

Digital Identity Ecosystems: Unlocking New Value

An interactive guide for executives

SEPTEMBER 2021



Contents

Welcome – the role of this guide 3

1 The case for digital identity now 7

1.1 Digital identity urgency 8

1.2 Digital identity in practice 11

1.3 Unlocking value with ecosystems 12

2 Identify your opportunity 14

2.1 Outline your opportunity 15

2.2 Using identity today 16

2.3 Prioritizing use cases 18

3 Understanding your ecosystem 20

3.1 Digital identity roles 21

3.2 Identifying key players 22

3.3 Your role in the ecosystem 24

3.4 Building trust in the network 26

4 Build or join an identity ecosystem 28

4.1 Existing or new ecosystems 30

4.2 Synergies with other ecosystems 32

4.3 Considerations for partnerships 35

4.4 Engaging the right partners 36

5 Define and deliver value 39

5.1 User-centric 41

5.2 Trusted 42

5.3 Interoperable 45

5.4 Public-private 48

5.5 Sustainable 50

6 Assessing the value and mitigating risk 55

6.1 Measure and refine 56

6.2 Assessing and mitigating risk 57



7 Different models for an ecosystem: four case studies 58

7.1 Thailand: Government-led national digital identity ecosystem 60

7.2 itsme, Belgium: Private sector-led national digital identity ecosystem 62

7.3 Velocity Network: Global digital identity ecosystem for career credentials 64

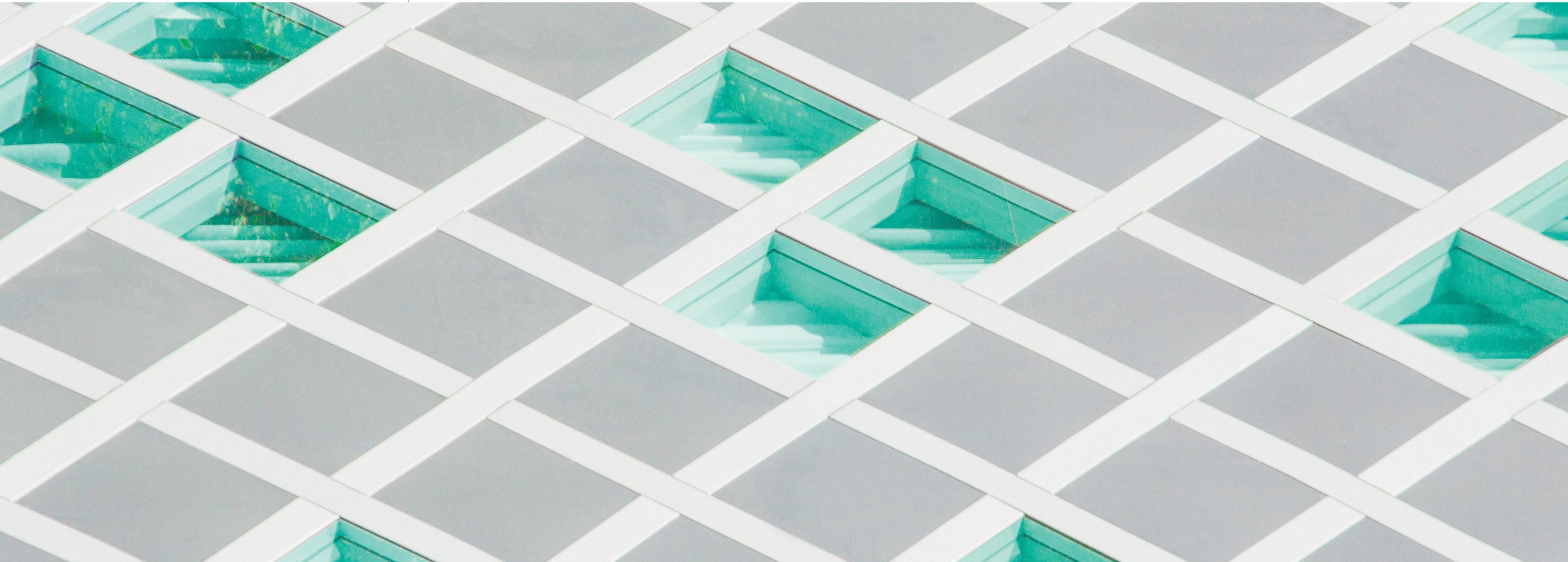
7.4 SoyYo, Colombia: Private sector-led national digital identity ecosystem 66

Conclusion 68

Acknowledgements 70

Endnotes 72

Welcome – the role of this guide



Since the beginning of the COVID-19 pandemic, both the scale and importance of digital interactions and services have accelerated. For providers of services, products and data to end users, it is now more critical than ever to be able to rely on the customer or partner at the other end of an interaction being genuine – from hiring a new contractor to transacting with a supplier. And it is not just digital interactions that rely on this kind of assurance. Physical interactions, such as someone having to prove their health status before travelling abroad or their age when buying alcohol or other restricted goods, require that the credentials they present can be trusted. As various aspects of our physical and digital lives become increasingly blended, the means to identify and verify ourselves, as well as the entities with which we interact, will also need to adapt. This is where digital identity comes in; regardless of whether interactions are physical or digital, it offers a means for all parties in an interaction to prove that they are who they say they are.

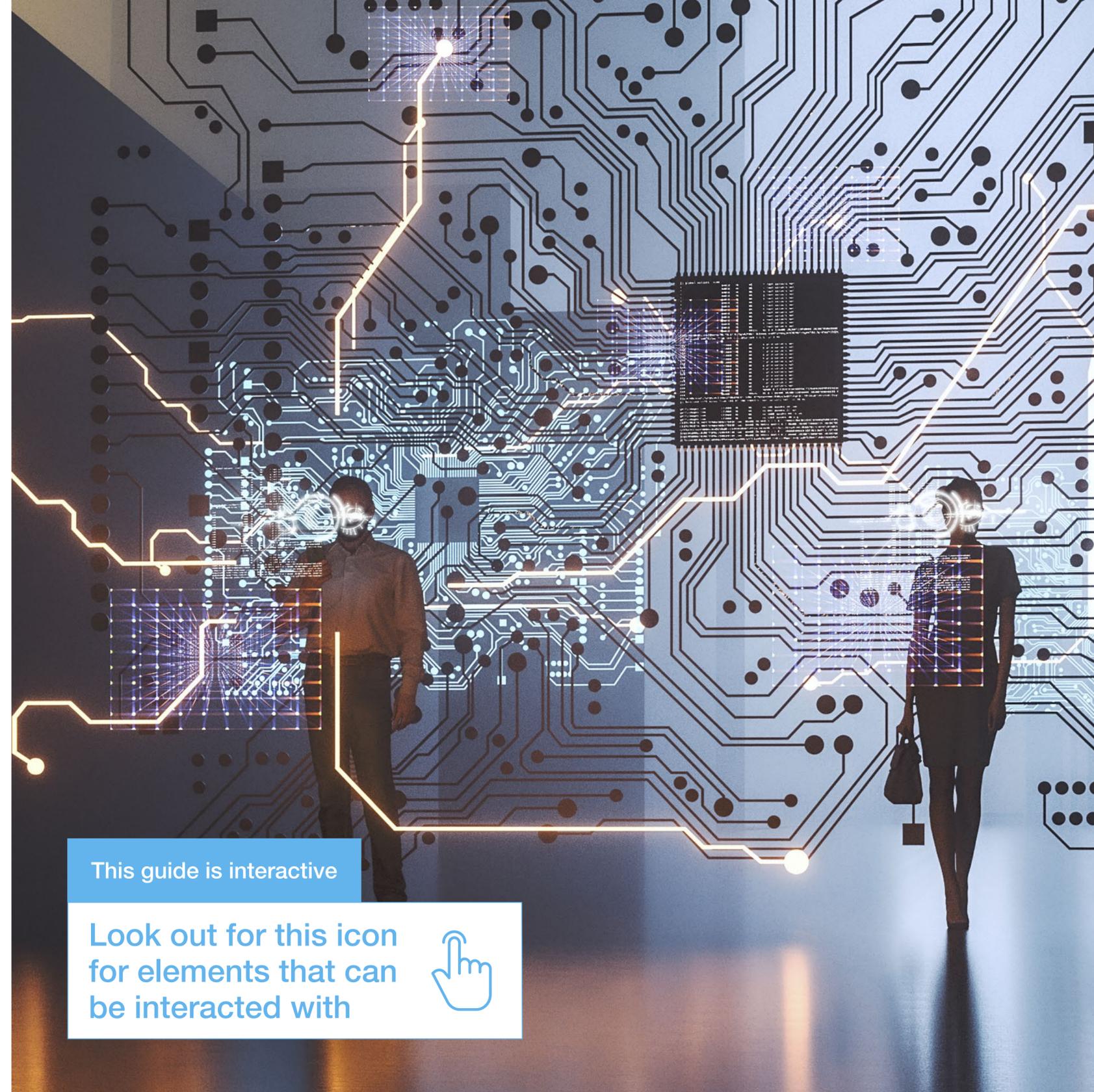
Digital identity can also help to deliver significant value by enabling greater efficiency for organizations, transforming user experience, reducing costs, and enabling the development of new services/products. Almost all organizations are now part of an identity ecosystem as almost all require identity data to operate, both in relation to managing their employees or serving their customers. Some

of these ecosystems feature organizations that we interact with in our daily lives: governments, healthcare agencies, telecoms, utility companies, banks and employers.

Digital identity ecosystems underwrite the environment of trust that organizations need to thrive while protecting the sensitive data that users are willing to share and/or verify to be able to participate in a particular interaction. In an age when trust is increasingly valued, users will choose the organizations who earn that trust through participation in an ecosystem that offers enhanced assurance.

This guide offers a set of tools that will help your organization to effectively navigate this process of transformation. It will help you understand why there is an urgent need to focus on digital identity, the role your organization should play, how to build new ecosystems or engage existing ones, and how to both define and deliver value for your users. Use the click links on the Contents page to navigate, each section offers insights and tools that will promote better understanding and assist with key aspects of strategic planning.

While the information in this guide has been presented in an order its authors feel is a useful one to follow in helping facilitate an organization's assessment of their digital strategy and the steps they need to take, the sections have been designed so that they can be read independently of one another.



This guide is interactive

Look out for this icon for elements that can be interacted with



What is the burning platform for identity?



Governments are investing heavily

Governments around the world are beginning to invest in digital identity services and frameworks. In 2020 Australia announced digital identity will be a major focus of its AUS\$800-million technology budget package.¹ As part of NextGenerationEU, France have allocated €72m on Digital Identity, while Germany plan to invest €200m into a European Identity Ecosystem.²



Flexible working is here to stay

COVID-19 resulted in historic shift in the job market, with working from home becoming the norm. 70% of the workforce are estimated to be working remotely by 2025.³ Trusted digital solutions are needed to support the increased demand for flexible working and onboarding, to verify education or identity credentials.



Governments are introducing Legislation

Governments globally are announcing new initiatives and instituting new regulations e.g., via Trust Frameworks and EU Digital Wallet.⁴ In response, organizations must act to understand their role and responsibilities in their ecosystem, and the impact or opportunities that digital identity will have on their operations.



Social responsibility is key within today's society

We are moving into a world where the identity of individuals and things is more important than ever. There is a need to act with integrity, responsibly handle data and protect privacy to safeguard citizens, e.g., trusted age verification without exposing an individual's identity.



Consumer digital identities are already here

Digital identity is set to transform many aspects of our lives and organisations need to be ready to determine their own path through what will be a fast-changing landscape. The market is already here, but it is fragmented. 6.2 billion identity apps expected to be in service by 2025, so now is the time to focus and collaborate.⁵



Acceleration of digitalization

The pandemic has created digital cultures and processes that are here to stay. On average, digital offerings have leapfrogged 7 years of progress in a matter of months.⁶ As digitalization continues to increase, Digital Identity is vital to ensure trust in these services now and in the future.

Key terms



Digital identity

A collection of individual attributes associated with a uniquely identifiable individual (e.g. name, date of birth, occupation, health status) stored and authenticated in the digital sphere, and which are trusted and used for transactions, interactions and representations online.⁷



Identity attributes

Criteria that are used to describe individuals, including (but not limited to) name, date of birth, nationality, address and fingerprints.⁸



Identity credentials

Issued to individuals by organizations that have verified an individual and can attest to their identity claim; additionally, identity credentials can also detail a qualification, competence or authority for an individual – examples include a passport, national identity card and driving licence.⁹



Identification

The process of establishing who an entity is within a given population or context; often takes place through identity proofing, which verifies and validates presented attributes, such as name, birth date, fingerprints and iris scans.¹⁰



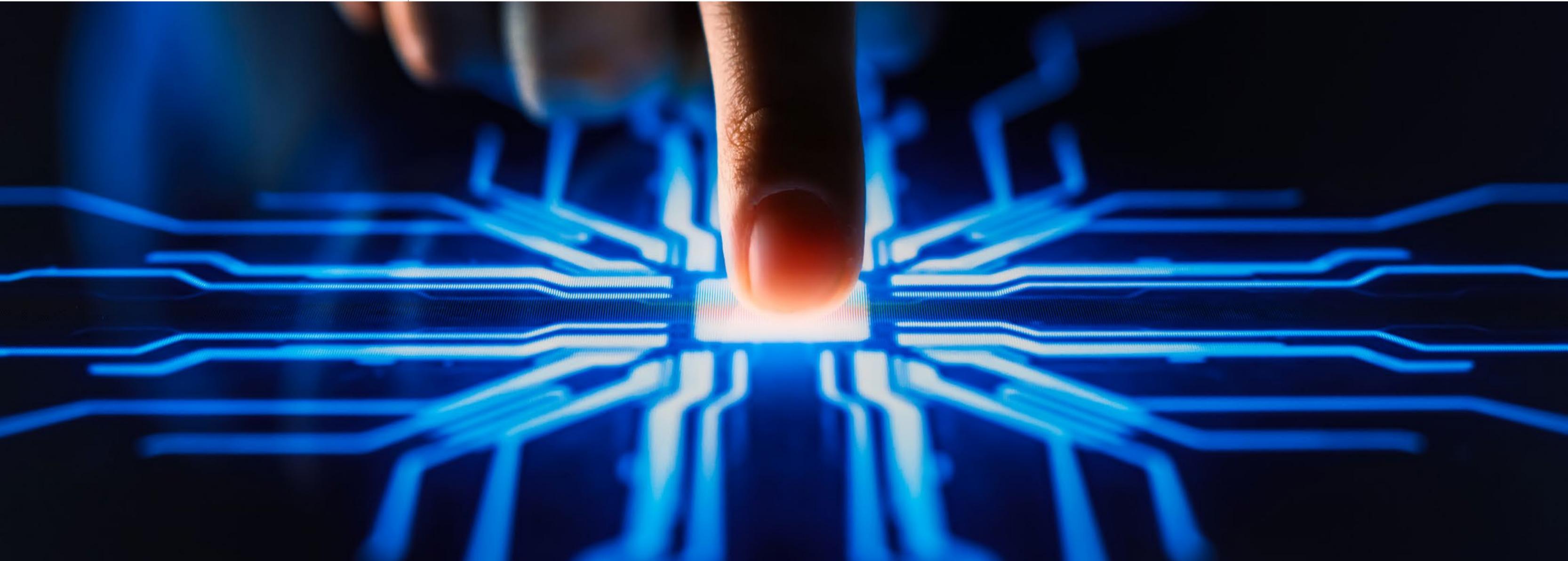
Authentication

The process of determining whether authenticators such as a fingerprint or password used to claim a digital identity are valid, i.e. that they belong to the same entity who first established that particular virtual identity.¹¹

If you need a reminder then click the button below to view this glossary at any point in the document

1

The case for digital identity now

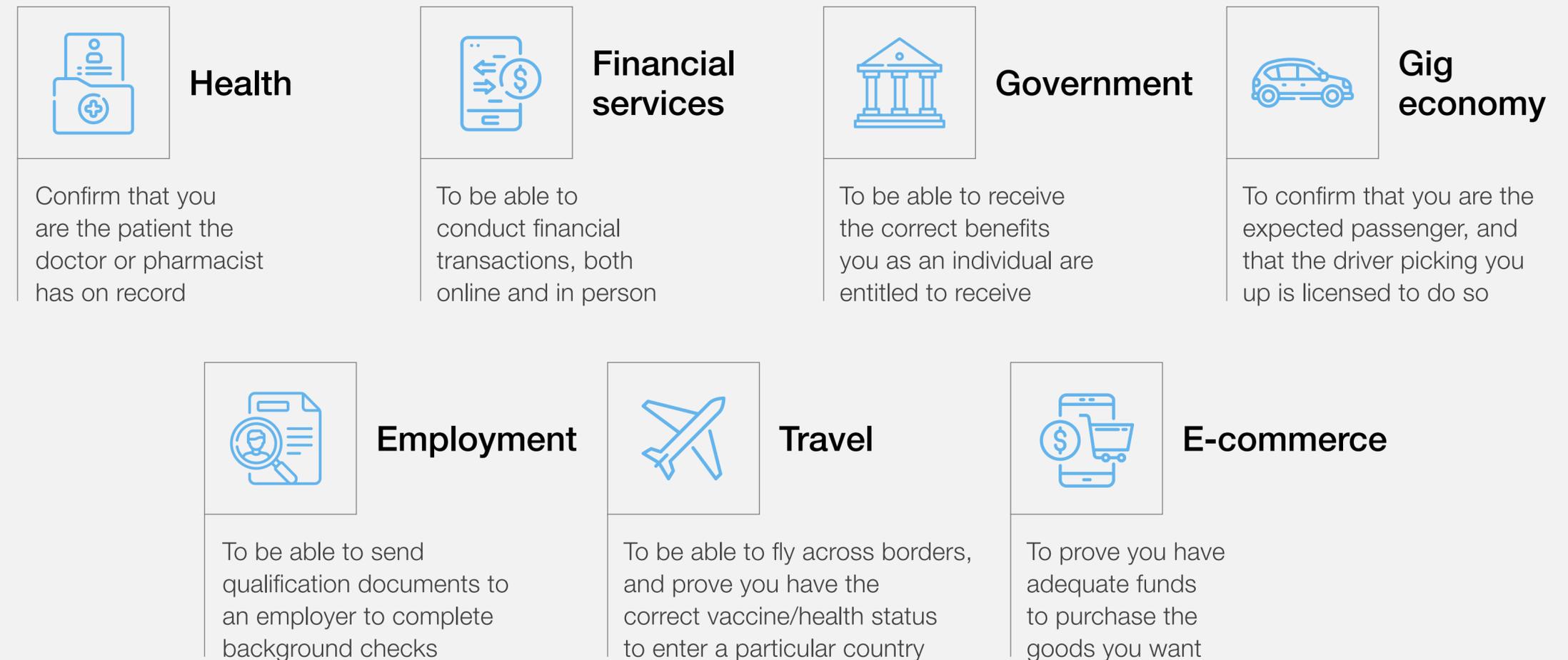


Digital identity urgency

Our lives are being fundamentally reshaped by an increasing reliance on digital forms of connection. With people, organizations and internet-enabled devices all interacting with one another virtually, we urgently require solutions that enable us to establish trust between ourselves and other people in the digital sphere, as well as carry out interactions that feel meaningful.¹² The COVID-19 pandemic has accelerated the need to identify and verify the identity of individuals and organizations across a wide range of sectors, in contexts as varied as the introduction of health-status certificates to remote onboarding for employees. This shift has also exposed the urgent need for greater international consistency, and collaboration across borders and sectors to enable individuals and organizations to both use and share their identity data more effectively and more securely.

FIGURE 1

Everyday requirements to verify your identity





In the context of international travel, for example, it is widely reported globally that there is widespread confusion among passengers about what type of credentials will be accepted by which country. Despite the relatively very low volume of travellers due to the pandemic, this lack of clarity has led to serious delays at borders; passengers are printing out credentials on paper, leading to increasing processing times and longer queues at airports. Both border forces and airlines have limited abilities to acquire and check the validity of passenger credentials in advance, which has hugely increased security risks and identity fraud. With organizations each having their own ways of describing and verifying identity data, it is often a confusing experience for the end user, as well as provoking worries related to privacy. This situation represents an opportunity to create value in an existing ecosystem where fewer but more trusted and standardized digital identity credentials would benefit everyone. To achieve that, organizations in the ecosystem must amplify the effectiveness of their efforts by working together.

As of August 2020, governments around the world had launched around 165 digital or partially digital identity schemes, and the market size for global digital identity solutions is projected to grow to \$30.5 billion by 2024.^{13,14} With our digital lives expanding so rapidly, and as we access a huge range of different services online, we are inundated with different means of digitally identifying and verifying ourselves. This often creates confusion and apathy, as well as making it far harder for an individual to know whether or not the service they are using is real and can be trusted. On the other end of all these new means of interaction, organizations also need to be able to trust that their users are who they claim to be, and in a way that not only creates value but also respects those users as individuals.

From the number of recent announcements relating to new legislative digital identity initiatives made by administrations around the world (e.g. the European Digital Identity Wallet scheme), as well as proposals to regulate private sector organizations globally, it is clear that the transformation of how we identify and verify ourselves has already begun.¹⁵ Organizations are beginning to reap the benefits of this cultural shift; for example, in India, costs to identify a customer (Know Your Customer (KYC) costs) were reduced by 86% via the new nationally recognized approach to digital identity, Aadhaar, and in Estonia, the time taken to register a new company in a paperless way using digital identity was reduced from 5 days to 18 minutes.^{16,17} As governments invest in and create new policies in this area, organizations need to understand how this will impact their future and reap the benefits. Digital identity has the capacity to transform both how organizations operate and how they interact with their users, and the trust and value that will be built as a result of embracing it will be critical to their success. It's vital, then, that organizations act now and begin to define their journey through that transformation.

BOX 1

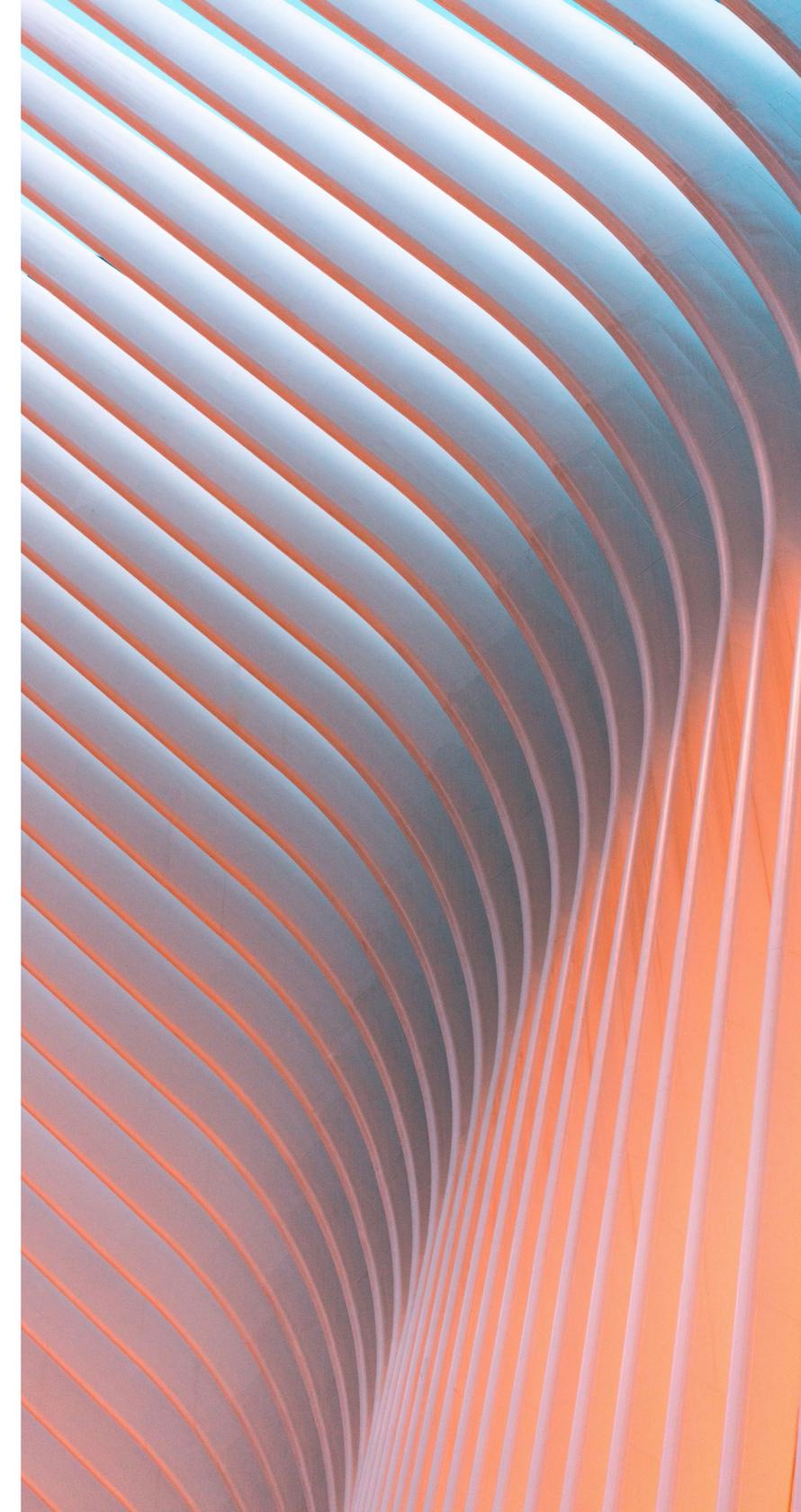
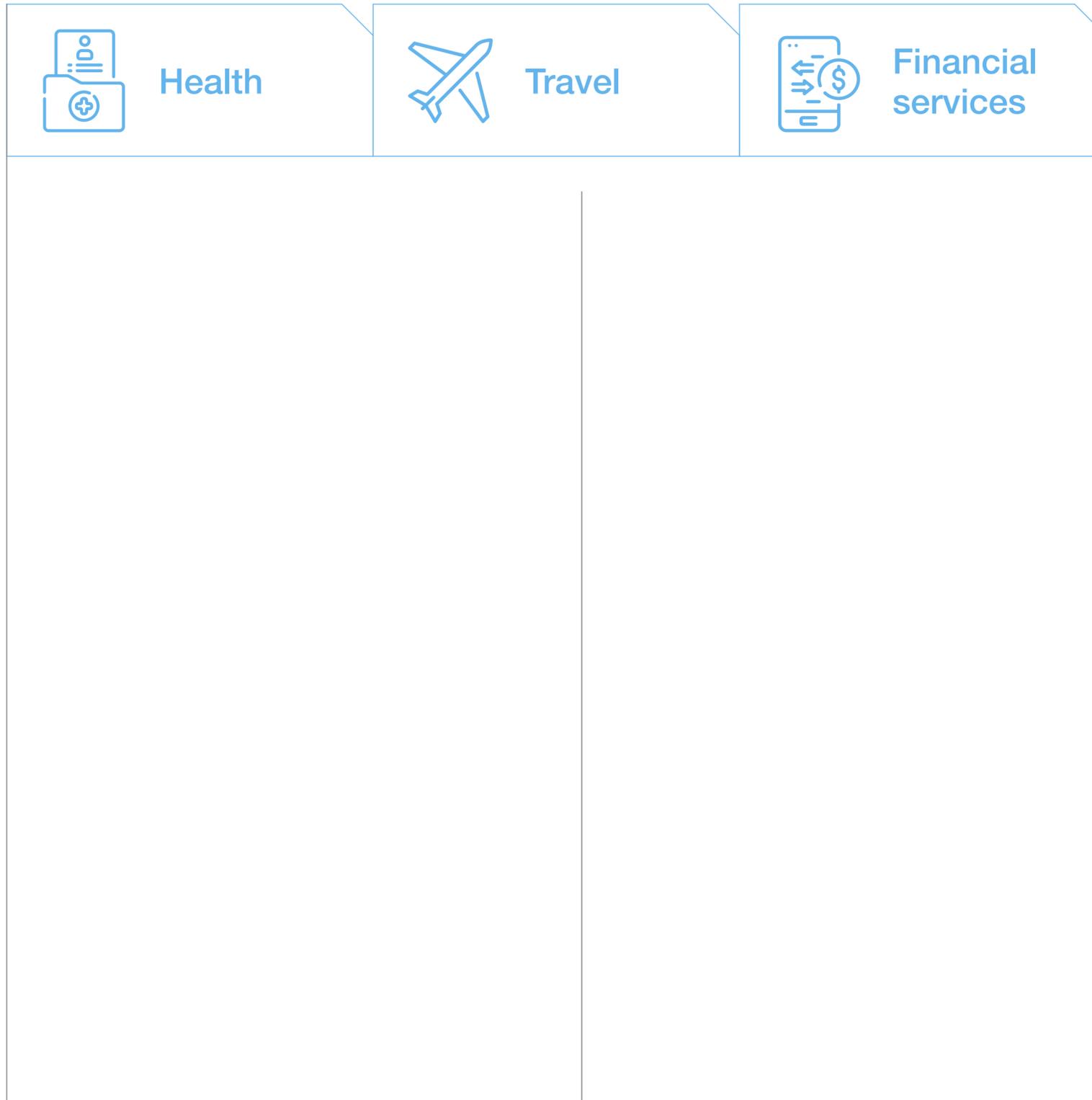
COVID-19 and digital identity in Belgium



During the COVID-19 pandemic, remote, digital-first, touchless interactions became a necessity for organizations. COVID-19 also represented the opportunity to use digital identity to facilitate trusted interactions between organizations and individuals for new use cases and services. In Belgium, they did the following:

- Online application for COVID-19 financial relief: a paper-based process that needed to be accelerated, digitized and remote
- COVID-19 vaccination app: identification of the correct person, and uploading of proof of vaccination and results of PCR tests (an enabler of a safe return to work, as well as increased use of travel and access to events, etc.)
- Online consultations with doctors: the need to identify and verify medical personnel, and to support a remote doctor-patient relationship
- COVID-19 testing platforms: the need to verify the identity of medical personnel accessing data

Digital identity in practice



Unlocking value with ecosystems

A **digital identity ecosystem** is a network of public and private sector players that work together to define, build and execute user-centric means for individuals to prove their identity across organizations. The value of such a network is based on the depth and breadth of collaboration it embodies, as well as whether or not it can generate greater usefulness, trust and efficiencies than the combined value of what each participant could contribute individually.²⁰

Collaborative innovations in digital identity involving different industries and sectors are key to the generation of new value for businesses and users, while also helping organizations realize efficiencies and growth.²¹ When offered a choice, users will tend to transact with businesses they can see already operate within trusted, privacy-enhancing ecosystems. The national passport is an identity credential that acts as the foundation of many identity ecosystems, being accepted across borders and by different sectors, and used in numerous contexts. Whether established or developing, digital identity ecosystems provide greater value for both individual users and organizations when they adhere to the following five principles: **user-centric**, **trusted**, **interoperable**, **public-private** and **sustainable**.

FIGURE 2

Principles of an effective digital identity ecosystem



All players in a digital identity ecosystem should be able to clearly define the value they bring to, and gain from, their involvement in such a network. The following describes what benefits can be achieved from moving into such a network:

User experience

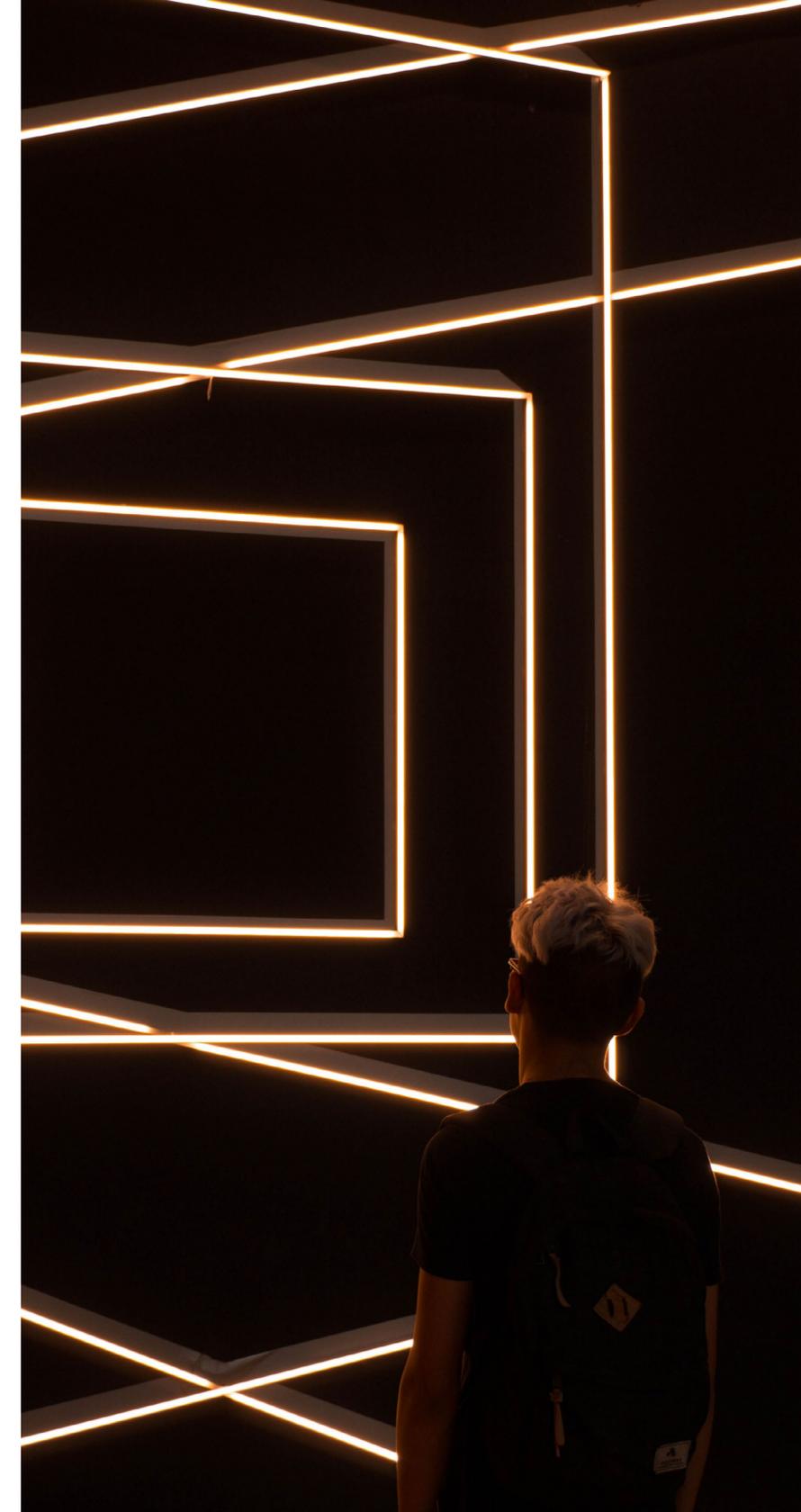
Business opportunities

Costs and risk of fraud



Digital identity is getting more attention as executives have factored it in their IT and business plan to do face-to-face and non-face-to-face transactions, such as digital onboarding for account opening or lending businesses. Major banks have initiated to be National Digital ID's proxy to provide one-stop digital identity solutions for their related companies and business partners.

Boonsun Prasitsumrit, Chief Executive Officer at National Digital ID Co. (Thailand)



2

Identify your opportunity



Outline your opportunity

Before you consider whether the value digital identity can bring to your organization makes it worthwhile for you to begin the journey towards adopting the principle operationally, you first need to look at how (or even whether) your organization uses identity data. Having established the context, including any use cases you already offer (it's very likely your organization already does), you can then think about potential new use cases for your users. You need to work out which of these are likely deliver significant value, both to the individuals and other entities that use your services, and to your organization. To identify which use case to make the strategic focus of your transformation as an organization, you'll need to consider not only its value but also its frequency. Choosing to develop the most viable use case will not only enable greater user adoption but also accelerate new business opportunities, promote efficiency gains and improve user experience. Using the tools in this section will help you understand how to provide repeatable value to your users, as well as to enhance opportunities for your organization to realize new value for itself.

Current use of digital identity

Daily there are several touchpoints where implicitly or explicitly an issuance or verification of credentials is done by your organization. What are your touchpoints?

Use case prioritization

a. Map pain points and frequency

Providing high-value use cases is key to realizing the beneficial adoption of digital identity. It's critical to identify which of your organization's business processes are characterized by repeated friction caused by the need to identify/verify identity for the user. Individuals are far more likely to use a service if it is both quick to use and makes their life easier. Using the **Use cases priority matrix** tool provided, assess use cases to understand which ones can provide the highest user value.

b. Prioritize potential

When thinking about the different use cases you could potentially offer individuals, you need to ask the right questions:

- 
Improving customer experience
 Can you avoid most identity checks and re-checks for your users, partners and employees?
- 
Reducing costs and increasing efficiency
 Can you reduce the number of inefficient (manual) processes relating to identity that impact your organization, individuals and other entities?
- 
Creating new business opportunities
 Can you offer identity credentials that others might use?

Using identity today

Key question



What does your organization currently do with identity data?

Outcome

This tool should help you understand the way your organization currently works with identity data and what services/transactions require it; this knowledge will feed into helping you think about which use cases are relevant to your organization and which interactions could be improved via a digital identity ecosystem.



There will be numerous business processes in your organization that involve the issuing or verification of identity data. To help you understand the different ways in which your organization currently works with identity data, use Figure 3 to document the various interactions that feature in each of these processes: those involving users, employees, suppliers and government agencies, etc. A clearer understanding of which of your services and/or transactions need to involve this data will allow you to better identify potential use cases for which you could provide an improved and more beneficial service via belonging to a digital identity ecosystem – ideally, one that allowed for trusted credentials being shared across sectors and borders. Listed in Figure 3 are some potential use cases that are relevant to a range of different industries; please add any that will be specific to your organization’s industry and geography (e.g. KYC and background checks).



FIGURE 3

Type of interaction	Do you use identity credentials for this interaction?	If yes, who provides the credentials you verify?	If yes, detail how you use the identity credentials provided

This table can be filled in 

Prioritizing use cases

Key question



How do you select and prioritize use cases for digital identity ecosystems?

Good digital identity can bring efficiency, trust and user experience – if it is used by individuals. The more useful digital identity is, the easier it is to gain more users. To gain adoption, there must be repeated value in the use cases offered to individuals, meaning that they will be encouraged to use the solution regularly to reduce friction and improve experience, and thus continue using it so that it becomes habit-forming. Using Figure 4, assess which use cases might maximize value for individuals, and thus which are more likely to result in greater adoption and, in turn, greater value for your organization and even other potential partners.

When thinking about the different use cases you could potentially offer individuals, ask the following questions:

✔ Improving customer experience

- What are the most frequent identity checks and rechecks for your users, partners and employees?
- Can you reduce the friction in these interactions?
- Are these daily/monthly versus a few times in their lives?
- What are the pain points in this particular user journey?
- Are there any processes that end users often complain about/get frustrated by/causes them to drop out of the service, or which generate a large number of support calls?

✔ Reducing costs and increasing efficiency

- What manual identity checks does your organization need to conduct?
- Can you reduce inefficient manual processes for both the organization and the individual?
- Are there identity credentials that can be reused across different organizations, industries and sectors?
- Can I provide individuals with a more efficient means of accessing our services/goods?

✔ Creating new business opportunities

- Will organizations trust the identity credentials you create?
- Can you offer identity credentials that others will pay to consume?
- Can you work with organizations outside of your industry to create and build use cases where identification is key?
- What services could you build with other organizations to improve an individual's frequent transactions/services?

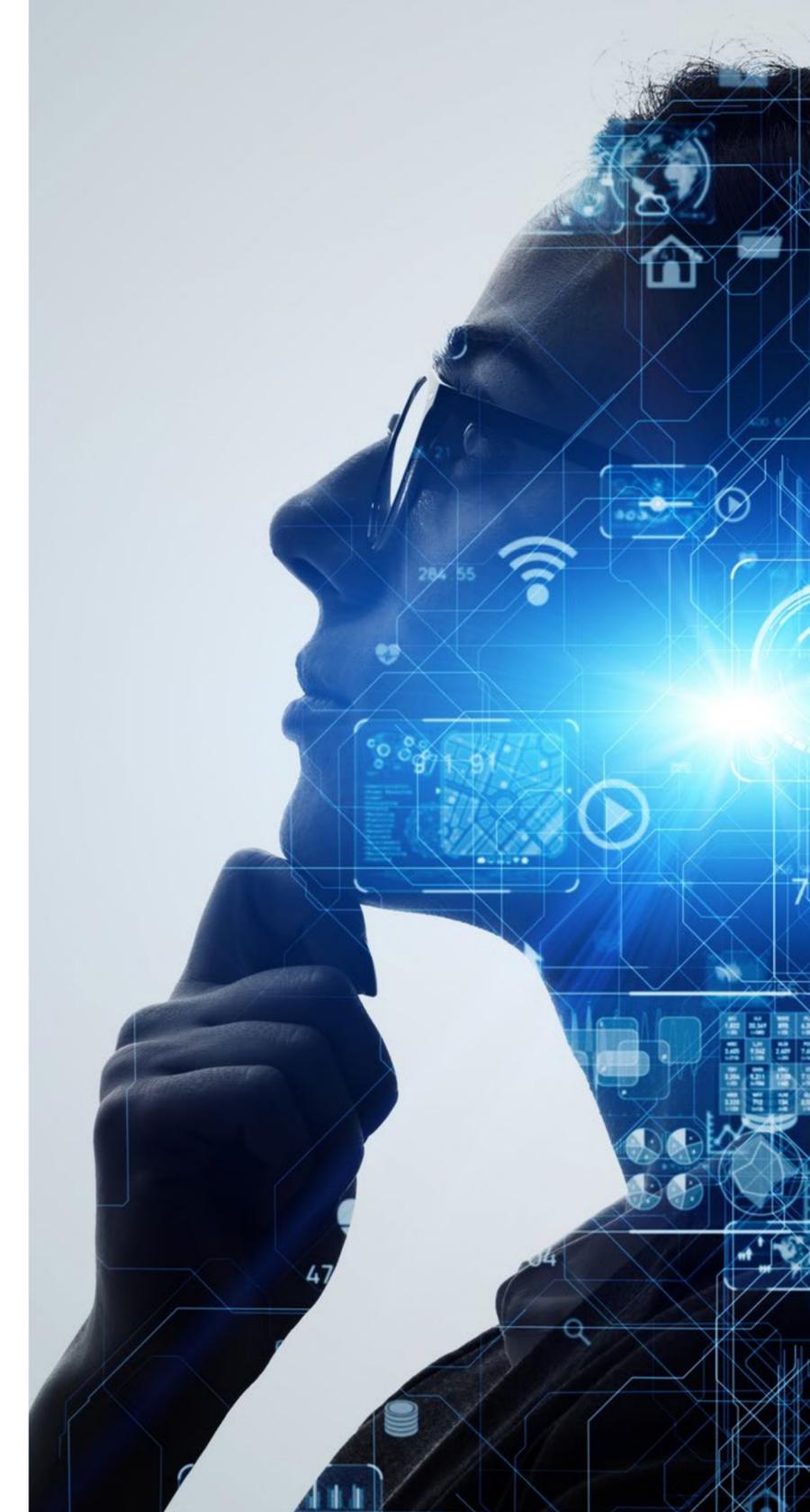
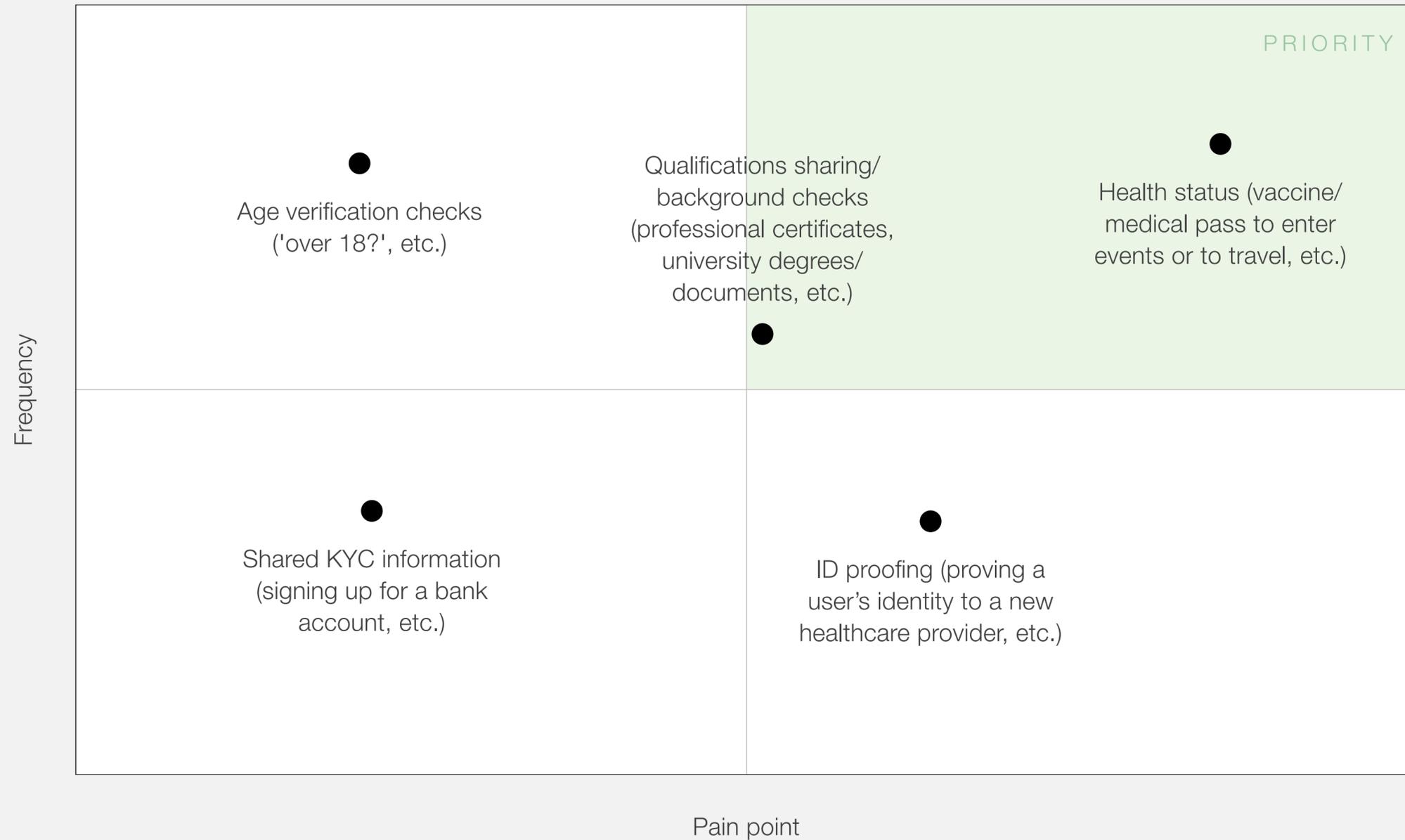


FIGURE 4

Use cases priority matrix (example)



Please adapt to the specific context in which your organization operates – this is simply an illustration of one set of possibilities

Outcome

This tool should help you to think of different use cases your organization can offer, and understand how to prioritize them to maximize the value for the individual, resulting in greater adoption and, in turn, greater value for your organization.

3

Understanding your ecosystem



Digital identity roles

Key question



What are the key roles in a digital identity ecosystem and who is best placed to fulfil them?

Outcome

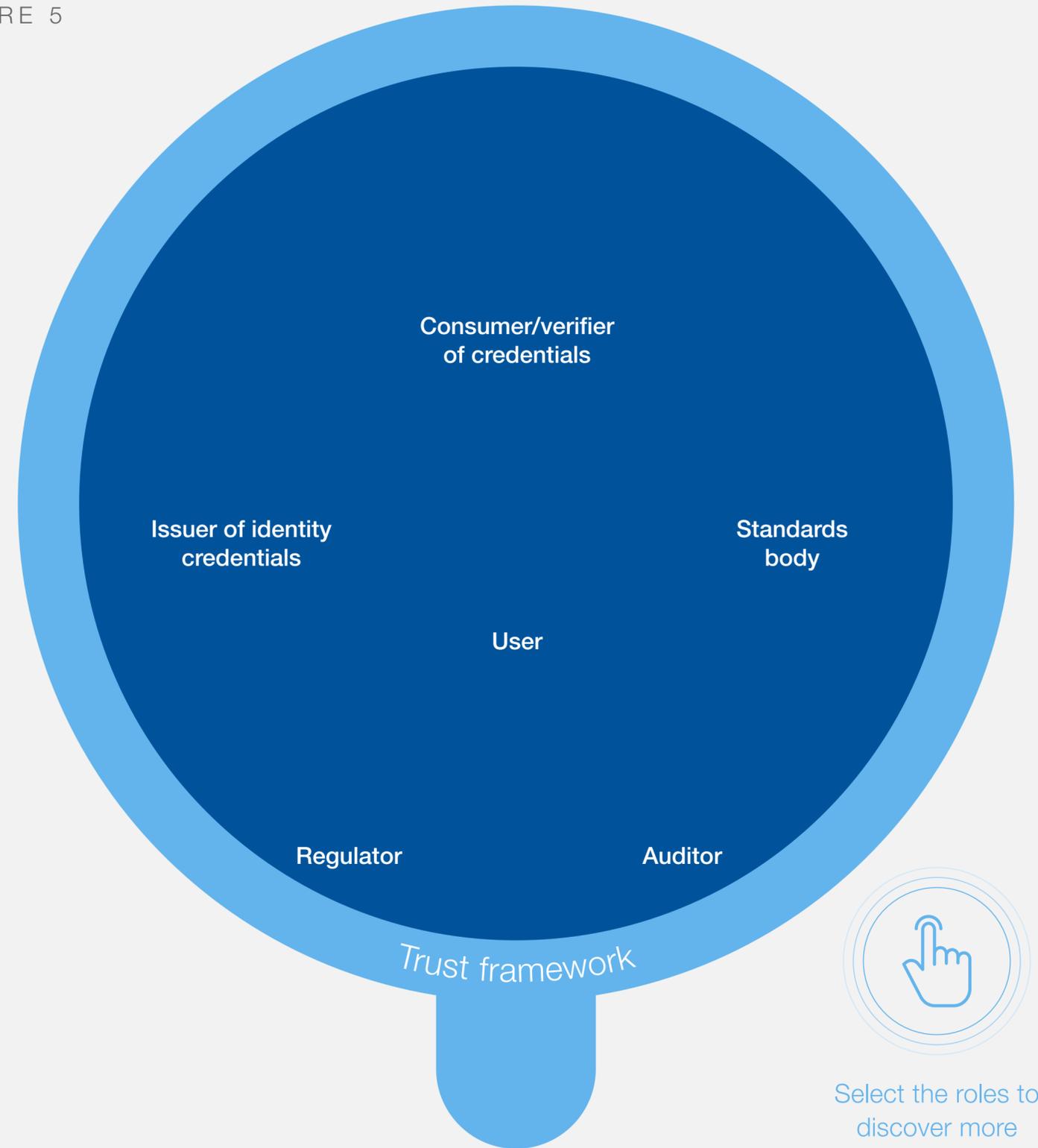
This tool should help you understand the different roles required in a digital identity ecosystem and the types of organizations you will need to partner with.



It is important to define a clear purpose, and thus a clear role, for each organization in an ecosystem. Although any of the roles described in Figure 5 can be fulfilled by organizations in either the public or private sector, not all of them will be applicable to every digital identity ecosystem – the actors involved will be dependent on the use case. In addition, most of these roles will most likely already feature in your ecosystem, and you may already fulfil multiple roles within a digital identity ecosystem, dependent on the use case (e.g. sometimes a consumer/verifier, sometimes an issuer). Being clear about roles that need to be fulfilled to operate an effective network means you are more likely to be able to identify and create effective relationships with the right kind of partner organizations.



FIGURE 5



Identifying key players

Key question



How do you identify the key players in your current ecosystem, and your relationship with them?

Outcome

This tool should help you understand the various structured interactions in which there may be an opportunity to gain efficiencies, as well as to improve user experience across the entities in your current ecosystem with which you interact with through digital identity; if there are standardized processes for certain interactions with users, partners, employees or government agencies, this presents the opportunity to use a digital identity ecosystem to deliver greater value.



Using Figure 6 will help make it clear to you who does what in the ecosystem in which your organization currently participates, and what identity-related interactions you currently have with each of them. Fill in the following information: the entities your organization issues identity credentials to, the existing processes and tools used, and the context for issue (e.g. account number and logins to enable customers to access their accounts). Next, fill in who your organization obtains identity information from, the reason you need it (e.g. regulatory compliance or a service-driven need) and the existing processes and tools that are used to collect this information. Finally, determine whether the use of tools and processes are consistent across your organization and across the wider ecosystem. This is designed to help you understand which organizations are currently part of your ecosystem, and what identity-related interactions you currently have with them.



FIGURE 6

These tables can be filled in 

Issuing identity credentials

Which organizations/entities?	What's the existing process?	What's the purpose/reason?

Verifying identity information

Which organizations/entities?	What's the existing process?	What's the purpose/reason?

Your role in the ecosystem

Key question



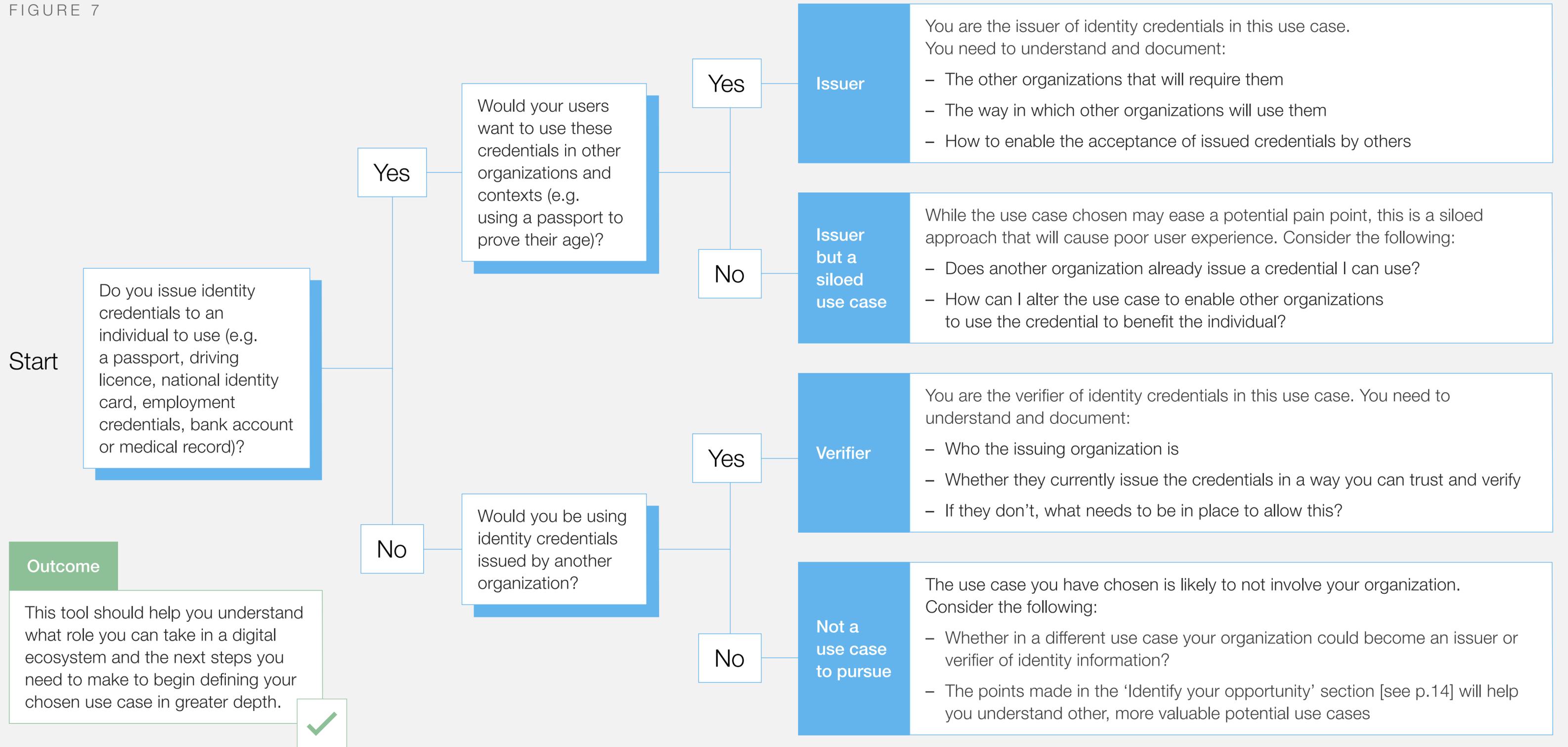
What role or roles do you currently play? Would you issue or verify identity for your specific use case?

It is likely that most organizations to which readers of this guide belong to will be either an issuer of identity credentials or a consumer/verifier of identity credentials – some possibly both. To better understand the role your organization currently plays, to develop it as part of your digital identity transformation journey, you must first understand it in operational context. Use Figure 7 to help clearly identify your organization’s role in any selected use case (is it the issuer, the verifier or both?), to identify whether that use case is worth pursuing in strategic terms, and understand how to begin defining the use case in greater depth.

Please note, this explanatory tool does not encompass the more niche roles in a digital identity ecosystem – regulator, auditor and standards body – as it’s likely members of the organizations that fulfil them will already fully understand their position. Remember that the role your organization plays might change according to which use case you choose to describe. In addition, before embarking on using this tool to describe a particular use case, it’s worth revisiting the section ‘Digital identity roles’ [see p.21] to make sure you are clear about the nature of each of the roles.



FIGURE 7



Building trust in the network

Key question

What identity issuers do you currently trust within your ecosystem, and what needs to be in place to enable trust within it?



Digital identity ecosystems are only valuable to an individual if the credentials which they issue can be accepted and trusted in multiple contexts. In turn, the more those credentials can be accepted and trusted in the ecosystem, the greater value they provide. 'Trust frameworks' and 'trust anchors' are both an important means of helping achieve trust.

What are trust frameworks?

As described earlier in this guide [see p.21], trust frameworks are typically a common set of principles, rules and standards that organizations in a digital identity ecosystem adhere to, allowing the reliable transfer of credentials between themselves and all the other participants. Organizations adhere to a set of rules defined by the framework, with actions being checked against the protocols as a means of embedding mutual trust within the ecosystem. These rules can operate across industries, across geographic territory or even internationally (e.g. those instituted by the International Civil Aviation Organization). Some of these frameworks underpin many interactions in our everyday lives. For example, to rent a flat, most landlords require proof of identity in the form of one or other type of government-issued identification – trust between the government (the issuer of the identity) and landlords is implicit.

What are trust anchors?

Trust anchors within a digital identity ecosystem are traditionally those organizations that complete identity-proofing checks as a means of then issuing traditional identity documents, such as passports, national identity cards and driving licences. Traditionally governments and regulated organizations (e.g. banks and utility companies) are held in a position of trust, and are subject to regulatory requirements in verifying the identity of their users.

Use Figure 8 to help you understand what else is needed in order to accept digital identity in a particular ecosystem – either from yourself or another participant organization. You can then determine who the current trust anchors are in your ecosystem, what the current position is on issuance and acceptance for digital identity credentials, whether anything needs to change in order for those credentials to be issued and accepted, and who might need to be part of the ecosystem to help enable change.

FIGURE 8

This table can be filled in 

Question	Answer
<p>Who are currently the trust anchors in your ecosystem? What identity credentials do you accept and who issues them?</p>	
<p>What sectors or organizations do people and organizations traditionally trust?</p>	
<p>Are there explicit trust frameworks in place to enable organizations to issue and accept trusted digital identity credentials? If not, what needs to change to be able to issue or accept these?</p>	
<p>Is your organization able to position itself to issue or accept trusted digital identity credentials? If so, what is required to do this?</p>	
<p>What is required for other organizations to accept your issued credentials? Are these already in place?</p>	



In our commercial approaches we have seen that the companies perceive great value in having an onboarding process with less friction and stronger fraud control against impersonation. It is also valuable to finish a transaction with an e-signature process that avoids non-repudiation.

Santiago Aldana Sanín, Chief Executive Officer, SoyYo

Outcome

The answers you give should help you determine who the current trust anchors are in your ecosystem, and what the state of issuance and acceptance currently is for digital identity credentials, and thus if anything needs to change in order for them to be issued and accepted; once the required changes are identified, you can determine who needs to be part of the ecosystem to enable these changes.



4

Build or join an identity ecosystem



We all interact with users, employees and providers as part of normal business operations, and most likely your organization is already issuing or verifying identity credentials.

It is also very likely that the issuance and verification of these identity credentials are conducted in a siloed manner. For example, contractors or consultants may have to complete background checks for various clients or organizations when working with them. In most cases, these checks have to be repeated every time one of these people moves between clients, resulting in unnecessary repetition and lost time, and therefore lost value for all parties involved.

Your organization aims to reach a point where digital identity can enable your services and can be widely used by individuals in more organizations in an ecosystem. Using these tools will enable you to understand whether you could join an existing ecosystem or if it would be better for you to create a new one, how you should choose and engage the right partners, and the next steps involved in advancing or building a digital identity ecosystem.

4.1 **Should I join an existing ecosystem or initiate the building of a new one?**

4.2 **What existing digital identity ecosystems are there, and what are the synergies?**

4.3 **Identify and implement new partnerships**

Choosing the right partners

Engaging the right partners

Existing or new ecosystems

Key question



Should you join an existing ecosystem or create a new one?

Outcome

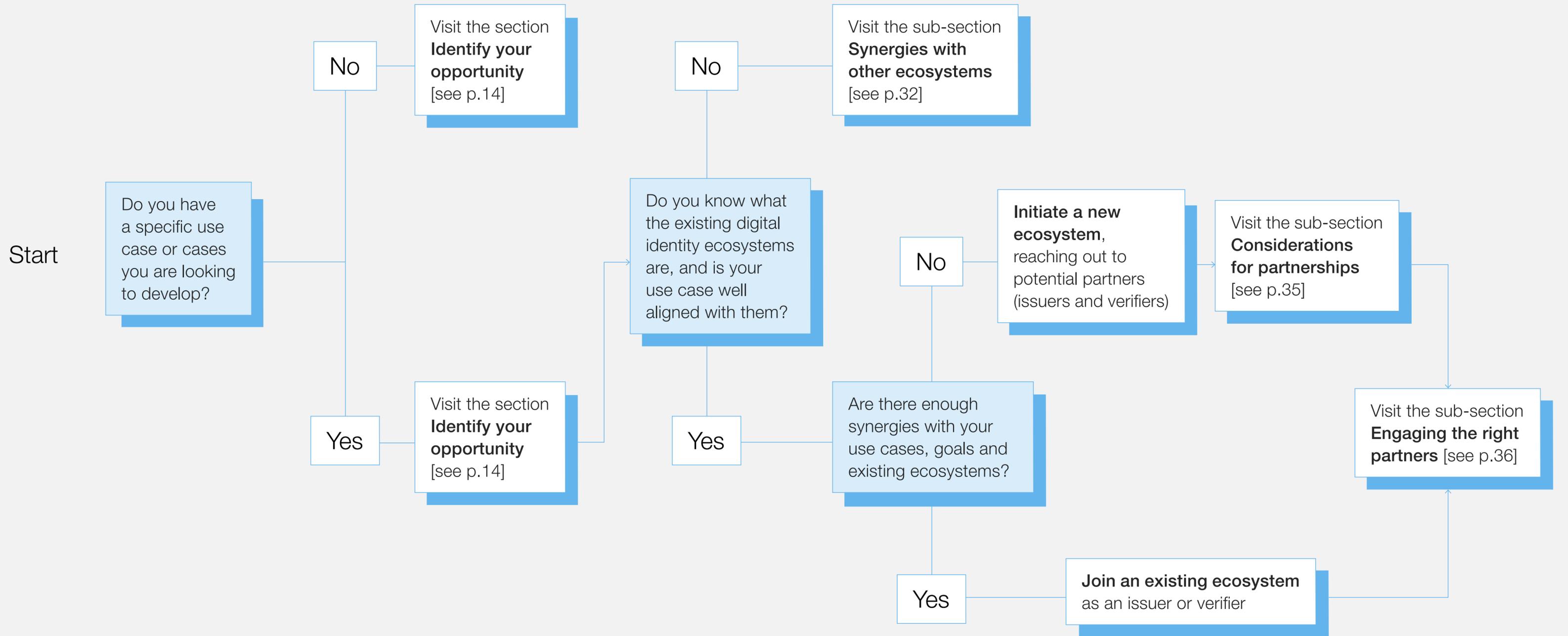
This tool should help you decide whether you are willing to utilize the benefits from an existing ecosystem for your digital identity use case, or instead that you need to convene new potential relationships in order to create greater value for your end user.



Depending on the existing relationships your organization has with others, and how developed digital ecosystems are in your market or sector, there are several choices you can make in your transformation journey towards digital identity – to help enable trust in your services and allow identity to be widely used by individuals. Use Figure 9 to help you understand whether you should be looking to utilize the benefits of an existing digital identity ecosystem for your use case, or you should convene new potential partners in order to offer greater value for your end user.



FIGURE 9



Synergies with other ecosystems

Key question



What existing digital identity ecosystems are there, and can they be used for your chosen use case?

Outcome

If there are existing digital identity systems that support your organization, use case and jurisdiction, there is potential for you to leverage these to accelerate greater value creation for your organization and users. However, if using the tool makes it clear your use case does not fit with any existing digital identity ecosystems, you may need to create a new one, beginning with identifying potential interested parties.



Given there are already a large number of digital identity ecosystems, before looking to create a new one it is well worth considering whether you can join an existing one that will allow you to accelerate value creation for your organization by unlocking certain benefits, such as a larger network that offers more choice and services to users, a larger user base and increased access to users. You may find that many of your existing partners are already a part of an ecosystem. Before using Figure 10, research the different relevant digital identity ecosystems that currently operate in your own country and internationally, and speak to other industry leaders to help you understand which ecosystems could support the use cases you want to pursue and who is involved in them. The ones already within your geographical territory and your industry, which are recognized by government and support your use case, are the best ones for your organization to look to become involved with.



FIGURE 10

This table can be filled in 

A. Which digital identity ecosystems already exist and what do they cover?

B. How aligned is this ecosystem with the vision of your organization?

Geography	Initiator	Name	What use cases are supported?	What industries are using, trusting and accepting digital identities?	Which organizations are involved?	If private-sector led, does it have government recognition?	Does it or could it support your use case or cases?	Do you have existing relationships with the members?	What stage is the initiative at (e.g. test, pilot, live)?
Within your own country	 Government								
	 Private sector								
International	 Government								
	 Private sector								

Example 1

(within a delimited geographical area, led by both private and public sector organizations): Germany's identity ecosystems offers organizations several options for trusted interactions

Example 2

(international, led by the public sector): the European Commission's digital identity ecosystem allows organizations and users to interact across borders

Example 3

(international, led by the private sector): Mastercard's ID Network enables digital interactions across ecosystems

Considerations for partnerships

Key question



What are the main things you should consider when choosing the right ecosystem partners?

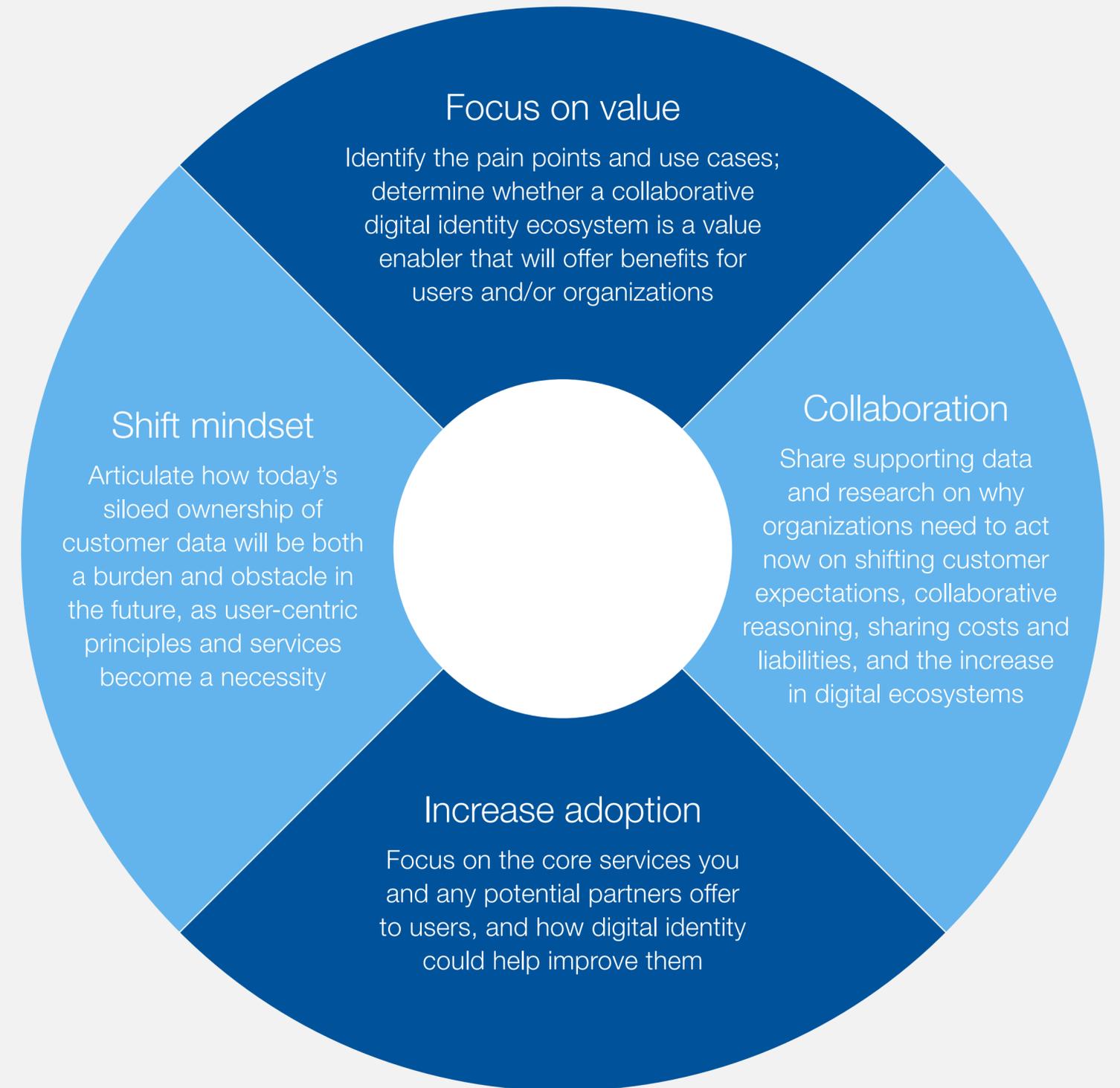
Outcome

This tool should help you understand what needs to be considered when selecting suitable partners for your ecosystem; use the 'Do' and 'Don't' guides to ensure you are able to decide who will provide the best value for your users and organization, and to avoid the mistakes that have resulted in low usability for users.



The following information can help you understand the key criteria in selecting the most appropriate potential partners for a new ecosystem, and the Do's and Don'ts of working together to reach a common goal, while avoiding the kind of mistakes that result in low usability and poor value for both your organization and users:

FIGURE 11



Engaging the right partners

Key question

?

How do you approach and then work with new partners?

Outcome

This tool should help you understand how to approach organizations, and how to then collaborate with multiple participants to form a common vision, focusing on a particular use case to prove the value of digital identity transformation in your ecosystem; once value has been proven with the use case for all parties, work can begin on additional use cases and the development of a wider strategy.



FIGURE 12

It is important to engage widely with both public and private sectors early on in the transformation journey, which will help to navigate factors such as regulation and user adoption. It is also crucial to understand and agree on respective roles, expectations and a way of working (something

which can be further clarified via a governance model). Using Figure 12, first identify where you are on the journey and whether some of the activities described can be completed in parallel. Next, follow the steps for engaging the right partners for your ecosystem:

Select to explore the steps for engaging the right partners for your ecosystem



Building supply and demand in a digital identity ecosystem: itsme, Belgium



Created by Belgium Mobile ID, the itsme digital identity scheme is an open ecosystem that allows all organizations who wish to do so to become members (currently around 4,000), and which provides services that range from basic log in and shared identification up to more advanced NFC (Near-Field Communication) authentication. itsme has taken a phased and collaborative approach to showcase and align with individual organizations and industries how they can benefit from digital identity, and build ecosystem-based use cases driven by digital identification.⁷⁰

Phase 1:

Industries and sectors: the key players in each industry need to adopt first, with impetus then spilling over to the smaller players

Financial services – Initial case, bringing high volumes and first movers

Travel – Identification for travel – use cases introduced later due to international complexity

Health – Digitalizing a mainly paper process and securing it (previously, unsafe tokens were used)

Phase 2:

Cross-sector use cases

After certain industries adopted digital identity, cross-industry horizontal use cases became possible, e.g. individuals can benefit from digital banking or health services as part of their travel journeys, bringing increased value and impact to the economy (the need to respond to COVID-19 offered an especially strong case for cross-sector collaboration for applications such as remote work or COVID relief).

5

Define and deliver value



It is important to purposively try to build a 'good' ecosystem, i.e. one with the right attributes to drive user adoption. Click on the following sections to learn more about the ways you can achieve this:

1
User-centric

2
Trusted

3
Interoperable

4
Public-private

5
Sustainable



Select the principles
to discover more

User-centric

Key question

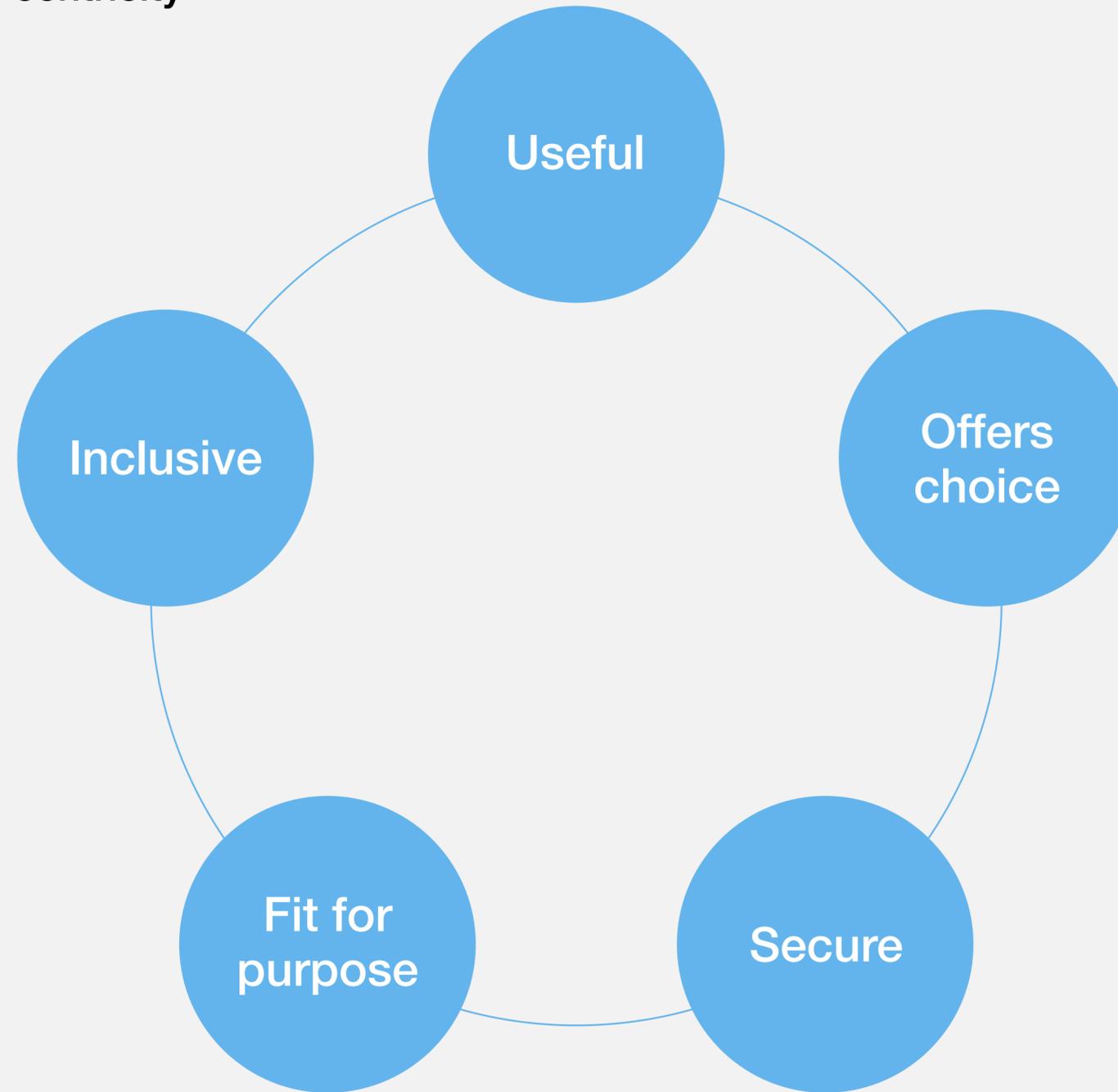


What are the key criteria to ensure user-centricity in your ecosystem?

One key criteria for a digital identity system to reach its full potential is for it to be controlled by the user, helping avoid any negative effects (e.g. poor user experience, data misuse and lack of privacy or security). Five equal elements of user value that a ‘good’ digital identity must satisfy were defined in a September 2018 report by the World Economic Forum entitled [Identity in a Digital World: A new chapter in the social contract](#); these are: fit for purpose, inclusive, useful, offers choice and secure – if all are met the digital identity can be said to be user-centric, and is more likely to be adopted.⁷¹



FIGURE 13
User-centricity



Select the elements of user value to discover more

Outcome

This tool should help you understand the criteria your ecosystem needs to adhere to that will enable it to be user-centric, as well as to improve user experience.



Trusted

Key question



How do you ensure trust can be embedded in your ecosystem?

The need to develop digital identity – a means of easily and securely identifying and verifying a person or other entity’s identity digitally – has been clear for some time, but has been amplified by the COVID-19 pandemic, which has accelerated our transition towards the digital world, from online shopping, paying bills and mobile banking to virtual doctor’s appointments, online learning and remote work. More robust means of digital identification can help to safeguard our privacy and security in these interactions while creating more seamless and efficient experiences and reducing fraud across sectors and industries.

For digital identity to be accepted across borders and sectors, organizations need to trust the data and credentials presented to them. Without general acceptance, the value of the digital identity significantly diminishes. To embed trust in ecosystems, the correct governance and frameworks need to be developed that allow for organizations to adhere to a set of principles, operate according to a set of rules and adopt a set of standards within a given environment. For example, the national passport is a credential that is trusted around the world. Border control, airlines and other travel organizations have the appropriate tools in place to verify the validity of passports to allow a traveller to cross borders and continue on with their journey. The International Civil Aviation Organization (ICAO) is in control of this framework and their governance structure allows the passport to be a trusted credential across different governments and other sectors.



Here we have listed some areas in an ecosystem's operations that must be aligned in order to embed mutual trust (dependent on the use case and organizations in your ecosystem, others may apply), to enable a more valuable, secure and trusted network for all parties to issue, verify and share trusted identity credentials. Work with your partners to understand and document what else is required.

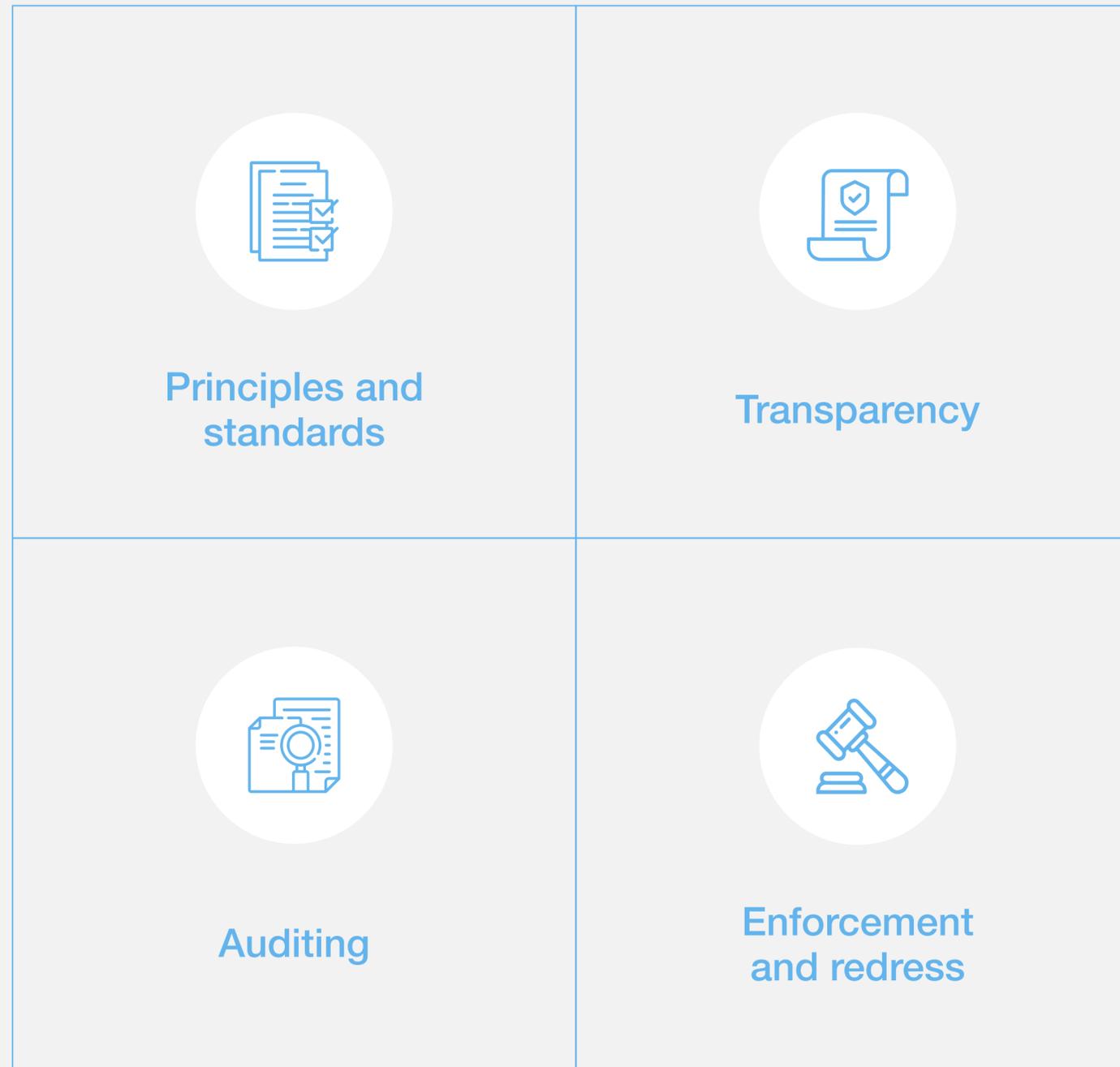
Outcome

This tool should help you understand the key principles that underpin a trusted ecosystem, and what is required to embed mutual trust within one, enabling a more valuable and secure ecosystem in which all parties issue, verify and share trusted credentials.



FIGURE 14

Alignment for a trusted network



Select the areas to discover more

Example: Digital identity for remote learning in Australia



Before COVID-19 changed the way we do so many things, university study was already begin to rely on remote as well as physical interactions, meaning that both students and their teachers needed to be able to prove who they say they are online. The pandemic has rapidly accelerated this need given that proving identity remotely has been difficult for students who have needed to stay at home during various COVID-19 lockdowns. Older, paper-based documents are not easily readable in a digital space, with proof-of-identity paperwork not clear enough when shown manually via a computer screen to be reliable.

Journey to trusted digital identity

Australia's Deakin University and Mastercard have worked together to pilot a scheme that enables students to take exams online. It allows students to create a digital identity in an app over which they maintain full control; this technology enables them, for example, to register an account on the university's digital portal without needing to reveal more than a minimal amount of personal data.

The benefits

- For students: digital identity is personal, portable and convenient, and significantly reduces friction; 72% of students who took part in the pilot found the process to be faster, and almost 80% said they would consider using digital identity for other purposes, too
- For the university: digital identity offered a way to transform certain processes into ones that are paperless yet still trusted; the use of digital identity could be expanded beyond teaching, assessing and issuing study certificates to create digital identity cards and validate digital transcripts⁷⁵



We are living in an era of hyper-connectivity, with digital services transforming shopping, business, politics, healthcare and communication. If we want digital services to blend effortlessly and invisibly with people's daily lives, we need to establish and safeguard trust in digital interactions.

Ajay Bhalla, President of Cyber & Intelligence, Mastercard

Interoperable

Key question



How do you ensure your ecosystem is interoperable with other digital identity ecosystems?

As an individual, the more places in which you can use your digital identity, the more value you gain from using it. Similarly, for organizations, the more they accept digital identities, the more efficiency gains they are likely to benefit from by reducing repetition and errors. For digital identity to become truly useful, being able to use credentials across organizations, sectors and borders is key. To achieve the broad adoption and acceptance of digital identities, there must be common agreements on rules and standards that allow different digital identities to be accepted in different organizations, for example: rules that underpin the ecosystem on what type of information is accepted, levels of assurance of the digital identity issued, the format for this data, the governance that defines the rules, processes, access rights and many other areas for issuing organizations, as well as the verifiers, redress mechanisms, etc. (the ‘trust framework’), plus a legal framework to provide guiderails. Once these structural principles are established, it will be easier for individuals and organizations to fully adopt digital identity as part of everyday life.

BOX 4

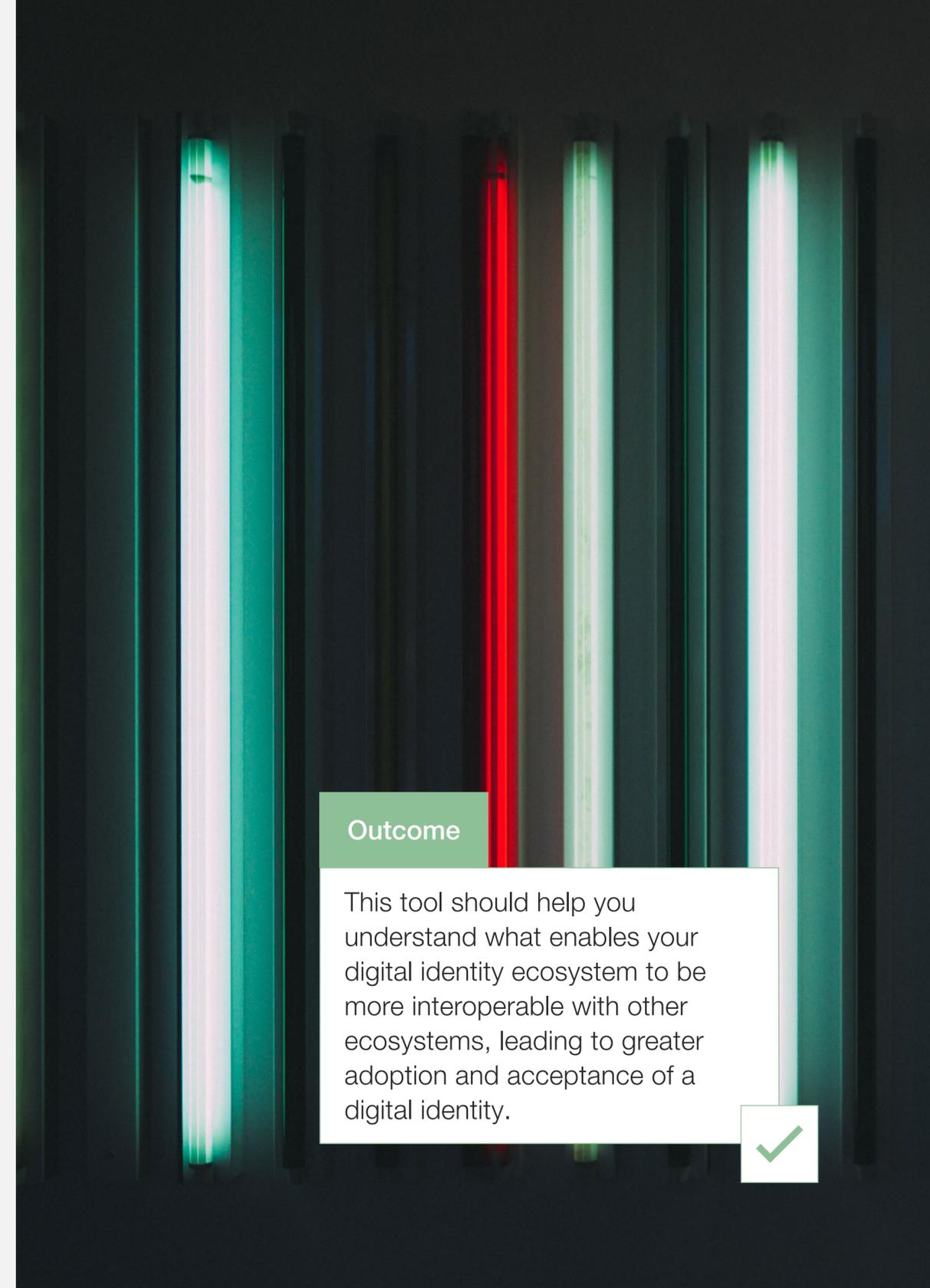
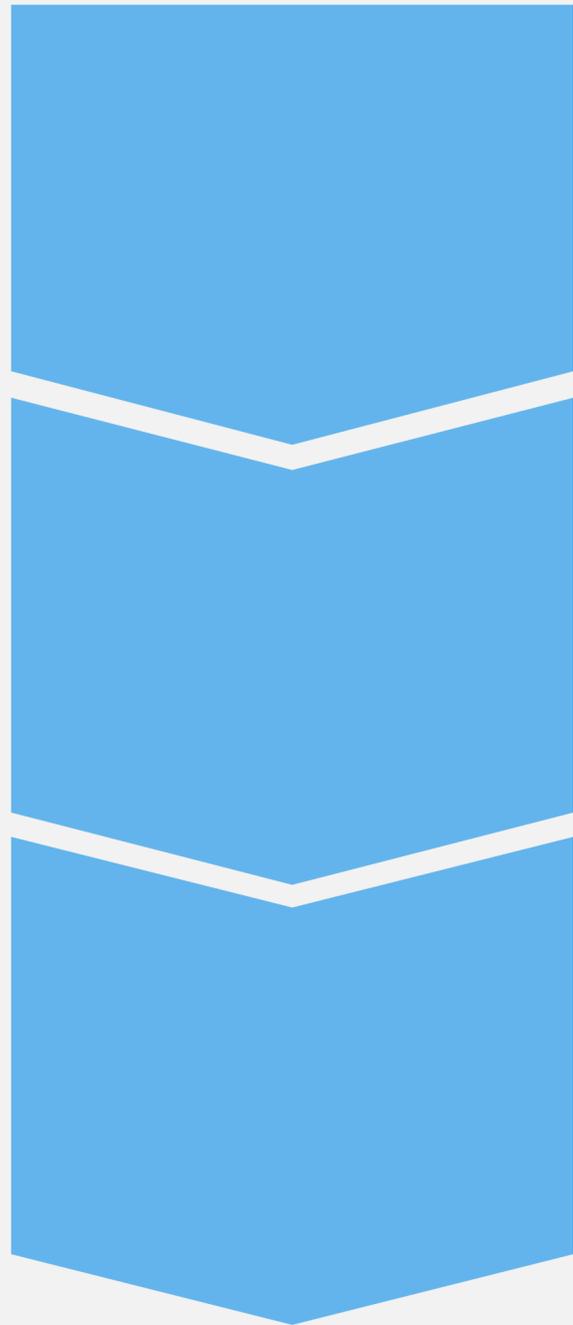
Example: How the passport system became truly interoperable

The national passport is an identity credential that has gained mass interoperability across both borders and sectors. The International Civil Aviation Organization (ICAO) has defined international standards on data to be included in the passport, established a trust framework that underpins the security required for the passport and exchanged data (including a global registry of trusted authorities), and instituted a legal framework that helps secure the entire ecosystem.⁷⁶ These rules enable states to legally accept the passports as an identity credential, and border authorities to quickly verify the data and issuing authorities by searching the common registry. This system of mutual acceptance has made the passport one of the most trustworthy and used identity credentials in the world.



FIGURE 15

Layer



Outcome

This tool should help you understand what enables your digital identity ecosystem to be more interoperable with other ecosystems, leading to greater adoption and acceptance of a digital identity.



Examples: Accepted and adopted – trust frameworks

Examples: Standardized format – identity credentials

Examples: Connecting the data standards

Public-private

Key question



Why is the best approach to digital identity ecosystems based on a public-private collaboration?

Outcome

The tool should help you understand the key strengths for each sector, and the role each of them plays in ensuring an ecosystem that is inclusive of all, embeds trust that enables the sharing of credentials, and which has high-value use cases that will bring greater opportunities for participating organizations.



Single-sector digital identity initiatives (e.g. when banks share KYC data to facilitate the open of a new account) have had limited success due to the competitive nature of a limited ecosystem, a lack of longer-term vision and common goals on adoption. But the way each of us now interact with the digital sphere is fundamentally across sectors, so it's critical that organizations start to look at their users in a more holistic way. For example, an individual may be a customer of a bank, a patient of a healthcare provider, and a jobseeker applying for work with multiple different employers, and all of the interactions this person will have with these three different organizations online will typically require the sharing of government-issued identity credentials (in addition to others). The ability to share digital identity credentials across sectors promises to make processes more efficient and less error prone for organizations, reduce unnecessary repetition for both organizations and individuals, and help create a better user experience. Schemes driven by a public-private ecosystem will be able to combine the strengths of the private sector: innovation, digitization and resources, and those of the public sector: standardization and regulation.

FIGURE 16

Collaboration between the public and private sector: why involve both?

	Public sector	Private sector
Unique strengths	<ul style="list-style-type: none"> Public-sector organizations are often the root source of trust within an ecosystem. They issue multiple key trusted identity documents, including passports, driving licences, national IDs, birth certificates and National Insurance numbers, and possess other data sources that can be used to verify identity They are able to enforce acceptance of identity, enforce formats of digital identity, change legal policy to support the ecosystem, and enable redress when required 	<ul style="list-style-type: none"> Provides a variety of use cases that can be used on a regular basis, even daily Incentivized to build a strong business case to increase value and drive adoption
Role in collaborative digital identity	<ul style="list-style-type: none"> Provides guiderails for a digital identity ecosystem (via a trusted framework, for example) Offers the authority of many trusted identity documents that provide users with identification (e.g. a passport) Governs legislation of digital identity and related policies for the identity verification life cycle (e.g. regulation for privacy and data protection) 	<ul style="list-style-type: none"> Drives user adoption through offering additional products and services that mitigate regular user pain points Has the ability to provide trusted digital identity Can consume or verify digital identity

BOX 5

How the public sector can engage the private sector

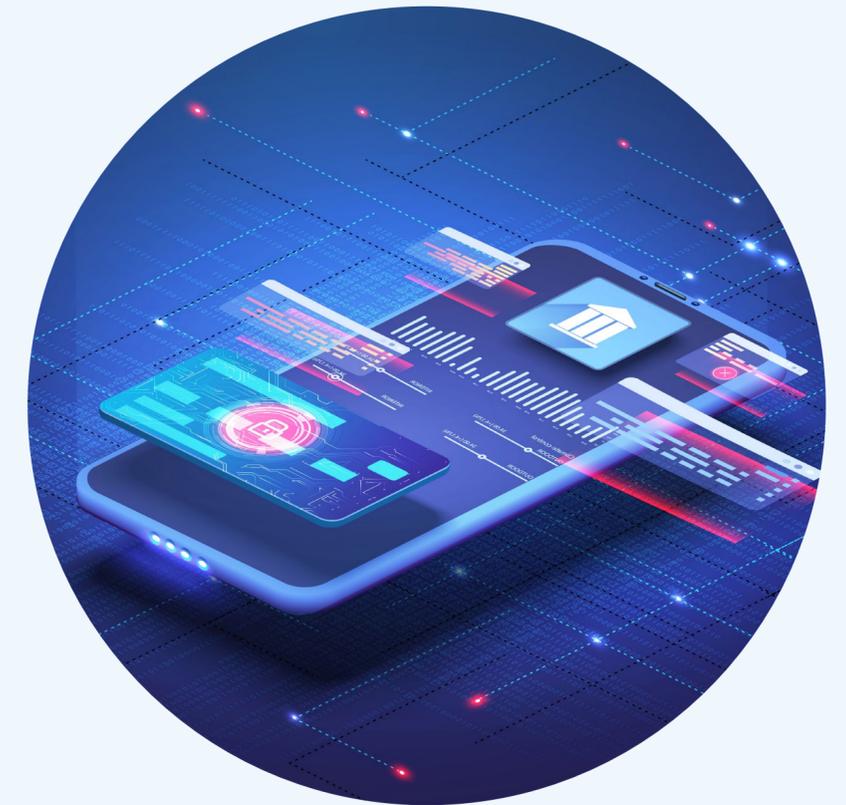
The government of New Zealand is currently developing a legislation-based trust framework that will drive national collaboration on digital identity. In parallel it has helped to establish Digital Identity NZ, a forum to facilitate understanding of the benefits of and needs for digital identity in industries such as energy, construction, agriculture and banking. This initiative will help the government to shape the right regulatory and accreditation framework such that both organizations and individuals can benefit from digital identity.⁸⁹



BOX 6

How government participation is key in privately-led ecosystems

BankID is a banking consortium co-owned by all major banks of Norway, with their networked relationships enabling individuals to seamlessly access banking and other services. One key feature of BankID is the fact it is recognized by the Norwegian government's digital portal – in most countries such recognition is conferred by an accreditation process. BankID is now used by 99% of Norwegian citizens, and on average 160 times per year, securing huge efficiency gains.^{90,91} Similarly, in India, the government-led Aadhaar scheme is now used by 88% of the population.⁹²



Sustainable

Key question

How do you embed the right financial and governance models into the ecosystem to ensure sustainability?



A sustainable business model enables continuity of the digital identity ecosystem over the long term, which in turn helps engender trust and increases adoption. Individuals and organizations are normally fairly quick to recognize when an ecosystem is unsustainable and as a result will be unlikely to accept it. To underpin ecosystem resilience, incentives must be established and clearly proven for all participants, as well as be allowed to evolve over time (which they are likely to need to do). Once an ecosystem is formed, it needs a viable funding model that has the potential to over time become self-sustaining. As the ecosystem develops, appropriate operational governance needs to be in place to ensure the network can maintain itself, as well as keep up to date with changes and advancements across markets, regulations, skills, processes and technology. The next section outlines each of the key areas that need proper consideration to help ensure that a new digital identity ecosystem can remain viable over the longer term.



Tool 1: Funding a digital identity ecosystem

What public-private funding approaches can help bring benefits?

Example: Thailand's new national digital identity scheme was funded by the Central Bank of Thailand; the ecosystem is driven by a joint venture with key financial sector players called National Digital ID (NDID).⁹³



Tool 2: Monetizing a digital identity ecosystem

What are the options for and advantages of user-centred sustainable financing?

Example: BankID, Norway's digital identity scheme is 100% free to user for individuals, but its credentials are offered commercially to identity service providers through a network of resellers.



Tool 3: Governing a digital identity ecosystem

What do you need to consider in formulating and maintaining a set of rules to adhere to?

Example: The Known Traveller Digital Identity (KTDI.org) is governed by a consortium of governments, airports and airlines via an agreed set of rules and standards; technical support is offered through specialized providers for parts of the solution, e.g. on biometrics and the authentication platform.

Key question



What are the different funding models for ecosystems?

Figure 17 describes some different funding models for digital identity ecosystems. Each ecosystem will require a particular approach based on context; some ecosystems will not require funding, whereas some may require all participating organizations to invest in development and operation. You should work with the partners in your ecosystem to understand how best to build and obtain the right level of investment using the most appropriate model.



Initial certification and funding are the most difficult areas in building an ecosystem – expertise wasn't widespread in the market, and at the beginning, investors were not sure about future success. Itsme adopts a shared financing model backed by banks and telecommunication groups.

Remy Knecht, Chief Operating Officer, itsme

FIGURE 17

	Government investment upfront	Public-private investment	Membership model with different membership types	Specialism- or proportion-based contribution
Description	<ul style="list-style-type: none"> Government provides the upfront investment and sets the direction, ensuring the digital identity ecosystem is launched 	<ul style="list-style-type: none"> Each member contributes an equal amount of money to the ecosystem, with distribution of funds based on the requirements of each working group 	<ul style="list-style-type: none"> Each organization's contribution to the ecosystem corresponds to the type of membership that it has chosen 	<ul style="list-style-type: none"> The contribution of the members to the ecosystem scales in proportion to a predefined driver (e.g. quantifiable revenue return or benefits for each organization)
Advantages	<ul style="list-style-type: none"> Can set the policy and direction for the public-private ecosystem Ability to provide trust anchors or certify the infrastructure 	<ul style="list-style-type: none"> Ease of implementation Investment risk is shared between all members equally Ability to offer multiple product or service offerings 	<ul style="list-style-type: none"> Enables tailoring of membership according to the type or role of each participating organization 	<ul style="list-style-type: none"> Enables equity of investment according to potential gains for each organization
Disadvantages	<ul style="list-style-type: none"> Government carries the initial risk until such a point that private-sector partners are onboarded 	<ul style="list-style-type: none"> Some members may stand to gain relatively more than others, meaning that some end up investing in the disproportionate gains of others 	<ul style="list-style-type: none"> Additional administrative burden, including having to define different membership types and commitments 	<ul style="list-style-type: none"> Extremely difficult to quantify and reach agreement on revenue return or benefits for each organization, and to tie this to a funding value

Outcome

This tool should help you understand some different funding models and how to decide which might be appropriate for you, based on your current position.



Key question



What are the different monetization options that will ensure sustainability in your identity ecosystem?

To enable a trusted service in commerce, trade, employment or other area, a digital identity ecosystem must be able to sustain itself. The conventional financial model avoids charging end users. Instead the verifiers which embed digital identity, such as e-commerce providers and banks bear the costs. A number of other monetization options now exist, however – use the information in Figure 18 to help you assess their viability against your use case, to identify which might be the most appropriate option for ensuring the sustainability of your particular ecosystem.

Outcome

This tool should help make clear the pros and cons of different monetization options; use it to assess their viability for your use case and jurisdiction, and to understand which is the most appropriate option to ensure sustainability.



FIGURE 18

	 Purchasing fee	 Subscription	 Pays per use	 No fee
Description	The participant pays a one-time purchasing fee for the digital identity, similar to current systems that rely on credentials in the form of passports or driving licences	The participant pays a yearly subscription fee in order to be able to make use of the digital identity offering	The participant or receiving party pays a small fee each time a data transaction is made via the digital identity offering	The ecosystem members decide to provide the digital identity offering for zero cost because it gains them other benefits (e.g. cost savings)
Advantages	Simple, one-off, upfront payment and thus no requirement for multiple payments; end user familiarity with an approach that aligns with the status quo	Subscription-based models offer greater granularity, reducing the cost impact to the individual; also provides the ecosystem with greater financial certainty as a result of repeat revenue	The pay-per-use model offers a lower barrier to entry; individuals will be encouraged to trial the offering in order to develop an understanding of its value	Lowest barrier to entry; zero cost will encourage uptake and unlock value in the digital economy; may create ‘stickier’ customers
Disadvantages	One-time payment may be considered a barrier to entry, with users initially unaware of the benefits that can be realized	Additional management requirement for participants to maintain subscription accounts, which may discourage adoption. Multiple payments result in additional transaction throughput of lower value payments leading to additional payment processing costs	Multiple payments result in additional transaction throughput of lower value payments, leading to additional payment processing costs	Zero revenue means that all ongoing development and operational activities (whether or not they are provided by a third-party supplier) will need to be funded by the participants in the ecosystem

Key question



Which governance functions are required in a multi-party digital identity ecosystem?

The values, rules and operational protocols agreed between partners – allowing trusted interactions between customers, citizens, partners from banking, e-commerce and trade – must be constantly maintained. Instituting good governance allows ecosystems to change and adapt when required, enabling them to constantly improve and transform user experience, as well as keep up to date with technological and security advancements.

Outcome

This tool should help you understand the business and operational governance functions required for an identity ecosystem, ensuring that the network can be managed with multi-party stakeholders, and that it can keep up to date with advancements in both technology and security.



FIGURE 19

High-level functions	Governance type	Description	Components	Governance type:
1. Governance		High-level governance to manage the key decisions within the ecosystem	Purpose, direction and membership, as well as managing working groups and committees, etc.	 <p>Business governance provides a foundation for mutual trust between parties with a shared vision for unlocking the value of an ecosystem</p>  <p>Operational governance provides ecosystem participants with the ‘rules of the road’ to govern the technological and operational aspects of the ecosystem</p>
2. Participant governance		Managing the ecosystem organizations to ensure compliance and participation	Compliance, onboarding, operations enablement, offboarding, etc.	
3. Data governance		Ensuring compliance with relevant legislation and appropriate use of data	Legal and data protection, data standards, data confidentiality, etc.	
4. Operations (technological and business)		Oversight of the operations that underpin the ecosystem to ensure functionality	Reporting, support, etc.	
5. Technological governance		Management of technology providers for the ecosystem	Change management, Cloud and hosting, platform, etc.	
6. Technology management		Ensuring technology can develop and update in line with emerging standards and technology advancements	Product development, release management, security, architecture, etc.	
7. Growth and innovation		Developing new features, use cases and new technology to enable ecosystem to keep pace with change	Go-to-market, new feature identification, etc.	

6

Assessing the value and mitigating risk



Measure and refine

Key question



How do you continuously measure and improve your ecosystem?

There are a number of ways in which the value digital identity brings to an organization can be measured, including financial gain and a reduction in costs, risk or friction. Given that digital identity benefits are likely to be experienced by the wider ecosystem once adopted, it is often difficult to measure direct benefits, but measures such as monitoring digital identity usage and quantifying efficiency gains or market potential for connected services could help to understand particular areas for improvement, and to support adoption, growth and customer satisfaction. A few examples of measurement methods are detailed here:

Metrics	Ways to measure	Example demonstrating how digital identity increases value
Market expansion	Number of users, number of transactions	itsme in Belgium has constantly increased its number of users – between 2019 and 2020 it grew by 20% ⁹⁴
Customer engagement	Analysis: what features are used	Introducing India's national digital identity-supported KYC drove a surge in banking onboarding of 190% between 2017 and 2018 ⁹⁵
Reduced cost	Cost per customer, operation cost or number of users	The costs of digitally asserting the authenticity of customers (KYC) were reduced by 86% via through a nationally recognized digital identity approach in India ⁹⁶
New business models	Number of new connected services	If the user consents, there is the potential for new connected digital services such as banking loans and health, e.g. as of 2019, in the US 66% of patients are willing to use virtual services for healthcare, and in July 2020, 67% more users had a digital bank account in comparison with the same figure for January 2020 (6% of population) ^{97, 98}
National economic gains	Indirect benefit (e.g. new business models)	At national level full digital identity coverage could unlock economic value equivalent to 3–13% of GDP ⁹⁹
Efficiency	Time it takes to complete a process	In Estonia, time to register a new company using digital identity was reduced from five days to 18 minutes by replacing paper-based processes ¹⁰⁰
Reduced friction in the user experience	Reports on social media, awards, recognition	Globally, 43% of banking onboarding is abandoned during complicated qualification processes, and 22% of users do not complete their purchase when they are required to create a new user account – digital identity can help solve this ¹⁰¹

Outcome

This tool should help you understand how to measure the success of your digital identity ecosystem, as well as assess the value it creates, giving you a quantifiable metric that allows you to understand its success and to explore ways to make improvements.



Assessing and mitigating risk

Key question



What are the key risks you might encounter with digital identity ecosystems, and what can you do to mitigate them?

Before progressing with the development of a digital identity ecosystem, the following risks should be understood so they can be better mitigated against:

Outcome

This tool should help you understand the main risks digital identity ecosystems are subject to, and the best ways to mitigate them



Membership structure creates a siloed system

- **Public-sector-only or private-sector-only ecosystems:** both limit the number of uses for digital identity services
- **Mitigate this risk:** join or create a collaborative digital identity ecosystem that includes parties from both the public and private sectors. Involvement of both is key: for the public sector it may be hard to expand new use cases or offer relevant interactions for users if the private sector isn't involved; in turn, public sector input is key for the private sector, especially in navigating regulations as they continue to evolve in light of new use cases, and in helping enhance trust in the ecosystem



Culture is slow to embrace innovation and change

- **Holding onto 'ownership' of users:** if the organizations involved are unwilling to change their mindset, seeing that they 'own' their users' data instead of allowing them to have more control over it, one may well find that operating the ecosystem in a collaborative spirit becomes more difficult
- **Mitigate this risk:** collectively, participants need to shift their mindset from 'owning' a user's identity towards serving them as an individual. Use cases need to be identified that demonstrate specific value in being more user-centred, and tests conducted to prove the value of this kind of activity



Ecosystem has both low relevance and value

- **Technology-first approach:** often digital identity solutions are built before proper consideration is given to the needs of both users and participants within the ecosystem
- **Mitigate this risk:** avoid focusing too much on the technology; instead, focus on the potential of particular use cases and the value that can be created (for help with this see Section 2.3, 'Prioritizing use cases' above (p.18))

7

Different models for an ecosystem: four case studies



Putting it all together



Thailand: Government- led national digital identity ecosystem

Context

In 2019, recognizing a need for a national-scale approach to digital identity in Thailand, the Bank of Thailand initiated pilot schemes with a range of different participants. The live system that emerged from this testing period is managed through a new, legally established entity called National Digital ID (NDID). Although the ecosystem was first established in the form of only a digital identity committee, since then several different players – initially banks – have become participants, offering customers a better experience and trusted, reliable digital interactions.

Use cases

NDID has supported the development of a national ecosystem and of use cases that are most beneficial to stakeholders.

2019-2020

Opening a bank account

Digital banking and onboarding are a key use case in Thailand, and made a natural focus for banks, who were the ecosystem's first adopters.

2020

Account for opening for financial services (not banking)

Other use cases were open securities trading accounts, mutual fund accounts, life insurance policies and other types of account, with users simply confirming their identity via an existing account for which their identification had already been verified.

2021

Tax filing for the Revenue Department

The Thai government itself forms part of the ecosystem: its Revenue Department is a key entity in helping drive digital transformation.

Roles in the ecosystem

Issuers and verifiers

- Banks
- Non-banks: securities, asset management, digital lending, insurance
- Government (e.g. the Revenue Department)

Other roles

- Orchestrator: National Digital ID (NDID)
- Regulator: Electronic Transactions Development Agency (ETDA)
- Standards Body: Bank of Thailand

Executive journey



Digital identity is getting more attention as executives have factored it in their IT and business plan for doing face-to-face and non-face-to-face transactions, such as digital onboarding for account opening or lending to businesses. Major banks have agreed to be NDID's proxy, providing one-stop solutions for their related companies and business partners.

Boonsun Prasitsumrit, Chief Executive Officer, National Digital ID

Interoperability

Dimensions

Data standards

Domestic interoperability

The national digital identity of Thailand focused on decentralized protocols such as blockchain to ensure user-control on data and decentralized ownership; biometric protocols can be used to ensure users can conveniently log in to their accounts to support e-Know Your Customer.

Policy and regulation

Thailand's national digital identity is regulated through the Digital ID Act, a set of digital identity guidelines issued by the ETDA; in Q2 of 2022, the ETDA will also regulate digital identity platforms and issuers of identity.

Trust and governance

NDID governs the standards and rules adhered to by the different organizations in the ecosystem.

Expansion of the ecosystem

- Q1 2020: 8 banks implemented the Open Bank Account 2018
- Q2 2020: 22 non-banks joined as verifier (securities, asset management, digital lending, insurance)
- Goal for 2021: 100 verifiers

Success measures

- 2020: 2 million transactions – usage accelerated by the need for trusted remote interactions as a result of the COVID-19 pandemic
- 2021: 50% increase in number of transactions
- Number of adopters: 8 identity providers and 40 verifiers
- User experience: processes can become 100% non-facing
- Organizational benefits: digital onboarding is key to the expansion of services
- User adoption and perception: digital identity is still new – NDID is focusing on expanding the types of supported use cases and driving public engagement

itsme, Belgium: Private sector- led national digital identity ecosystem

Context

Belgium has a national digital identity card called eID, and a private sector-led, government-recognized scheme called itsme. Created by Belgium Mobile ID, the itsme digital identity scheme is an open ecosystem built in 2017 that allows all organizations who wish to do so to become members (currently they number around 4,000). itsme offers a broad range of digital identity solutions, from digital signatures to shared identification and NFC-based verification that enable cross-sector digital services.

Use cases

Roles in the ecosystem

Issuers and verifiers

- Major Belgian banks leveraging strong existing KYC data in Belgium
- NFC-readable ICAO passports and eID cards: needed to scale fast internationally

Verifiers

- First movers: government and banks (generated trust, and initial high volumes needed for the start-up to survive)
- Second wave: 2nd tier banks (online banks), insurance companies and utility companies
- Third wave: healthcare (boosted by demand created by COVID-19), online businesses
- Fourth wave: Internet of Things (Laggers = retail sectors)

Other roles

- Government: distributes the certification or trust mark for service providers
- Banks: generated trust (specific to Belgium) and high initial volumes
- Value-added resellers: generate scale
- Financial regulators/EU Commission: close cooperation to align with regulation and innovation (for mutual benefit)

Executive journey



Initially we were “selling” the identity services (login, share id, confirm, sign), but we quickly realized that the market lacked inspiration to understand how a digital identity could be beneficial. We started “selling” key use cases per industry – e.g. a call centre case was accelerated from six days to three minutes: traditionally, people calling to switch mobile operator (number portability) get a letter of acceptance sent by the call centre, they need to fill it in and return it, then the call centre scans it, initiates the transfer of the number (a process that takes six days). Using itsme, with the mobile number on the screen the call centre can now send an approval request for the number transfer for which there’s a legal audit trail equal to a Level of Assurance. The transfer can now be done in three minutes.

Remy Knecht, Chief Operating Officer, itsme

Interoperability

Several decisions were taken to support interoperability both at national and international level:

Dimensions	Domestic interoperability e.g. the connection between identity providers and the public sector	International interoperability	Why were these decisions taken?
Data standards	Data exchange: via the Federal Authentication Service (a hub to which all of the Belgian government’s 3,500 applications are linked); both the national eID and itsme use the same national identifier (the National Register Number).	Adoption of sector-level standards: – ICAO-compliant NFC readable passports – EU NFC-readable eID cards – Upcoming data sets for CDD, healthcare	Common data set known and accepted across borders.
Identity standards	Open proven standards (OpenID Connect, OASIS DSS, CSC, iShare).		Accepted and implemented by many big platforms (e.g. Adobe, Microsoft Active Directory B2C, Firewalls).
Policy and regulation	Belgium issued a Royal Decree based on the European Union’s eIDAS to regulate Digital ID.	eIDAS EU notification.	Cross border interoperability and international expansion.
Trust and governance	<ul style="list-style-type: none"> – FAS trust framework for government applications defined by the Belgian G-Cloud Board – Identity scheme defined by itsme has transparent requirements to generate industry trust – AML/PSD2 as aligned with the National Bank 	eIDAS, ETSI, CEN, NIS, ISO27000, AML/CTF, FATF, PSD2, EBA Guidelines, EU CCOC, Schrems II.	Cross-border and industry acceptance.

Velocity Network: Global digital identity ecosystem for career credentials



The right to work, to free choice of employment, is a basic human right. We envision a world in which every person has access to personalized career and development opportunities at the time it matters. Breadth of trusted individual career data and the free flow of it are key to personalized guidance and better opportunities.

Dror Gurevich, Chief Executive Officer and Founder, Velocity Network Foundation

Context

Efficient development and deployment of human capital require the free flow of trusted data relating to people's skills, education and credentials. It has been widely recognized that individuals' resumes, LinkedIn profiles and any other self-reported career records cannot be seen as trustworthy sources of information, yet employers still rely on them as sources of information about people's careers. Applicant and employee career credentials are currently verified through 100-year-old, manual, error-prone processes that are weeks long and expensive.

Solution: verifiable career and education credentials, and a user-controlled approach to issue, share and verify credentials and enable a trustworthy 'Internet of Careers'.

Impact:

- 1 billion people move jobs every year; verifying people are who they say they are adds unimaginable cost and friction to the labour market
- In addition, most employers identify lack of current career credentials data on their existing employees as a top-three barrier to the efficient use of talent

Use cases

Self-sovereign career credentials (education, employment history, licences, certification, training, skills, etc.) that can be applied in the following areas:

- Hiring
- Career mobility
- Education
- Learning
- Job matching
- Compliance management
- Payroll
- Right to work
- Credit scoring
- Insurance

Roles in the ecosystem

Issuers and verifiers

- Employers
- Training providers
- Professional associations
- Licensors
- Education providers
- Background screening providers
- Assessment vendors
- KYC providers
- Contingent workforce providers

Verifiers

- Staffing functions in organizations

Other roles

- The Velocity Network is managed by the Velocity Network Foundation (a cooperative, non-profit organization that provides a common rulebook and framework for interoperability, and which promotes global adoption and support)
- The Velocity Network is composed of nodes managed by different organizations (issuers or verifiers) and credential-agent operators; credentials are managed in wallets provided by wallet providers

Executive journey



The democratic, non-profit nature of the governance, and the open-source framework will make Velocity Network a true public utility layer. This is why we are calling it the Internet of Careers. It sets Velocity apart from other frameworks in this space and is what enabled the fantastic tractions we see, as the biggest vendors in the education and employment markets join the network, driving the supply and demand flywheel.

Dror Gurevich, Chief Executive Officer and Founder, Velocity Network Foundation

Interoperability

Dimensions

Domestic interoperability

Data standards

For career credentials, the Velocity Network Foundation established a committee responsible for data interoperability standards. Membership is open to all those interested in Velocity Network Foundation stakeholders, especially those with expertise in product management and development, particularly related to self-sovereign identity, education, human capital management, privacy security and blockchains.

The committee is responsible for:

- Researching, formulating and recommending technical and data syntax and structure standards affecting the technical design of the Velocity Network
- Assuring interoperability between issuers, verifiers and holders participating in the Velocity Network, or any other verifiable credentials networks

Identity standards

In governing the ecosystem, the Velocity Network Foundation is committed to enabling technical interoperability within the network and across different blockchain networks and different verifiable data registries, via rigorous adherence to industry standards.

Policy and regulation

The Velocity Network is a permissioned network: issuers, verifiers, node operators and credential agent operators are vetted by the Velocity Network Foundation's registrar.

The Velocity Network Foundation has established a committee responsible for compliance to global, cross-jurisdictional regulations. Membership is open to all interested Velocity Network Foundation stakeholders, especially those with expertise in compliance development, particularly related to education, employment, privacy, FCRA, securities and cryptocurrency.

Trust and governance

The Velocity Network Foundation is an open, non-profit organization that provides a rulebook and framework to enable operational and legal clarity, governing the use of the Velocity Network by all involved parties.

SoyYo, Colombia: Private sector- led national digital identity ecosystem

Context

SoyYo is a company founded in 2020 by Colombia's three major banks, to provide digital identity services that will enable the economic growth of the country by offering confidence, privacy and security in transactions. This ecosystem will manage the interactions between four kinds of participants: (i) users, who are the owners of their identity and information, and who will create a digital identity on SoyYo's platform; (ii) the verifiers, which are companies that interact with users and need to trust the identity and information of the user in relation to their transactions; (iii) issuers, which are companies that give validated information that is required in the transactions between users and entities; and (iv) trust providers, which are companies that have a strong relationship with users, that have made a strong KYC process, and which help bring new users to the ecosystem.

Use cases

Q1 2021: P2P verification

A need was identified to validate the identity of a person in peer-to-peer (P2P) interactions where there are impersonation fraud risks; for example, in P2P fund transfers, or when a public services company is sending a technician into someone's home.

Q2 2021: Onboarding

Most of the companies SoyYo approached have shown a need to improve their onboarding process by incorporating mechanisms that assure that their potential client is who they say they are, and that offer validated online information about that client.

July 2021: E-signature

- This use case can complement other use cases, such as onboarding
- Creates a strong and differentiating product by incorporating digital identity verification in an e-signature process

Roles in the ecosystem

Verifiers

Three major banks act as trust providers and verifiers:

- Bancolombia
- Banco de Bogotá
- Davivienda

The role of trust provider is also open to other companies that have a robust KYC process.

Issuers

- Registraduría Civil is the government entity that issues a digital identity to all citizens; SoyYo validates the identity information with them
- Bogotá's Commerce Chamber gives SoyYo information about companies that is useful when onboarding companies
- KYC and Anti-Money Laundering (AML) authorities offer the financial and AML information that is required in some transactions
- RUNT provide information about driving licences and the status of cars

Other roles

- Orchestrator: SoyYo
- Regulators: Superfinanciera and URF (in charge of the supervision and control of the financial system)

Executive journey



In our commercial approaches we have seen that the companies perceive great value in having an onboarding process with less friction and stronger impersonation fraud control. It is also valuable to finish a transaction with an e-signature process that avoids non-repudiation.

Santiago Aldana Sanin, Chief Executive Officer, SoyYo

Dimensions	Domestic interoperability e.g. the connection between identity providers and the public sector	International interoperability	Why were these decisions taken?
Data standards	Data exchange: obtaining and exchanging identity information from Registraduría Nacional, which is the government identity issuer.	N/A	The information obtained is compared with the OCR end BCR of the physical document, in order to ensure it belongs to the right person.
Identity standards	Solution being integrated with OpenID and SAML in order to enable interoperability with external directory services.	N/A	Due to the COVID-19 pandemic, more people are working from home and companies want the administrators of their core systems to be authenticated by SoyYo in order to ensure their employees are the only people who can gain access.
Policy and regulation	Strong privacy and security policies (by design).	N/A	Security and privacy are key to enhancing trust for all participants in the transactions.
Trust and governance	Key to link to trust anchors <ul style="list-style-type: none"> – Key linkage with trust providers (three banks and any additional approved organization with strong KYC data) – Registraduría offers trust in the national identity that identifies citizens – Access to a database that has biometric information of governmental processes 	N/A	Link to trust anchors in the state.

Conclusion



Around the world, people's everyday lives are being transformed by new technology, as companies and organizations in every sector look to reap the benefits of embracing the digital economy. As a result, the ways in which individuals identify and verify themselves must also change, moving away from processes that are manual and paper based – something that has been accelerated by the COVID-19 pandemic. As a fundamental and shared public good, digital identity is something that organizations must get right.

This moment presents a great opportunity for executives to embrace digital identity, and to understand how their organization can capture new value by establishing or participating in a digital identity ecosystem. These collaborative networks offer a means of creating new connected services, business models and marketplaces – and early movers will benefit most from trusted customer interactions, which will operate across a much broader ecosystem than their competition. To succeed, organizations need to understand and adopt a user-centred model and use it to transform how they operate and interact in existing and new ecosystems.

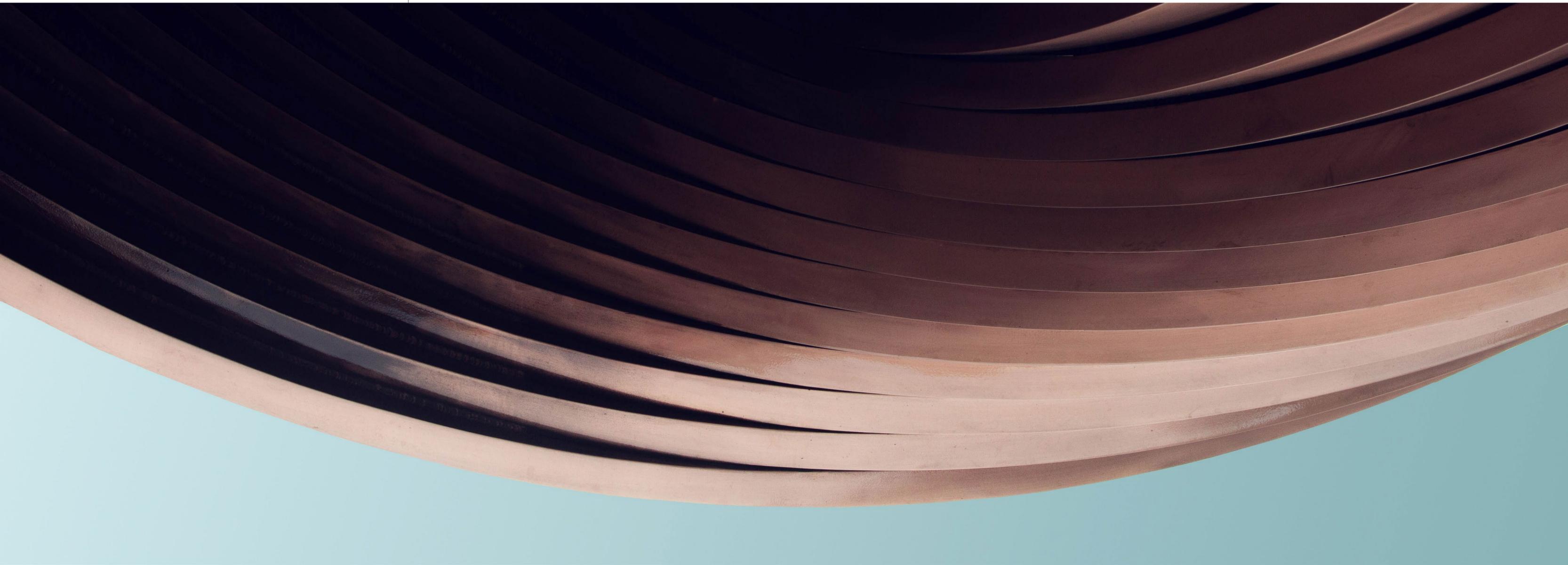


What's next?

After using this guide to maximize success, executives must continue to align with partners and:

- Understand that this is a transformation journey: digital identity will impact many parts of your organization and daily interactions, but change also brings opportunity
- Develop new business services reliant on enabling a user to access many different services seamlessly, with trust embedded throughout
- Keep up with emerging regulations, coalitions, standards – the pace of change and growth is rapid, especially with an international and regional focus on digital identity (e.g. the European Union's regulation for a digital identity wallet and vaccine passports)
- Ensure a change mindset pivots your organization away from the concept of owning the user and their data to interacting with and serving them
- Have an inclusive mindset, promoting the participation of all customer groups in thinking and designing digital identity-enabled services

Acknowledgements



The World Economic Forum would like to thank Accenture for its valuable support in the creation of this guide, which draws on the expertise and experiences of a range of organizations currently cooperating on progressing the digital identity agenda.

Contributors

Absa Group Limited
Accenture
ATB Financial
Banco Santander
Bank of Thailand
Belgian Mobile ID SA (itsme)
Cambia Health Solutions
CARIN Alliance
Center for Financial Regulation and Inclusion (CENFRI)
Commercial International Bank (Egypt)
Demos
Digital Identity Extraordinary
Emirates NBD
European Commission
Government of Germany
Government of India
Government of New Zealand
Government of the United Kingdom
HD Catalyst B.V. (driving IKKE Netherlands)
Humana
Irish Life
JP Morgan
Kantara Initiative
Kiva.org

KLM Royal Dutch Airlines
Leavitt Partners
LuxTrust S.A.
Mastercard
MTN Group Ltd
NDID
NEC
Nixu Cybersecurity (driving SisulD)
Omidyar Network
ONEZERO1 (driving Emerald)
Open Digital Trust Initiative
OpenID Foundation
Robert Bosch GmbH
SAP
Sedicii Innovations Limited
Smart Africa Secretariat
SoyYo
Standard Bank
SWIFT
SwissSign AG
TechUK
The Investing and Savings Alliance
The Open Identity Exchange
Trulioo
UBS
Velocity Career Labs
VerifyMe
Verimi GmbH
Verum Capital
VIDA (Verified Identity for All)
Vipps AS
Women In Identity Foundation
Yoti
Zaka.io
Zurich Insurance Company

Authors

For the World Economic Forum

Derek O'Halloran, Head, Platform on Digital Economy and New Value Creation

Manju George, Head Strategy, Platform on Digital Economy and New Value Creation

Cristian I. Duda, Lead, Digital Identity, Platform on Digital Economy and New Value Creation

For Accenture

Christine Leong, Managing Director, Global Decentralized Identity and Biometrics Lead

Jessica Johnson, Senior Manager, Decentralized Identity, Multiparty Systems

Jack Keeling, Consultant, Decentralized Identity, Multiparty Systems

Design and editorial

Studio Miko

Laurence Denmark, Creative Director

Alistair Millen, Creative Director

Phoebe Barker, Designer

Dan Smith, Digital Designer

Ally Ireson, Editor

Joanna Peios, Editor and Proofer

Endnotes

- <https://www.raconteur.net/digital/what-does-the-future-of-digital-identity-look-like/>
- https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility_en
- <https://www.forbes.com/sites/carolinecastrillon/2021/12/27/this-is-the-future-of-remote-work-in-2021/>
- <https://ec.europa.eu/commission/presscorner/>
- <https://www.juniperresearch.com/press/digital-identity-app-in-use-to-exceed-2025>
- <https://www.globalbankingandfinance.com/digital-future-the-evolution-of-workforce-and-technology-trends-that-are-now-shaping-the-new-world/>
- <https://learn.g2.com/digital-identity>
- <https://www.gov.uk/government/publications/attributes-in-the-uk-digital-identity-and-attributes-trust-framework/understanding-attributes>
- <https://opencreds.org/specs/source/identity-credentials/>
- http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf
- http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf
- http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf
- <https://www.mckinsey.com/industries/public-and-social-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id>
- <https://www.marketsandmarkets.com/Market-Reports/digital-identity-solutions-market-247527694.html>
- https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663
- <https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/digital-id-the-opportunities-and-the-risks>
- <https://e-estonia.com/wp-content/uploads/eestonia-guide-2018.pdf>
- <https://apnews.com/article/air-travel-travel-changing-economy-airlines-business73b55c3da0a07012f20bd6913743e806>
- <https://www.statista.com/topics/6178/coronavirus-impact-on-the-aviation-industry-worldwide/>
- <https://www.accenture.com/gb-en/insights/strategy/cornerstone-future-growth-ecosystems>
- http://www3.weforum.org/docs/WEF_Digital_Identity_Strategic_Imperative.pdf
- <https://tech.co/news/average-person-100-passwords>
- <https://www.biometricupdate.com/202010/digital-identity-apps-to-outnumber-cards-by-2023-juniper-research>
- <https://www.forbes.com/sites/blakemorgan/2019/12/16/100-stats-on-digital-transformation-and-customer-experience>
- <https://www.gartner.com/en/documents/3697317/>
- <https://e-estonia.com/solutions/business-and-finance/e-business-register/>
- <https://spectrum.ieee.org/computing/software/why-software-fails>
- <https://www.signicat.com/blog/the-battle-to-onboard-2020-the-impact-of-covid-19-and-beyond>
- <https://www.mckinsey.com/industries/public-and-social-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id>
- <https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/digital-id-the-opportunities-and-the-risks>
- <https://www.oliverwyman.com/our-expertise/insights/2020/jul/digital-identity.html>
- <https://www.cnbc.com/2021/03/23/consumers-lost-56-billion-dollars-to-identity-fraud-last-year.html>
- <https://www.bbtimes.com/technology/digital-identity-is-the-next-big-thing-to-reduce-cost-to-acquire-a-customer-cac>
- <https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/digital-id-the-opportunities-and-the-risks>
- <https://www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx>
- <https://e-estonia.com/>
- <https://e-estonia.com/solutions/healthcare/e-prescription>
- <https://www.swissign-group.com/en/konsortium.html>
- <https://www.swissign-group.com/en/ueberswissign/meilensteine.html>
- <https://www.find-tender.service.gov.uk/Notice/009822-2021>
- <https://beta.staffpassports.nhs.uk/>
- <https://www.iata.org/en/programs/passenger/travel-pass/>
- <https://www.forbes.com/sites/alisondurkee/2020/08/25/un-report-tourism-industry-covid-19-faces-1-trillion-loss-100-million-jobs-at-risk/>
- <https://sisuid.com/rulebook/>
- <https://ktdi.org/>
- <https://www.goodhealthpass.org>
- <https://www.singpass.gov.sg/singpass/common/article?newsIndex=7>
- https://csrc.nist.gov/glossary/term/relying_party
- http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf
- <https://serviceinnovationlab.github.io/digital-identity-glossary/>
- <https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf>
- <https://www.iso.org/about-us.html>
- <https://csrc.nist.gov/glossary/term/audit>
- <https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation>
- <https://dictionary.cambridge.org/dictionary/english/regulator>
- <https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/digital-identity-trust-framework/>
- <https://www.gov.uk/government/consultations/digital-identity-and-attributes-consultation/digital-identity-and-attributes-consultation>
- https://csrc.nist.gov/glossary/term/identity_provider
- <https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework>
- <https://www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework>
- <https://www.congress.gov/bill/116th-congress/house-bill/8215/text?r=20&s=1>
- <https://verimi.de/en/about-verimi/>
- <https://www.velocitynetwork.foundation/>
- https://www.onlinezugangsgesetz.de/SharedDocs/downloads/Webs/OZG/EN/9-point-plan.pdf?__blob=publicationFile&v=1
- <https://www.theguardian.com/world/2021/may/22/new-id-law-aims-to-help-reduce-digital-shyness-in-germany>
- <https://verimi.de/en/for-partners>
- <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>
- https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en
- <https://www.mastercard.com/news/perspectives/2021/digital-id-in-a-virtual-world-how-to-prove-that-you-are-really-you/>
- <https://www.itsme.be/>
- http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf
- https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663
- <https://www.swissid.ch/en/app.html>
- <https://www.ledgerinsights.com/oracle-randstad-blockchain-career-credentials-velocity-network/>
- <https://www.mastercard.com/news/perspectives/2021/digital-id-in-a-virtual-world-how-to-prove-that-you-are-really-you/>
- <https://www.icao.int/about-icao/Pages/default.aspx>
- <https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework>
- <https://diacc.ca/trust-framework/>
- <https://www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework>
- <https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/digital-identity-trust-framework/>
- <https://smartafrica.org/knowledge/digital-id/>
- https://www.carinalliance.com/wp-content/uploads/2020/12/LPCA_CARIN-Alliance-Federated-Trust-Agreement_FINAL-12.3.2020.pdf
- <https://myidentity.org.uk/>
- <https://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html>
- <https://www.who.int/groups/smart-vaccination-certificate-working-group>
- <https://www.w3.org/community/dic/>
- <https://pages.nist.gov/800-63-3/>
- <https://ktdi.org>
- <https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/digital-identity-trust-framework/>
- <https://www.iif.com/Publications/ID/4416/FRT-Episode-94-BankID-and-the-Future-of-Identity>
- <https://www.paconsulting.com/insights/is-bankid-positioned-for-the-future/>
- <https://www.statista.com/statistics/1170678/india-share-of-population-covered-under-aadhaar/>
- <https://www.ndid.co.th/>
- <https://thepappers.com/digital-identity-security-online-fraud/belgian-identity-app-itsme-gets-eur-247-mln-to-finance-growth-plans>
- <https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/digital-id-the-opportunities-and-the-risks>
- <https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/digital-id-the-opportunities-and-the-risks>
- <https://www.scnsoft.com/blog/telemedicine-statistics>
- <https://www.onespan.com/blog/reducing-friction-in-online-account-opening-with-digital-identity-verification>
- <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth>
- <https://e-estonia.com/wp-content/uploads/eestonia-guide-2018.pdf>
- <https://www.onespan.com/blog/reducing-friction-in-online-account-opening-with-digital-identity-verification>



COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org