approaches need to be adaptable to a rapidly changing environment. Digital can adapt. Paper will struggle.



### FLEXIBLE, OPEN & INTEROPERABLE

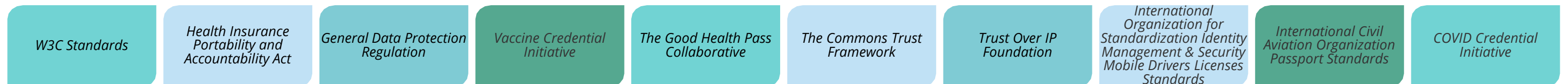
Many countries and agencies have different technology starting points. We need to collectively build on open, global standards to enable those different technologies to inter-operate.



### INCLUSIVE, ACCESSIBLE & EQUITABLE

Enable solutions and approaches that can be inclusive, accessible and equitable. Many jurisdictions want solutions that are free to citizens.

**Adhering to standards, frameworks, and coalitions is critical to establishing sustainable and equitable digital identity solutions:**



# Citizen Digital Identity and Digital Credential Archetypes

Citizen Digital identity and digital credential solutions can support citizens across a range of use cases. Digital credentials won't just help citizens across the world resume "normal" life in the wake of COVID-19 – digital identities are likely to become the future standard practice across industries.

	1 TRAVEL (+HEALTH)	2 "BACK TO LIFE"	3 SERVICES + COMMERCE
ISSUE	<p><i>International and Domestic</i></p> <p>While using traditional identification for domestic and international travel, citizens are often required to <b>provide more than necessary</b>, and endure <b>high-touch verification experiences</b>. Meanwhile, verifiers are unable to securely confirm <b>individual health statuses in the wake of COVID-19</b>, and often encounter <b>malicious actors</b> who exploit identity systems.</p>	<p><i>Work, School, Dining, Entertainment, Shopping, and More</i></p> <p>As employers, educational institutions, businesses, and other venues establish long-term COVID-19 protocols for <b>safe attendance at work, school, and more</b>, some organizations are requiring individuals to demonstrate proof of vaccination or test.</p>	<p><i>Social / Government, Banking, and More</i></p> <p>Proving identity while applying for and obtaining services, opening a bank account, or making purchases, often requires <b>in-person interaction, extensive paperwork, and several usernames and passwords</b> across centralized systems.</p>
SOLUTION	<p>A digital solution that will enable a citizen to securely exchange personal data in a <b>standardized process</b> and uses authentication mechanisms such as passenger <b>biometric recognition</b> throughout the journey.</p>	<p><b>A trusted digital tool that allows customers, students, and employees to prove their health status to a verifier prior to entry</b> without unnecessary exposure of personal data, and the ability to indicate when their health status has changed.</p>	<p><b>A single, reusable, decentralized, digital credential</b> that validates an individual's identity without openly revealing sensitive information and <b>removing the need for backup verification and multiple logins</b> due to the trusted nature of the credential.</p>
FUTURE VISION	<p>Individuals will hold a <b>dynamic digital identity and credentials</b> that are accessible <b>on their mobile device</b>, enabling more seamless domestic and international border crossings in an age of changing restrictions, including restrictions and policies related to health status.</p>	<p>Employees, students, and customers can more safely <b>return to physical workspaces, classrooms, restaurants, entertainment venues, and more</b> to collaborate with colleagues and peers after showing a certified digital health status.</p>	<p>A citizen can receive services and products from government entities, financial institutions, and businesses using the same, trusted credential, <b>streamlining complex processes, improving the customer experience, and leveraging leading practice privacy and security safeguards.</b></p>

# Spotlight on Digital Travel and Health Credentials

Travel and health are two spaces where digital credentialing could make a significant impact.





## Travel

The International Civil Aviation Organization (ICAO) states that a Digital Travel Credential (DTC) **“is intended to temporarily or permanently substitute a conventional passport with a digital representation of the traveler’s identity.”**





## Health

A digital health credential contains **health information that is securely stored on a mobile device in a secure mobile wallet.** The digital health credential binds the citizen’s identity to their health information (e.g., vaccination record, test results).

### WHAT VALUE CAN DIGITAL TRAVEL CREDENTIALS PROVIDE?

-  At an airport, provides full passenger self-service through the **check-in** experience, document-free identification through **security screenings**, and smoother **boarding**
-  **Maximizes privacy** of individuals as unnecessary information is not physically observable (i.e., a QR code is used rather than a number or the same barcode)
-  **Increases trust** between verifiers and individuals on airports, trains, and other forms of transportation
-  **Places the citizen in control** of the credential

### WHAT VALUE CAN DIGITAL HEALTH CREDENTIALS PROVIDE?

-  Provides patients with a **trusted health credential** accessible on their digital device, enabling **return to work and travel**
-  **Helps to prevent against fraudulent paper documents** by allowing authorities to securely issue a credential to a citizen’s mobile wallet, which can help prevent misuse
-  **Increases trust among verifiers** that the individual holding the credential is who they say they are
-  **Increases speed of verification** for the aviation and entertainment ecosystem, supporting the reopening of economies

**Example: Digital Passport or Driver’s License**

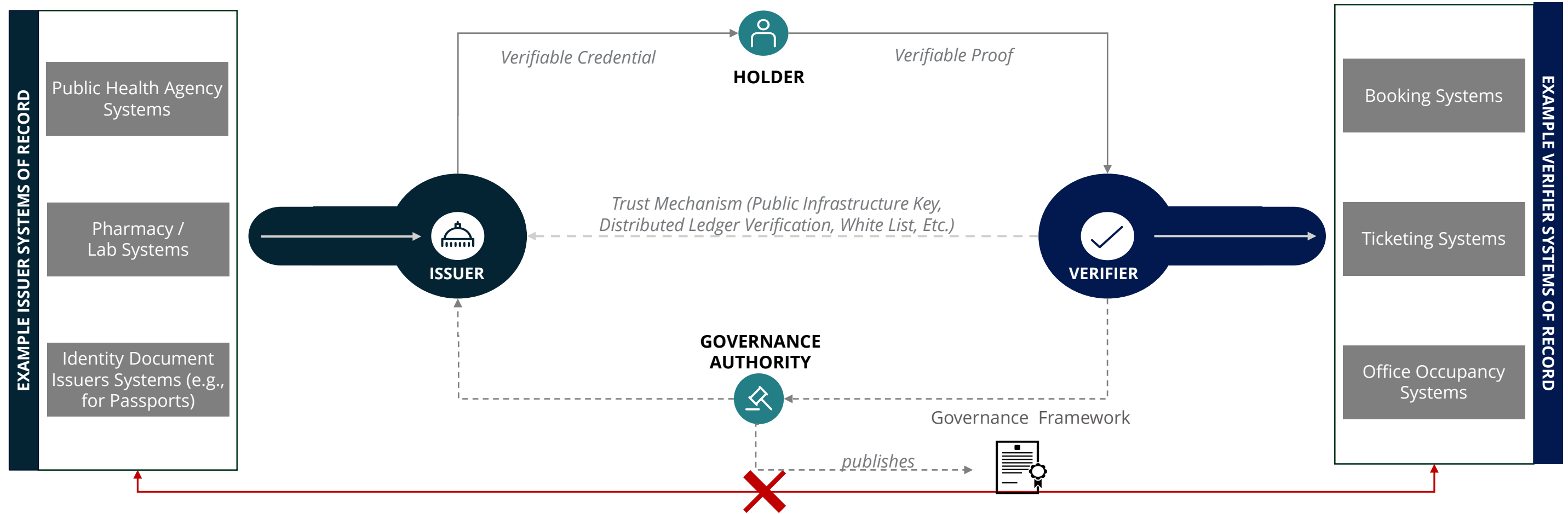
**Example: Digital Vaccine Credential**

***In addition to travel and health, there are countless other credentials one could virtualize, including: visas, refugee cards, employee / education IDs, birth certificates, indigenous persons travel documents, credit/debit cards, and more.***



# Potential Solution Architecture (Modular) and Capability Options

Deloitte helps organizations fulfill their mandate to **issue verifiable credentials** from systems of record they use and focus on their core responsibilities. Verifiers can also **obtain verifiable data** from their customers and **integrate that data with their workflow**, whether it's issuing a boarding pass or planning a trip to the office.



## Solution Capability Options

While the underlying architecture should remain largely the same to enable interoperability, some entities may wish to focus on building out specific capabilities that address their most pressing requirements.



**Mobile Wallet:** Mobile application where citizens can securely maintain their personal data and prove their ID and health status to verifiers



**Digital ID Citizen Portal:** Platform for citizens to view and manage their personal information in a single location, accessed using the digital identity credential



**Health Credential:** COVID testing and vaccine history accessible via the digital wallet and certified by trusted labs and health providers



**Ecosystem APIs:** Capabilities to integrate data owned by third parties so that digital credentials can serve as an ecosystem platform



**Issuer and Verifier App:** App and/or portal and other capabilities so that issuing authorities can certify an individual's data, and verifiers can trust and validate it



**Communications Platform:** Platform for two-way communication between citizens and organizations, e.g., health providers, to support management of public health, contact tracing and other needs



**Rules & Policy Engines:** Engine to validate the identity and health data required for citizens to travel to a particular location or conduct a given activity

# Deloitte's Citizen Digital Identity and Digital Credential Services

Deloitte can support organizations throughout the process of developing, deploying, and maintaining digital identity and digital credential solutions.



**Cybersecurity**

**Protecting digital identity solutions** from hacking and data loss should be integrated throughout the design, build, and operate stages in the process.

➔

Deloitte's core citizen digital identity and digital credential services are augmented by an **existing portfolio of 200+ assets** and **119 global alliance collaborators** that can accelerate development and integration and provide differentiation and competitive advantages.

# Deloitte Qualifications

Deloitte has experience developing and deploying citizen digital identity and digital credentials across geographies and sectors.

UK FINANCIAL CONDUCT AUTHORITY (FCA) REGULATORY SANDBOX	CANADIAN PUBLIC SECTOR	UK INTERNATIONAL TRAVEL	CANADIAN FINANCIAL SERVICES SECTOR	AUSTRALIAN CIVIL AVIATION REGULATOR
<p><b>CONTEXT</b></p> <p>Optic was accepted into the UK's Financial Conduct Authority (FCA) Regulatory Sandbox, which allows business to test innovative propositions in the market with real consumers. The initial focus was to work with industry participants, including Seders, Curve, Monese, B-Social and one major UK bank to build an open and scalable ecosystem which improved customer experience and protection, whilst solving challenges for financial services clients and beyond.</p> <p><b>ECOSYSTEM PARTICIPANTS</b></p> <ul style="list-style-type: none"> <li><b>Deloitte</b> – Orchestrates the ecosystem as well as providing the business facing KYC product (Optic)</li> <li><b>Evernym</b> – Provides the connection to the distributed network and the consumer facing identity applications.</li> <li><b>Onfido</b>: Verifies consumers' identity and issues reusable credentials</li> <li><b>Banks &amp; FinTechs ("Relying Parties")</b> – Receives and validates credentials to onboard customers (KYC) prior to providing financial services products</li> <li><b>FCA</b> – Provides clarification and guidance on the regulatory acceptance of digital identity credentials</li> <li><b>Government</b> – Released call for evidence on how the public sector can drive adoption of digital identity and how this could strengthen UK Plc.</li> </ul> <p><b>OBJECTIVES ACHIEVED</b></p> <ul style="list-style-type: none"> <li>Market appetite</li> <li>Technically robust solution</li> <li>Regulatory acceptable</li> <li>Privacy and security enhancing</li> </ul>	<p><b>CONTEXT</b></p> <p>A large Canadian Province was seeking to explore the implications of Digital Identity to their operations and how the province's role a Digital Identity issuer may unfold. In Canada, provinces hold the responsibility for Canadian's foundational ID's (birth certificates), driver's licenses, as well as the delivery of government healthcare. Deloitte Canada conducted a series of workshops to both educate the client and work through a set of strategic options. Within the chosen options, possible implications were articulated.</p> <p><b>ACTIVITIES</b></p> <ul style="list-style-type: none"> <li>Facilitated discovery and ideation workshops</li> <li>Developed strategic choices for the Province based on prioritized Digital ID use cases</li> <li>Explored economic model options for funding Digital ID operation through research in interviews with key stakeholders</li> <li>Facilitated creation of Digital ID roadmap for province</li> </ul> <p><b>OBJECTIVES ACHIEVED</b></p> <ul style="list-style-type: none"> <li>Initial strategic choices articulated</li> <li>High level roadmap created</li> </ul>	<p><b>CONTEXT</b></p> <p>Deloitte UK has developed a platform and ecosystem that is designed to meet digital verification requirements of health credentials for the travel industry. The prototype addresses the need to request, verify and trust data relating to passengers' COVID-19 status. This is done in a way that respects individual privacy while keeping data secure. Passengers' COVID-19 test result is stored on their own mobile to be only shared with their consent and verified securely during their trip, by airports, airlines, and borders.</p> <p><b>FEATURES</b></p> <ul style="list-style-type: none"> <li><b>Health Checks</b> – The prototype enables digital verification of any type of credential</li> <li><b>GDPR</b> – Requesting and/or retaining healthcare data has GDPR implications, it is desirable for such records to be held by the passenger/employee and shared via explicit consent where appropriate</li> <li><b>Air Corridors</b> – The service runs on open and globally interoperable data standards; it can support any healthcare credentials and can be embedded in pre-departure or on on-site processes across both outbound and inbound processing</li> <li><b>Digital Travel Credentials</b> – The service can be extended beyond health credentials to any identity credential</li> </ul> <p><b>OBJECTIVES ACHIEVED</b></p> <ul style="list-style-type: none"> <li>Fit to fly credentials are a catalyst to enable COVID-secure travel</li> <li>There is potential for submission of approved documents into airport / airline systems before visiting an airport Onsite testing retained as an exception channel should visitors find their paper credential is not accepted</li> <li>Identity and verification (ID&amp;V) is required at the point of testing</li> <li>Scope includes arriving, transferring and departing passengers, airport staff and associated third parties, and all flight crew</li> <li>Passengers checking in online must demonstrate their fit-to-fly credential before receipt of their boarding card</li> </ul>	<p><b>CONTEXT</b></p> <p>The Canadian banking sector decided to actively pursue Digital Identity solutions in order to improve the customer experience, reduce the risk of fraud, and to drive innovative products/services for customers. Through a series of engagements with key stakeholders, Deloitte Canada supported clients with a range of activities in order to articulate their strategy and identify opportunities to execute on that strategy.</p> <p><b>ACTIVITIES</b></p> <ul style="list-style-type: none"> <li><b>Use Case Identification</b> – Prioritized a list of key use cases based on interviews and research</li> <li><b>Market Sizing</b> – Estimated the total size of prioritized digital ID use cases within financial services</li> <li><b>Benefits Sizing</b> – Estimated the financial benefits accrued to client through the implementation of digital ID services</li> <li><b>M&amp;A</b> – Completed strategic and financial due diligence on multiple M&amp;A targets within the digital identity space in Canada</li> <li><b>Stakeholder facilitation and alignment</b> – Brokered and facilitated several alignment sessions with key players in the FSI ecosystem regarding Digital ID implementation and strategy</li> </ul> <p><b>OBJECTIVES ACHIEVED</b></p> <ul style="list-style-type: none"> <li>Digital ID strategies and roadmaps articulated for key players</li> <li>Use cases prioritized and benefits calculated</li> <li>Successful M&amp;A transactions completed</li> </ul>	<p><b>CONTEXT</b></p> <p>As part of regulatory service delivery transformation, Deloitte assisted the Australian Civil Aviation Regulator to transform its paper-based pilot's licenses into a digital format. Aviation licenses are issued as per standards set out by ICAO and are obtained after extensive training and practical experience. Maintaining licenses also require routine reviews and assessments that have to be captured on a license document. Over time, these paper-based documents become unwieldy and cumbersome. ICAO is still finalizing their standards for a digital license, but the Australian regulator is an early mover with a concept license that they have launched with Deloitte's assistance.</p> <p><b>FEATURES</b></p> <ul style="list-style-type: none"> <li><b>Download</b> – Ability to download a copy of a license to a user's mobile wallet through user-initiated action and consent</li> <li><b>Security clearance</b> – Validation of the currency of extended security verification and clearance that is required for all aviation sector personnel by Australian law</li> <li><b>ICAO standards</b> – Data layout of the digital license in line with data standards and requirements of ICAO – internationally recognized</li> <li><b>Push updates</b> – Ability to push updates to the digital license of changes to permissions and qualifications, currency of information and other updates</li> <li><b>Verification</b> – Verification of the authenticity of a license through a QR code scanning mechanism</li> </ul> <p><b>OBJECTIVES ACHIEVED</b></p> <ul style="list-style-type: none"> <li>Leveraging technology already in the hands of people</li> <li>API oriented design that leaves a minimal technical footprint and maximizes the value of existing IT assets</li> <li>Single source of truth</li> </ul>

# Contact Our Team

Connect with our team to learn more about citizen digital identity and digital credentials.



**Costi Perricos**  
Partner  
United Kingdom  
[cperricos@deloitte.co.uk](mailto:cperricos@deloitte.co.uk)



**Jamie Sawchuk**  
Partner  
Canada  
[jsawchuk@deloitte.ca](mailto:jsawchuk@deloitte.ca)



**Esther Dryburgh**  
Partner  
Canada  
[edryburgh@deloitte.ca](mailto:edryburgh@deloitte.ca)



**Philip Horwell**  
Senior Manager  
United Kingdom  
[phorwell@deloitte.co.uk](mailto:phorwell@deloitte.co.uk)



**Giselle D'Paiva**  
Senior Manager  
Canada  
[gdpaiva@deloitte.ca](mailto:gdpaiva@deloitte.ca)



**Nathaniel Thomas**  
Manager  
USA  
[naththomas@deloitte.com](mailto:naththomas@deloitte.com)

**To learn more, visit** <https://bit.ly/3eUY2P2>  
**To contact us, email** [GlobalVaccinesWorkingGroup@deloitte.com](mailto:GlobalVaccinesWorkingGroup@deloitte.com)

Thank you.

# Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms and their related entities. DTTL (also referred to as “Deloitte Global”) and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 264,000 people make an impact that matters at [www.deloitte.com](http://www.deloitte.com).

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the “Deloitte network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2021. For information, contact Deloitte Touche Tohmatsu Limited.