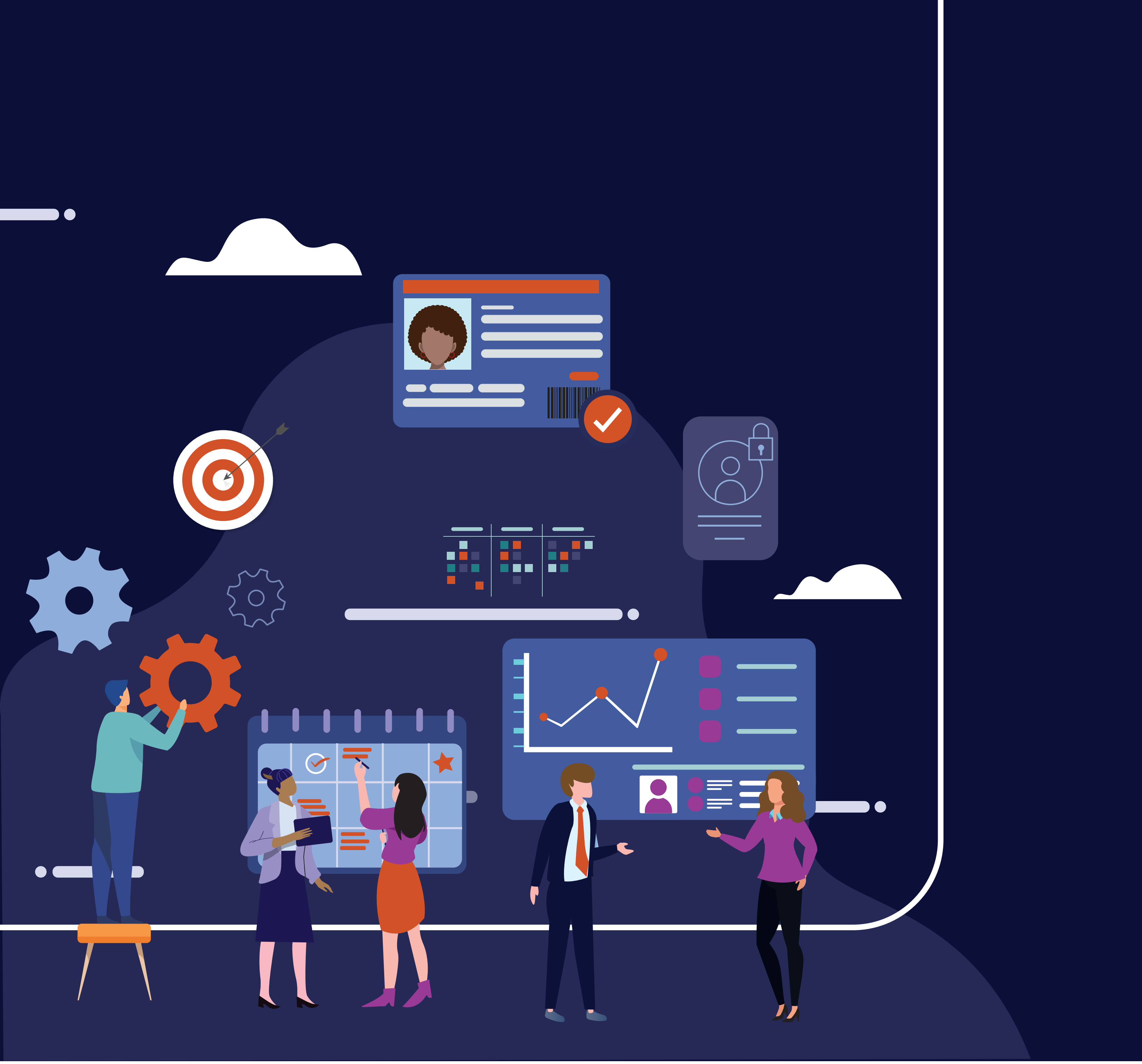


DIACC

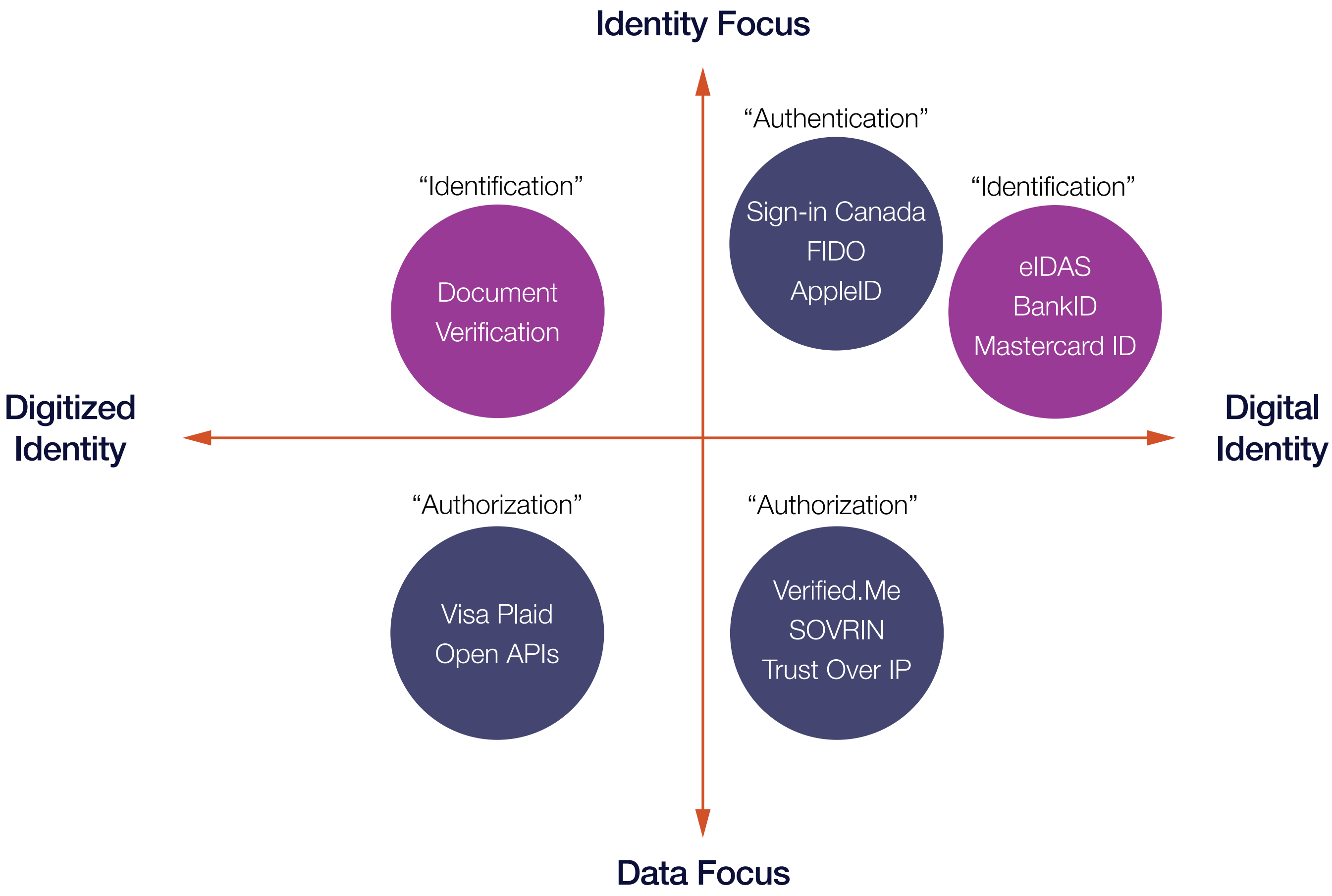
Five Year Strategic Plan

October, 2020

Contents

What does digital identity look like today?

What does digital identity look like today?



Theme: Identity vs Identification

Growing use of mobile document verification solutions for digital onboarding. By themselves they do not enable re-usable or portable digital identities.

Theme: Identity vs Data

Much focus on sharing of personal data. This includes proving identity or entitlement through the sharing of attributes. It also includes the broader sharing of personal and transactional data through open APIs. This blurring of the lines creates complex governance challenges.

Big tech companies that have amassed huge data are also increasingly dabbling with identity.

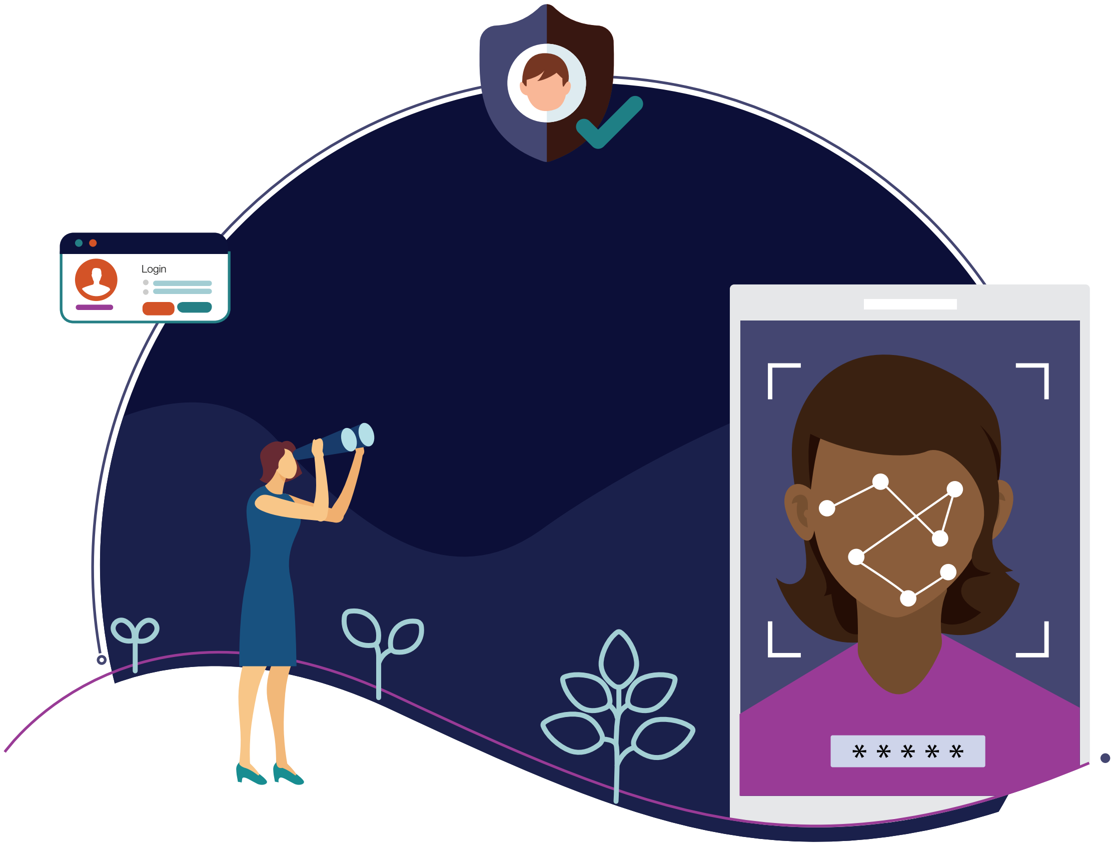
Theme: Data Integrity

Ensuring the integrity of data is key to trusted digital identity. This has brought cryptography to the fore, especially in the development of Verifiable Credential standards.

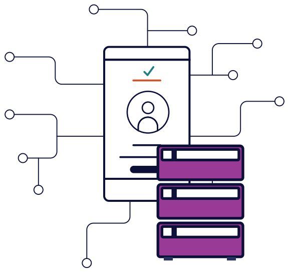
Theme: Governance

Decentralized identity standards enable the rails. Trust frameworks are needed to set the rules.

What might digital identity look like in five years?

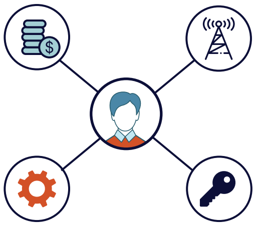


Potential future scenarios



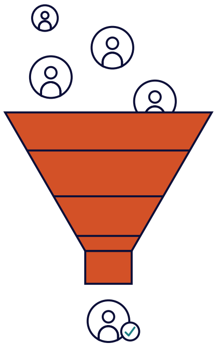
Platform Identity

A walled garden environment where identity is used to keep the user on the platform (or group of affiliated platforms). The platform identity is made available for use in other contexts but the aim is always to make the platform the center of the user's digital life. Data about the user will be obtained from many sources and aggregated within the platform for its benefit. The commercial model is driven by the commercial model of the platform.



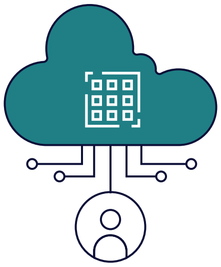
Operator Networks

Groups of operators, typically from regulated industries such as financial services or telecoms, form consortia to enable the sharing of identity and attribute data. Schemes are established around each consortium which govern all aspects of the identity and attribute sharing network. This includes requirements for participation, fees, and liability. Identity and attribute data are obtained from known, vetted sources. The network still places a strong emphasis on privacy, allowing the user to have transparency and control of what data is shared and with whom.



Self-Sovereign Identity

Identity and attribute data is funneled through a wallet or agent employed by the user. Open and standardized frameworks allow the user to obtain verifiable and potentially trusted data from the parties it interacts with and share that data with other parties. Some parties are happy to provide verifiable data to the user without being paid. For other parties, commercial frameworks that add value to the data (e.g. by providing liability) will be developed potentially outside of the technical infrastructure used to share data.

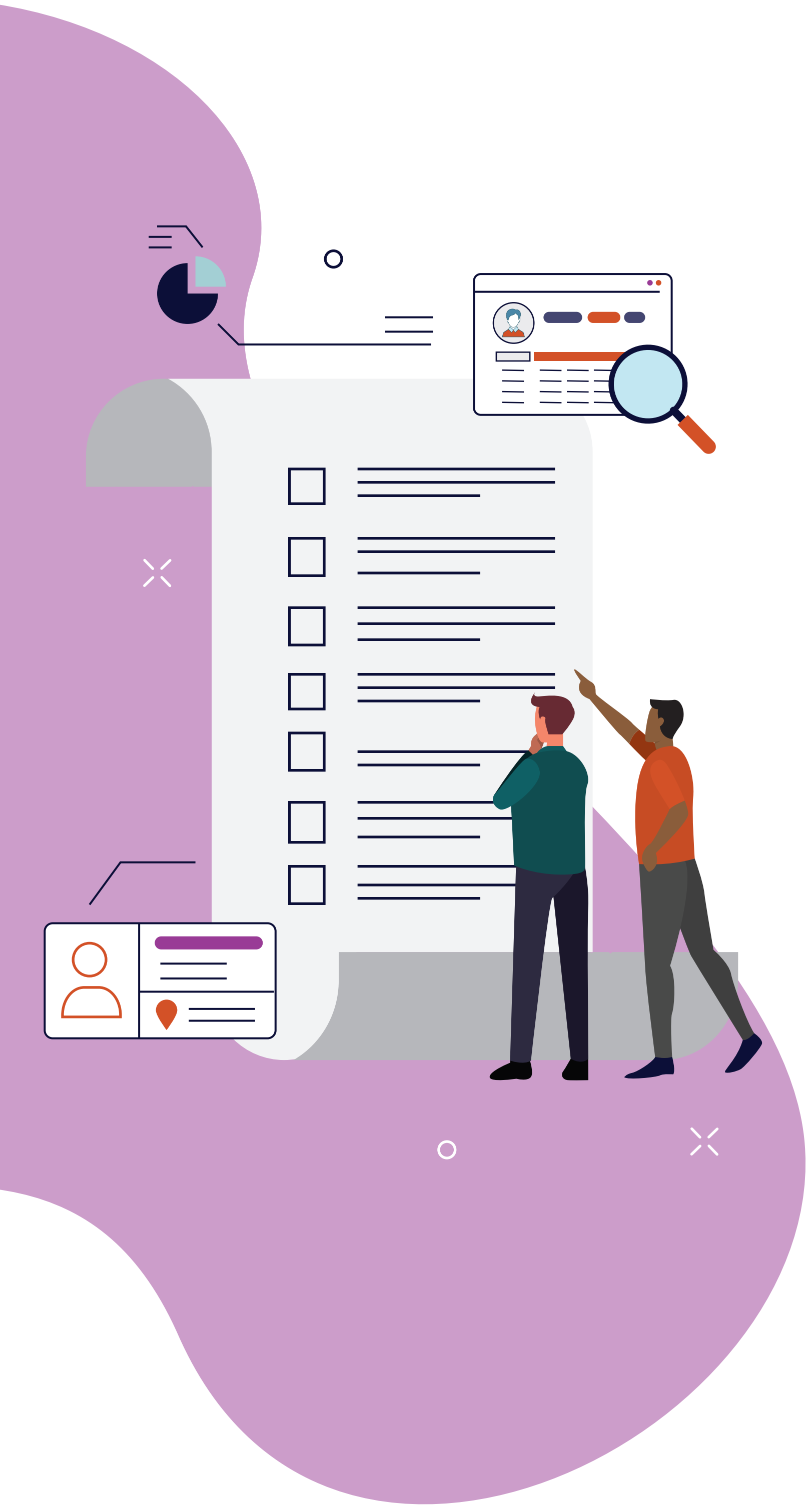


Open APIs

Data about the user is made available to the user through standardized open APIs. These APIs are provided by organizations in many sectors including financial services, energy, education, and health. They provide access to all types of data including transactional data as well as identity attributes that the user may wish to assert. The APIs enable the user to establish many independent bilateral links between the services it uses. Some APIs will be regulated and non-commercial, others will be commercial. Aggregators seek to simplify the ecosystem by integrating with multiple service providers.

The DIACC anticipates that all of the above scenarios will play some role in shaping the digital identity landscape.

The scenarios as narratives



Platform Identity

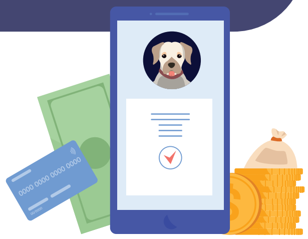
No significant change from today. The internet giants have tried to adapt their business models away from advertising revenues but consumers are not willing to pay. The net effect is that while additional regulatory controls are being placed around them, the system is still fundamentally the same. So end-users have limited visibility on what information is held about them or how it is used.

"On the internet still no one knows you're a dog"

Operator Networks

To sign up and use secure digital services, users need to be able to provide reliable information about their identity. Users already trust regulated organizations to provide trustworthy services like banking and protected internet access, it was natural for them to look to those organizations to help them with digital identity too. Secure identity exchange networks help responsible organizations share user information, with the user's consent. It may not work everywhere but does help in those services where identity matters the most.

"How can you be a dog if you've got a bank account and mobile phone?"



The scenarios as narratives

Self-Sovereign Identity

Users and businesses alike have begun to realize the need to fundamentally change the way personal data is managed. For businesses, personal data is a now a significant liability due to data protection risks. Users see the value of being able to hold their data and take it where they need it. Of course for this to work the data presented by users needs to be reliable and trustworthy. This is why users have started to use cryptographic wallets to collect and share signed data. These allow them to share just the signed data needed in a particular context. Users now need to look after their data better, much like they look after their money.

"On the internet you can now prove you are a dog."

Open APIs

Identity networks as we envisaged them never really took off, due to a combination of users not really understanding what digital identity is and organizations not appreciating the longer-term business benefits. Instead, organizations across the economy have been forced to open up APIs allowing services to access user data (with the user's consent) from other places. Users link together different services as the need arises. It is down to the individual service to piece together all the data it collects into something meaningful for the particular user. Most individual users, of course, don't remember all the connections and links they have set up.

"We don't know if you are a dog,
but we can see you like doggy treats."

What are the key challenges to DIACC that arise out of the potential future scenarios?

DIACC's role in scenarios

How well would scenarios align with the values of DIACC members?

Requirement	Platform	Operator Networks	Self-Sovereign	Open APIs
Participation	L	H	M	M
Transparency	L	M	H	L
Accountability	L	H	M	L
Confidentiality	L	H	H	H
Integrity	L	H	H	M
Availability	M	H	H	M

The above high-level evaluation of each of the scenarios is based on the governance and operational requirements as described in DIACC's whitepaper "Making Sense of Identity Networks", which reflects DIACC member values and expectations for identity networks. More detail behind the intent of each requirement is included in the appendix of this document.

This evaluation demonstrates that the self-sovereign and operator network scenarios are best aligned with DIACC member values, with the open APIs scenario providing challenges particularly in governance, and the platform scenario being the least aligned.

What influence does the DIACC currently have?

Platform	Operator Networks	Self-Sovereign	Open APIs
None	Good	Good	Limited

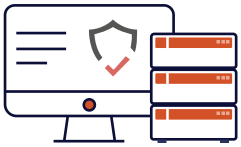
Challenges the scenarios create for the DIACC

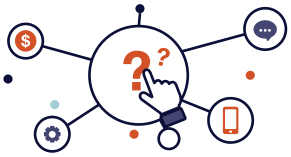
Platform Identity

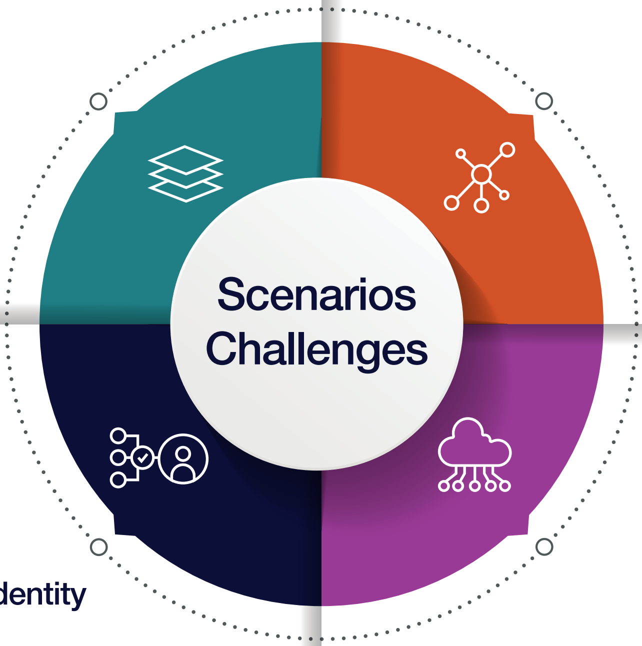
- DIACC currently has limited influence
- Many challenges to governments and businesses over participation
- Removes opportunity for a level playing field
- Monopolies that require government intervention
- Convenience to users hides negative impacts
- Sustainability of current commercial model unclear
- Variable quality data
- Minimal incentive to adopt the PCTF

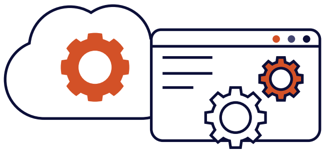
Operator Networks

- Availability of government data sources
- Unclear source of authority for digital ID standards across the economy (parallel working bodies)
- Lack of existing policy development around acceptance of cross-sector digital identity and data sharing
- Reducing the learning curve for general consumers on what it is and why it's important
- Lack of funding for digital government services holds back penetration of services
- Commercial sustainability unclear
- Ensuring critical mass of organizations and users participate









Self-Sovereign Identity

- Governance evolving separately from the PCTF
- Commercial sustainability and liability unclear
- Unclear source of authority for digital ID standards across the economy (parallel working bodies)
- Need to protect vulnerable people
- Availability of government data sources
- Avoiding de facto standards
- Complex landscape may need complex legislation
- Reducing the learning curve for general consumers on what it is and why it's important
- Ensuring critical mass of organizations and users participate
- Lack of funding for digital government services holds back penetration of services

Open APIs

- DIACC currently has limited influence
- Commercial model unclear
- Open data may not have good provenance
- Unclear source of authority for digital ID standards across the economy (parallel working bodies)
- Utility for businesses and people may be limited unless its about more than identity data
- Governance likely to be dictated by regulation rather than agreement or contract
- Availability of government data sources
- Lack of funding for digital government services holds back penetration of services

What key challenges are common across scenarios?

Creating Market Conditions

Standards

The source of authority for digital identity standards across the economy is unclear due to parallel working body efforts across Canada.

Regulatory

Government has an important role to play in digital identity. The provinces and territories are primary sources of foundational identities. Regulation needs to allow digital identity solutions, including the controlled opening up of data.

Promoting Market Growth

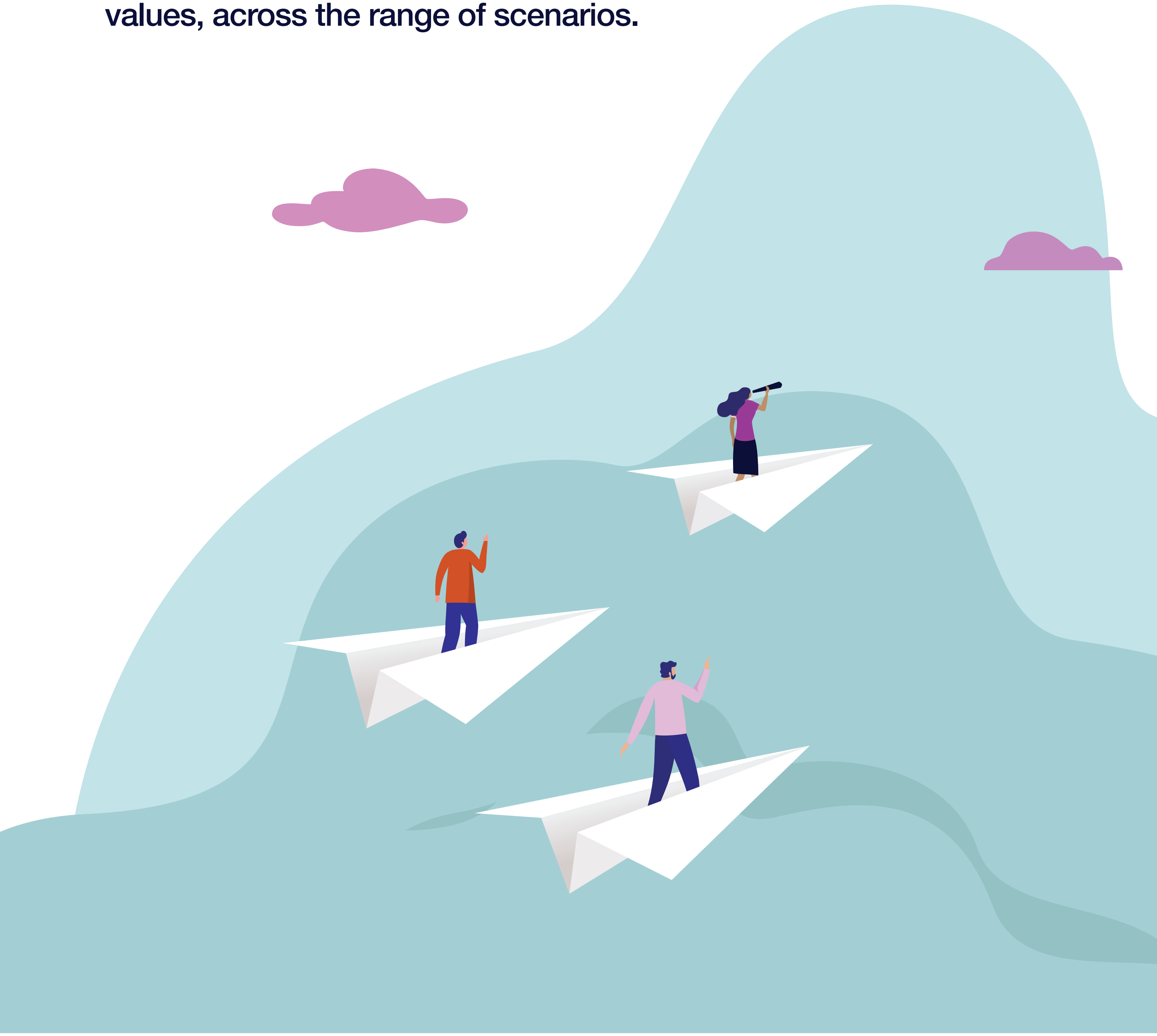
Sustainability

While each scenario provides a varying perspective, commercial sustainability and viability are either unclear, underdeveloped, or unproven. Considerations for liability should also be included in this category of challenges as the responsibility around personal data exchanged needs to be carefully examined.

Inclusion

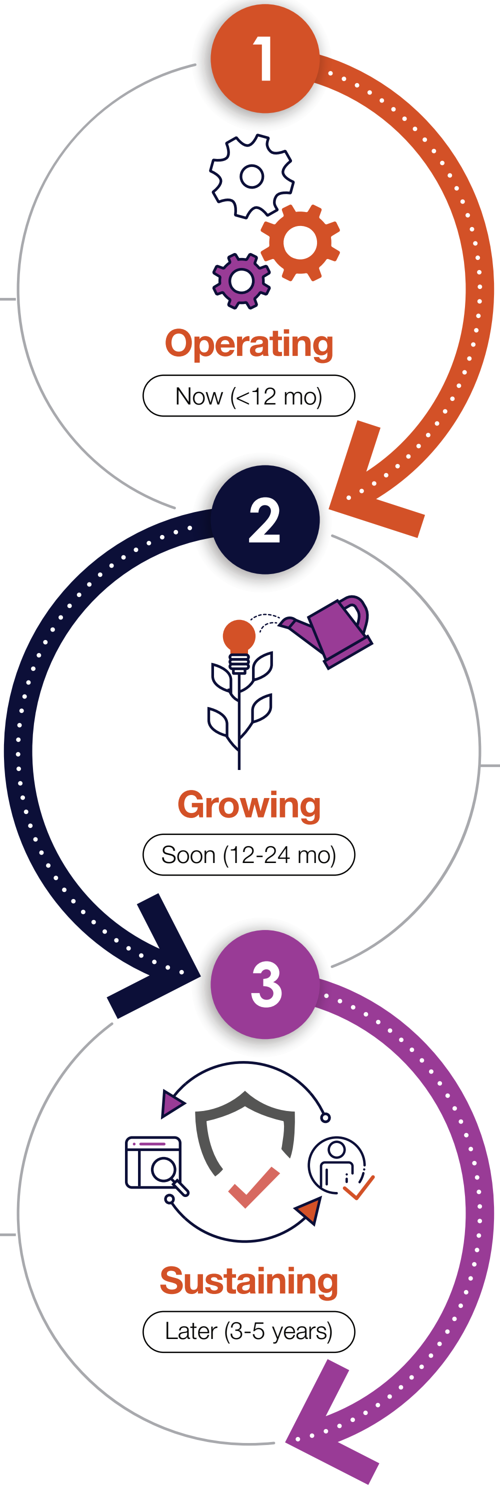
Ensuring that a critical mass of providers and users adopt digital identity products is significant across all scenarios, while also ensuring those that are typically excluded can get access to services or can be provided with better experiences than those that exist today.

Regardless of how the landscape evolves, the DIACC must have clear goals and actions to support positive strategic outcomes in line with DIACC members' values, across the range of scenarios.



What will DIACC do to address these key challenges?

Meeting the five year challenges



1

Operating

Now (<12 mo)

- Obtain senior recognition in federal, provincial, territorial and municipal governments on the importance of digital ID and DIACC's role
- Address parallel efforts across DIACC, the Joint Councils and other bodies
- Prioritize, consolidate and author remaining PCTF components
- Enable agency and empowerment to access public and private sector data sources
- Develop & deliver the PCTF Trustmark Program
- Identify key policy and regulatory enablers and barriers to digital identity growth

2

Growing

Soon (12-24 mo)

- Grow the DIACC – provincial/ territorial, new sectors, increase industry engagement
- Rapid certification and recognition of compliant services and solutions
- Continue to refine and broaden the scope of the PCTF
- Promote regulatory change on behalf of the DIACC community
- Educate end users on the importance of digital ID and promote member progress
- Monitor market evolution and respond to developments outside of influence

3

Sustaining

Later (3-5 years)

- Obtain broad understanding of need and value of "good" digital identity
- PCTF Trustmark recognized widely as symbol of trustworthy digital identity
- International alignment or export of the PCTF to key economic partners
- Enable agency and empowerment to access public and private sector data sources
- Concerted effort to address needs of digitally excluded
- Monitor market evolution and respond to developments outside of influence

Join DIACC to secure our digital future

Join the ecosystem by becoming a member, with the opportunity to:

- Get important introductions to grow partnerships and business opportunities
- Attend or host cross-sector events and workshops where real problems are solved
- Learn how to build your identity team
- Access insider information and gain insights to inform your strategy
- Raise your organization's market visibility with spotlights and publications
- Make your resources go further as part of a community of leaders driving change and innovation in digital ID
- Influence the Canadian and global marketplace

Let's build trust together as global leaders connecting Canadians to each other and to the world. Join us to lead Canada's digital economy and solve real-world challenges. We look forward to the next five years and beyond.

Contact us for membership options and benefits.

diacc.ca @mydiacc /company/mydiacc /mydiacc