MOBEY FORUM REPORT

January 2023

THE RISE OF DIGITAL IDENTITY WALLETS: WILL BANKS BE LEFT BEHIND?

A report by Mobey Forum's Digital Identity Expert Group

THE RISE OF DIGITAL IDENTITY WALLETS: WILL BANKS BE LEFT BEHIND?

Report by Mobey Forum's Digital Identity Expert Group

Co-Chairs:
Jukka Yliuntinen, Giesecke+Devrient Mobile Security GmbH
Kevin Faragher, Interac

Report Executive:
Reuben Jacob, TD Bank

Expert Group Participants:
Peter Fjelbye, Nets
Merja Ågren, Nordea
Mikko Hiekkataipale, Nordea
Bo Harald, MyData.org
Thomas Fromherz, Netcetera
Arjen Hollander, Thales Group
Erik Vasaasen, Okay
Antti Kettunen, Tietoevry
Roland Eichenauer, Nets
Mats Enqvist, BankID BankAxept AS
Eldo Devole, SHC

mobey forum

Copyright © 2023 Mobey Forum

Contents

Introduction	4
Trust Economy, Digital Identity and Digital Identity Wallet	5
Guiding principles	6
The landscape	6
Roles for banks	8
Business models	12
Liability	12
Use cases	13
Ingredients of Successful Digital Identity networks	14
Role of Non-Banks (Public Sector and Big Tech)	15
Outlook and Conclusions	17
Appendix	18
Working of a Digital Identity Wallet	18
Technical Standards	19
Regulatory Environment	20
Trust Over IP	22
Decentralized Digital Identity Models	23
Join Mobey Forum	25

Introduction

For decades, banks have acted as the trusted custodians of customers' personal data. With strong Know Your Customer (KYC) procedures, strict regulation, high customer engagement, and best in class security and authentication, banks have a unique opportunity to expand their portfolio of services to become brokers of trust in the trust-based digital economy or 'Digital Trust Economy', where entities including people, businesses, and machines can exchange data with each other in a reliable and trustworthy manner.

The objective of this report is to provide decision-makers and strategic leaders within financial institutions with the information required to answer the question: "What can banks do to ensure that they will not be left out of the Digital Trust Economy?".

By considering viewpoints from banks, and through an analysis of the current landscape, trends, regulation, opportunities, and risks, this report will arm decision-makers and leadership within the banking industry with the knowledge and expertise required to take a leading position in the Digital Trust Economy. This report also features insights from a survey of prominent financial institutions around the world, conducted by the Expert Group in mid 2022, and reflects the current views of the financial institutions on the topic of Digital Identity Wallets.

Trust Economy, Digital Identity and Digital Identity Wallet

One of the best ways to build trust online and in wider economies is through the use of Digital Identity. The Expert Group defines Digital Identity as a collection of verified information about an individual, organization, or device that exists online (or on a network). Digital Identity provides a trust layer to online transactions, enabling entities (individuals, businesses, devices etc.) to establish the authenticity of the counterparty they are engaging with online and establish confidence in the transaction.

The existence of multiple identity credentials issued by multiple Issuing Parties can make managing credentials challenging. To solve this challenge, Digital Identity Wallets can be leveraged by entities to effectively store and manage their Digital Identities.

The Expert Group defines a Digital Identity Wallet as a software application, such as a mobile, desktop, or web application, that enables strong identification for individuals, organizations, or devices, and facilitates the ability to present, verify, store, and manage identity credentials to other entities in the network. The Digital Identity Wallet can also be referred to as a data, fact, or trust wallet.

In addition to storing and managing data attributes and credentials, a Digital Identity Wallet can also be used to determine the eligibility of individuals to securely connect to devices and add a trust layer to the Internet of Things (IoT).

It's important to note, however, that the term "Wallet" is an imperfect label. It is often used to describe a mobile application and can have different meanings and perceptions associated with it. The Expert Group believes that the terminology used to describe an end user application should be meaningful to the customer—something that the customer can relate to and resonate with. For example, Apple changed the Passbook branding of their mobile app to Apple Wallet so that customers could easily grasp its functionalities resembling those of an actual physical wallet.
For the purposes of this report, however, the term Digital Identity Wallet will be used.

Some examples of Digital Identity "Wallets" include BankID mobile apps in Scandinavia, Verified.Me in Canada, and Aadhaar in India, to name a few. Digital Identity Wallets can differ in the way they are implemented, and have different models, standards, and technologies around which they are built. Some of these will be described at a high level in the appendix.

Guiding principles

The Expert Group determined that the Digital Identity Wallet should be developed around the following guiding principles:

Choice and Consent: The Digital Identity Wallet should be built around the customer's choice and consent. The customer must be able to choose if they would like to opt in and should not be required to do so. Furthermore, a customer's personal information should only be shared with their consent.

Transparency and Simplicity: The Digital Identity Wallet should have a user interface that is easy to understand and must be transparent regarding the way the customer's data is stored, shared, and verified.

Control and Privacy: The customer should be able to own and control their data attributes and credentials. The issuer, Relying Party, and Digital Identity Wallet solution provider must not be able to track where or how the identity attributes are used.

Minimal Data Sharing: Only essential information about a customer should be shared and should only be done so through zero-knowledge proof, selective disclosure, and other techniques to minimize data sharing. Steps should be taken to protect customer privacy and prevent oversharing as much as possible.

Interoperability: As momentum grows in the Digital Identity Wallet space, a plethora of tech standards and governance mechanisms are being developed and adopted. Interoperability among wallets issued by governments, fintech, Big Techs, and banks, should be the foundational standard.

Human-Centered: The Digital Identity Wallet must keep the customer at the center of its design. The user experience should be an extension of the customer's life and must focus on adding value to the customer's life.

Security: The Digital Identity Wallet must have strong security protocols and authentication mechanisms in place to ensure that only the owner of the identity credentials has access to the wallet and personal information is not misused. It should also be possible to restore a wallet and its credentials securely and conveniently.

The landscape

The digital economy has a trust issue. It is extremely challenging to authenticate and verify the identity of an individual over a digital channel. Most of the most common methods used today, such as password combinations, knowledge-based authentication etc., have several shortcomings and risks.

As the world becomes increasingly digitized, governments across the world have recognized the need for a robust Digital Identity system and are prioritizing legislation aimed at protecting customer information.

In Europe, eIDAS, which provides regulation around electronic identification and trust services related to electronic transactions, is being updated to account for different trust services, improve efficiency, better meet user expectations, and meet market demand.[1] The

[1] https://www.eumonitor.eu/9353000/1/j4nvke1fm2yd1u0_j9vvik7m1c3gyxp/vljcg0sohcyk/v=n2p/f=/com(2021)290_en.pdf

Copyright © 2023 Mobey Forum

regulation also seeks to establish a Digital Identity Wallet, which will be available to all EU entities (citizens, residents, businesses, etc.).

Canada hasn't come up with a nationwide regulatory framework for Digital Identity yet, but provinces have made significant strides in the Digital Identity space on their own. Furthermore, many of the provincial discussions are moving towards the provision of a Digital Identity Wallet. The Digital Identity programs in Ontario and British Columbia, for example, are exploring Digital Identity Wallets with the functionality to store, manage, and use identity credentials.

Several other countries have government-led Digital Identity or digital trust systems, such, as Estonia's e-ID and India's mAadhaar, which have seen wide scale adoption. Other countries such as the United Kingdom, the United States, Japan, Australia, and China, are also following suit. (See Appendix for more information on Regulation.)

In fact, research from Gartner indicates that over 30% of national governments will provide Identity Wallets for mobile phones by 2024.[2]

From a consumer perspective, there is a strong demand for Digital Wallets. Over 66% of Americans expect to have a Digital Wallet by 2023 and 54% of consumers in all age groups prefer to use a Digital Wallet issued by a bank.[3] With people relying on identity proving and verification on an almost daily basis, issuing a Digital Identity Wallet can enable banks to better meet customers' needs, stay relevant in customers' lives, and remove identity-related pain points, providing issuing banks an opportunity to potentially have a competitive advantage and improve brand loyalty. Even though providing a Digital Identity wallet may present an opportunity for banks to improve the customer experience and to increase engagement, this alone does not mean they are best suited for the role of a Digital Wallet issuer or provider, but it is a good basis to build on.

Examples of Digital Identity systems that have been set up by banks include BankID in Norway and Sweden, and Canada's Verified.Me. All these systems have successfully been able to bridge the divide between private and public sector to drive adoption. Markets are however very different and each geography requires thorough analysis on local drivers and users preferences.

As the demand for Digital Identity grows, there has also been significant progress made regarding the technical standards around this domain. These standards provide specifications and guidance around how credentials can be expressed, consumed, and verified in a manner that is secure, private, and seamless. Examples of leading standards include W3C(VC), OIDC, Mobile Driver's License (mDL), and Fast Identity Online 2 (FIDO 2) to name a few. (More information on standards in Appendix.)

In addition to Digital Identity standards, there are also Digital Identity Wallet models that provide a methodology for the implementation of Digital Identity Wallets. These models provide guidelines around how identity attributes should be issued, stored, managed, presented, and verified – to name a few. The three main models are 1) Federated Identity Model, 2) Self Sovereign Identity Model and 3) Hybrid Decentralized Identity Model.[4] (More

[2] https://www.gartner.com/en/newsroom/press-releases/2022-02-21-govt-tech-trends-2022-press-release

[3] https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/consumer-trends-in-digital-payments

[4] https://verified.me/wp-content/uploads/2021/04/Primer-and-Action-Guide-to-Decentralized-Identity.pdf

information about how a Digital Identity Wallet works and the various models available in the Appendix.)

The Expert Group says that with most governments moving towards Digital Identity and the issuing of a Digital Identity Wallet, now is the time for banks to think about their role in the Digital Identity system.

Roles for banks

The Expert Group believes that for banks to unlock new use cases and value streams, they should not only focus on serving their customer's financial needs, but also their customer's broader life needs. One of the ways banks can do this is by going beyond the traditional trust services they have historically provided and provide Digital Identity -based services.

A recent McKinsey report on the consumer data opportunity and the privacy imperative found that the highest number of survey respondents (44%) trust financial institutions and healthcare companies with data management and privacy,[5] while the corresponding figure for public sector and government, telecommunications, consumer-packaged-goods, or media and entertainment companies was less than 13%.

The growing need for trusted online identity means that Digital Identity services can enable banks to be more embedded in their customers' daily lives. The Expert Group also believes that banks, with their strong position of trust, can play a prominent role in the Digital Identity space to mitigate their risk of disintermediation in a world where banking and the future of money is being disrupted.

To determine their approach towards Digital Identity, banks should start by looking at their broader strategic framework and objectives to determine how Digital Identity can help them achieve their goals. Banks should prioritize the following benefits Digital Identity can deliver against their strategy's critical success factors:

- Improve customer experience
- Lower operational costs
- Mitigate risk and reduce fraud
- Add new revenue streams
- Create deeper customer relationships

The complexity and breadth of Digital Identity networks means there are several roles a bank can play in the network. The most common roles include: 1) Wallet Issuer 2) Credential Consumer /Relying Party (RP) 3) Credential Issuer/ Identity Provider (IDP) 4) Authentication Provider and 5) any combination of these.

1. Wallet Issuer

Benefits:

- Potential to generate new revenue streams by sharing data
- Embeds bank as key player in the digital economy
- Embeds the bank in the customer's non-financial digital life
- Monetizes internal investments in authentication, KYC compliance and security
- Ownership over the customer experience
- Ownership role of network governance

For banks prioritizing the addition of new revenue streams and looking to deepen relationships with customers, Digital Identity Wallet issuance offers a possible approach for banks to control the entire customer experience around their online services, including the identity verification piece. This, in turn, means

[5] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

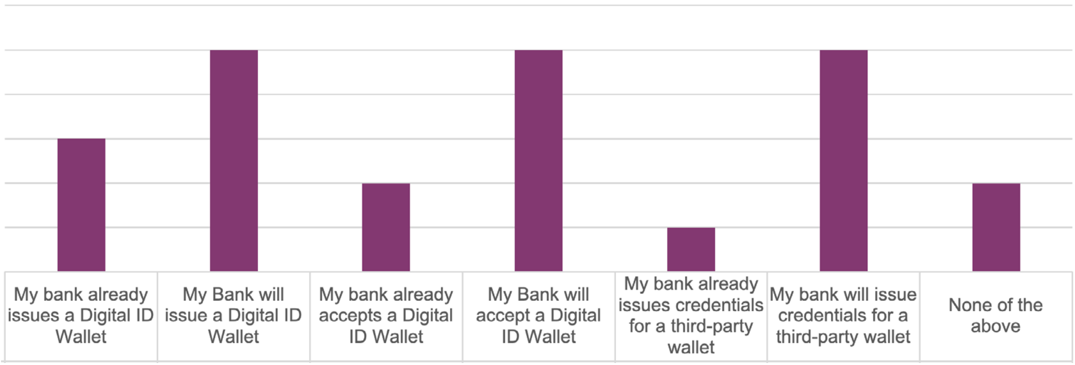
Copyright © 2023 Mobey Forum

that banks would be able to offer a unique and differentiated customer experience and be first to market with new digital offerings – a key opportunity to gain a competitive advantage.

In fact, momentum is building among global banks toward accepting and issuing Digital Identity Wallets and Digital Credentials. The Expert Group surveyed several banks in North America, Europe, and Africa to get a more comprehensive view of banks' positions with regard to Digital Identity Wallets.

In this survey, 66% of banks report that they have already issued a Digital Identity Wallet or will issue a Digital Identity Wallet in the future,

Does or will your bank issue or accept Digital ID Wallets?



In Europe, eIDAS regulation will likely drive this trend, as it mandates large businesses, such as banks, to accept Digital Identity Wallets. General Data Protection Regulation (GDPR) article 20 mandates that all enterprises make the data rights holder´s data available. This is a very expensive and cumbersome operation without interoperable generic wallets.

Regulation is not the only driver for banks to adopt the role of wallet issuer. It should be noted that 40% of banks that participated in this survey were not impacted by the eIDAS regulation, suggesting that it is not only regulation driving this trend, but rather that banks see actual value in issuing Digital Identity Wallets.

For banks looking at provisioning their own wallet, the Expert Group believes that there is much to learn from the world of payment apps, especially around how these apps can provide value-added services that enhance customer experience and drive usage. Banks can follow a similar approach by providing an offering that brings together banking, payments, identification, insurance, and more. However, the Expert Group also cautions that there is inherent complexity, operational overhead, and risk involved with issuing a wallet. Winning strategies around market fit, customer adoption, product development, and customer retention are imperative to a creating and launching a successful product. Banks would also need to build partnerships and bring more participants, consumers, and issuers to reap the rewards of network effects.

2. Consuming credentials / Relying Party (RP)

Benefits:

- Reduce friction and cost of onboarding new customers
- Reduce fraud
- Comply with regulation in some jurisdictions

In this role, banks can leverage credentials issued by governments, other banks, and third parties to streamline the customer experience and reduce the operational cost of onboarding/KYC. However, it is important to note that in this scenario, banks would most likely incur costs for consuming the credentials from an Identity Provider.

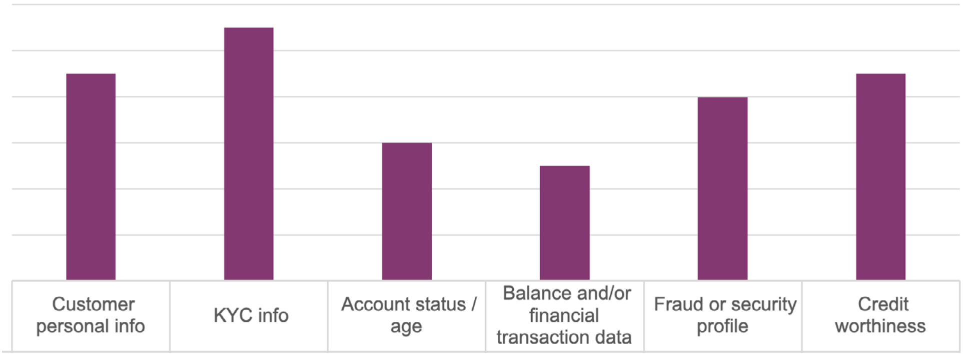
According to the Expert Group survey, third party credentials that banks are most interested in consuming to better serve their customers are: customer's personal information, KYC information, credit worthiness, and customer fraud profiles. This information aligns with credentials that banks are willing to provide to third parties.

For banks that are looking for a comparatively low risk and easy-to-implement approach to participating in the Digital Identity system, consuming credentials is the best way forward as it is most likely that governments and other Identity Providers will start issuing their own credentials. Banks acting as Relying Parties can then leverage these credentials to drive their own use cases. For banks in Europe, adopting this approach would also help meet the requirements of eIDAS regulation.

What kind of credential attributes you are or would you like to receive to serve cistomers better?

Other:

1. Proof of accreditation
2. Proof of employment
3. Business identity information



Copyright © 2023 Mobey Forum

3. Issuing credentials / Identity Providers (IDP)

Benefits:

- Potential to generate new revenue streams by sharing data
- Improves the bank's role as a player in the digital economy
- Improves the role of the bank in customers' non-financial digital life

For banks that don't include Digital Identity Wallet issuance on their strategic roadmap, there is an opportunity to issue their own credentials and have those issued to a third party Digital Identity Wallet. Acting as an issuer of credentials gives banks an opportunity to be an authority of trust in the Digital Identity system.

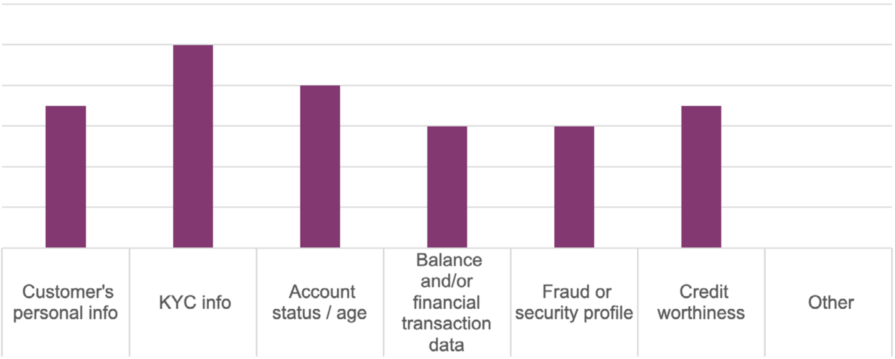
Compared to issuing a Digital Identity Wallet, this approach would lower costs since it eliminates the need to implement and support a wallet. The downside of this approach, however, is that banks might struggle to offer a distinct customer experience or build out their brand without issuing their own wallet.

Banks that do go the route of issuing their own credentials for third-party Digital Identity Wallet consumption would be akin to banks issuing their credit or debit cards to be managed by third-party payment wallets, where whole user experience is based on the Wallet Provider's design and implementation. This leaves very little room for banks to differentiate themselves from the crowd.

When it comes to issuing credentials, the choice of partner(s) becomes important. Banks can partner with multiple third-party wallets, allowing them to make their credentials available across many channels and potentially bring the banks closer to the life events of their customers and potential target audience.

Survey from the data indicates that, when it comes to deciding which credentials to issue, banks are most comfortable providing KYC information.

What kind of data does or will your bank consider providing to other parties in the future, assuming a liability scheme that meets your risk appetite is in place (or zero liability)?



The Expert Group recommends that as banks consider the kind of data they are willing to share, they should also consider how the data they provide can be used for the larger benefit of society. Banks that go beyond providing KYC information can offer richer Digital Identities that have the potential to unlock significantly more use cases and add greater value in customer's lives.

When exchanging information within the identity network, banks surveyed feel that the most important considerations are customer privacy, customer consent and liability.

The Expert Group concludes that banks don't necessarily need to provision a wallet to be front and center in the Digital Identity system. Instead, they can start by creating the infrastructure that enables the issuing and verifying of verifiable credentials. Using this infrastructure, banks can make inroads into the identity space by embedding identity services into online channels. While banks think about the role they would like to play in the Digital Identity system, they should also start having conversations with the lines of business about how they can redesign their services and processes to work with verifiable credentials and ensure that they are able to establish connectivity and work with Digital Identity Wallets. Further information on roles and their definitions can be found in the Appendix.

Business models

The specific business models behind a Digital Identity network differ for each jurisdiction and depend on the competitive landscape, regulation, and other factors. In general, the economic model trends towards the Relying Party (RP) paying a transaction fee to receive the validated data from the Identity Providers (IDPs) and the trusted network. Revenue generated from RP fees is often shared across IDPs and the network operators to recoup investment in the network, cover operational and governance costs, and ultimately generate more profit for both parties.

It is rare for the end consumer to be charged to share their data. While consumers do benefit from the convenience, most would not expect to pay to share data that is rightfully theirs.

In some cases, IDPs and network operators could charge a premium to guarantee the validity of the data being provided—a sort of insurance premium for the RP that helps offset risk in high value transactions or when sourcing data from IDPs with lower level of assurance.

Liability

For Digital Identity to be viable and accepted, it needs to be trusted. Currently, there are multiple technologies, models, and standards related to Digital Identity that can provide a high level of assurance for Digital Credentials. Depending on an organization's requirements, they can design and implement their processes in a way that allows them to issue or consume credentials with varying levels of assurance. However, to effectively utilize Digital Identity, banks must also model how to manage liability. If a bank is an Identity Provider and a Relying Party using a Digital Identity credential issued by the bank becomes a victim of fraud, the question is: how much liability falls on the Issuing Party vs the Relying Party.

Copyright © 2023 Mobey Forum

For example, legislators typically consider banks and financial institutions to be the “victims” in cases of identity theft. However, unless insured, banks often need to absorb the costs of such fraudulent actions. There may be cases where the business and marketing practices of the third-party RPs may negligently lead to identity theft. In such cases, financial institutions (Issuing Party) may face potential liability for the negligence of third-party RPs.

Existing Digital Identity schemes have solved for liability by having either a zero-liability model or a limited liability model. Banks should ensure that their liability model is transparent—enabling each party in the value chain to assess their risk and match it with their own risk appetite. Finally, liability equals cost, and businesses considering operating in the Digital Identity space need to be able to assess this cost and cover it accordingly.

Use cases

Since Digital Identity is expected to become the standard method for authentication in the future, it will be a key driver of the digitalization of bank services. Within banks, there is a plethora of use cases where Digital Identity and Digital Identity Wallets can be applied. The Expert Group surveyed leading financial institutions to glean which use cases these institutions prioritize when it comes to extracting value from a Digital Identity Wallet.

What is the most important specific use case in a banking context that can benefit from Digital ID Wallet?

1. **Onboarding 75%**
2. **KYC AML 25%**
3. **Digital signing 8%**
4. **Embedded finance 8%**

It comes as no surprise that a majority of banks reported that Digital Identity Wallets would be most beneficial for onboarding processes. Digital Identity Wallets can be leveraged to significantly improve the customer experience during onboarding by streamlining the identity validation process and enabling a fully digital experience. For example, banks in Canada can leverage their Digital Identity Wallet to make opening an account a completely virtual process, eliminating the need for an in-person branch visit to verify identity. By removing branch visits, a significant customer pain point, banks were able to dramatically improve the customer experience.

KYC/AML and digital signing use cases could also significantly benefit from the use of a Digital Identity Wallet. Currently, banks that don’t have a fully digital onboarding experience have cumbersome KYC/AML processes requiring physical paperwork and several manual steps that are time consuming and costly. Banks that offer digital onboarding (without leveraging Digital Identity) receive far too many false negatives where a genuine customer fails to clear the process. When it comes to this particular use case, Digital Identity Wallets can help streamline the customer journey, eliminate paperwork, and drastically reduce the number of false positives. Banks in India can leverage the Aadhaar Digital Identity System, cutting KYC/AML costs by over 80%. Norway has also been able to significantly cut costs related to digital signature use cases by leveraging Digital Identity.

Embedded Finance is another area where banks can leverage Digital Identity Wallets to provide 'Embedded Identity' for non-financial institutions. Businesses that need to verify customer identities such as mobile network operators, car rental agencies, etc., can leverage bank-based Digital Identity credentials by embedding Digital Identity Wallets into their checkout process. This would be similar to how Apple Pay has been integrated to merchant checkout pages.

While the above use cases represent a more short-to-medium term opportunity for banks, Digital Identity Wallets can also potentially be used to drive future use cases in Open Banking, the Metaverse, and Decentralized Finance.

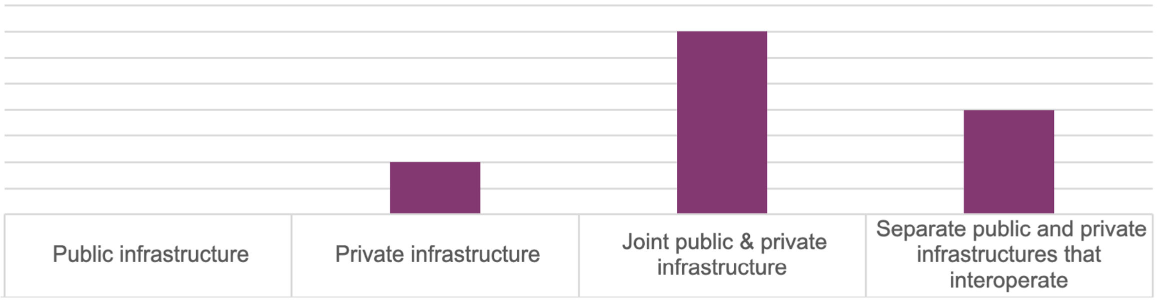
For banks still on the fence, the Expert Group believes that using Digital Identity Wallets for internal use cases can be a start. Digital Identity Wallets can provide a secure and low-friction user experience that solves many of the challenges that currently plague organizational access management systems, such as high costs, security vulnerabilities, and manual processes.

Ingredients of Successful Digital Identity networks

In most cases, banks are most successful at spearheading a Digital Identity system that was developed by a consortium of leading banks coming together and taking the initiative to set the standards, framework, policies, and governance for the Digital Identity system. This approach has enabled Digital Identity to reach the majority of its users and has also enabled banks to unlock more use cases. Finland's Bank eID, Norway's BankID, Denmark's NemID, and Sweden's BankID are all examples of successful Digital Identity schemes built by a consortium of banks. Similarly, Canada's Verified.Me is another example of a Digital Identity solution led by Canada's major banks.

While there is global momentum building for banks to issue and accept Digital Identity Wallets and Digital Credentials, it is important to note that entities outside the finance sector are slow to accept Digital Identity. When these non-bank entities participate in the Digital Identity system it will increase the richness of the use cases being implemented. The Expert Group believes that regulation will be the primary driver of adoption in the non-bank space.

What do you see as the ideal technical identity network infrastructure operating model?



Copyright © 2023 Mobey Forum

The Expert Group's survey highlighted a lack of confidence in the public sector to establish and operate a successful Digital Identity infrastructure on its own. The group believes that joint public and private infrastructure or separate public and private infrastructures that interoperate are the best options for implementing Digital Identity systems. Separate public and private infrastructures that interoperate can potentially be very beneficial, as it can help build the locus of control and responsibility, keeping both clearly delineated.

On a more technical note, it's well understood that achieving trust between two parties requires technological and governance-level interoperability. This means that interoperable Digital Wallet systems cannot be developed solely based on individual technical standards or components. To achieve a truly global Digital Wallet system, the bank's trust infrastructure architecture must include both technical and governance frameworks, as well as interoperability, across each layer of the stack. Interoperability requires standardization on applied technologies, and we address one of the key frameworks in the appendix.

As identity standards constantly emerge and evolve, some will be complementary while others may be in competition with each other. The Expert Group calls for banks to join together and lead the way to set these standards, especially regarding trust models. This includes addressing how liability is covered between system participants and determining on what terms business is conducted. One example of this is Findy, a joint public-private sector initiative in Finland. The stakeholders in this initiative are collaborating to build a Digital Identity Ecosystem beyond eIDAS.

Role of Non-Banks (Public Sector and Big Tech)

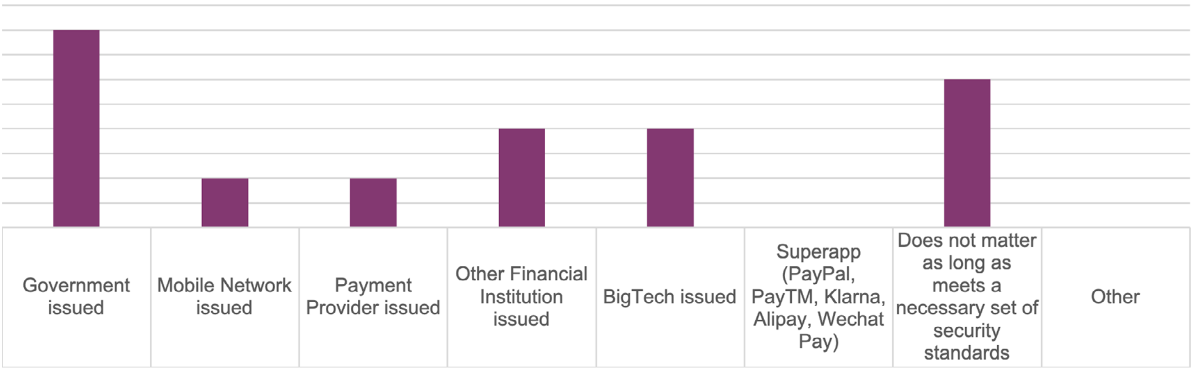
When it comes to Digital Identity systems, one of the key challenges is driving adoption and usage frequency. To overcome these challenges, more entities need to participate in the ecosystem as Relying Parties.

However, as banks have been relatively risk-averse and very selective about who they receive data from and who they share data with, bank-led Digital Identity networks have been slow to bring more Relying Parties into the ecosystem. As a result, use cases continue to be limited.

It is important to highlight that this trend is changing. While most banks would primarily consider and be comfortable accepting government-issued wallets, the Expert Group believes that in time, as more networks are built, and standards, privacy, security, and interoperability increase and mature, banks will be more open to accepting wallets from other financial institutions, Big Tech, etc.

This is evidenced from the survey where several banks report that the issuer of the wallet does not matter so long as it meets a necessary set of security standards. The Expert Group believes that the reason banks are not open to super apps or fintech companies is because of the expectation that they might charge for a service and the lack of customer reach for these apps.

Which of the following Identity Wallet issuer types would your bank consider accepting:



Ultimately, the Expert Group believes that the most trusted identity attributes are those issued by the government and, as a result, the Digital Identity strategy and vision put forward by governments are the ones that will prevail. Governments will set standards around technology, security, governance, and privacy. Government regulation will also drive adoption of Digital Identity and bring more Relying Parties into the ecosystem.

Big Tech has identified the potential of rich Digital Identities and have made significant investment and consolidation in the Digital Identity space, but progress is extremely slow.

Apple recently announced that users can add their Digital Identity documents, such as a driver's license or state ID, to their Apple Wallet and then tap their device to verify their identity at select checkpoints.

Microsoft has also partnered with leading identity verification providers such as Acuant, Clear, and Jumio to name a few, to launch Microsoft Entra Verified ID – a decentralized identity service. There are also a number of technology companies investing in Digital Identity and venture capital investments are very high in this space. One such case is how Avast is building momentum in the self-sovereign identity space through the acquisition of Evernym and Securekey, which are both leading Digital Identity technology companies. Avast has since been acquired by Norton Lifelock, further highlighting the focus in this space.

With Big Tech seeking to incorporate Digital Identity credentials into their own wallets, banks that want to stand up their own Digital Identity Wallet need to be cautious. Big Tech firms have global reach, harmonized user experience, control of devices, lack of cross-border constraints, and strong product development experience. However, the Expert Group believes that banks looking to issue their own Digital Identity Wallet need to leverage the fact that customers don't trust Big Tech with their personal information as much as they trust banks. While Big Tech has a larger customer base compared to banks, and is more experienced in the product realm, the strength of banks lies in their position of trust and experience dealing with regulators.

Copyright © 2023 Mobey Forum

Outlook and Conclusions

The momentum shift towards digital transactions for all aspects of our life's financial, health, education, commerce, entertainment, and social needs is not slowing down. Traditional identity and access management systems are simply not equipped to handle the challenges that come with the volume, velocity, and variety of these digital use cases.

From protecting the digital safety and security of individuals in the Metaverse, to providing a single authentication layer for Open Banking, Digital Identity overcomes the deficiencies and limitations found in traditional Identity Access Management (IAM) systems.

One of the biggest advantages of Digital Identity has, is that it provides a system where the individual is the true owner of their identity information and controls how this information is managed, stored, and consumed.

Growing demand by customers to protect their identity, coupled with regulation geared towards protecting customer information, the Digital Identity space is extremely lucrative and attracting players from Big Tech and fintech to startups.

For centuries, banks have enjoyed a strong position of trust. Today, banks have a unique window of opportunity to expand beyond the domain of traditional banking and become leaders in the Digital Identity space. However, as the competition in the space heats up, this window of opportunity will close fast, and banks must act now if they want to play a role in the future of the Digital Trust Economy.

The convergence of Digital Identity Wallets and Payments Wallets will present a unique opportunity, according to the Expert Group. With regulation being built around incorporating Strong Customer Authentication (SCA) to further secure payments, supplementing payments with Digital Identity is a solid option to authenticate online payments while minimizing customer friction. This is a space where banks—with their experience, reach, regulatory position, and funds—are primed for success.

The Expert Group believes that banks should have a strategy for Digital Identity and determine what role they would like to play in the Digital Identity system to seize these opportunities. Banks also need to collaborate closely with governmental bodies, who are responsible for Digital Identity as this sets the basis for strong and widely-trusted implementations. Furthermore, banks should be part of forums and expert groups, and to contribute to the Digital Identity conversation. They should ensure they are engaged and informed about the latest trends and standards, and also keep an eye on regulation.

As a concluding note, the Expert Group at Mobey Forum believes that it is the responsibility of the banking sector to elevate its role and contribute to the Digital Identity system. Digital Identity holds great promise for society at large. Without banks, it's going to be very difficult for society to stand up a Digital Identity system. So, it's not just about a business case, it's about driving positive, real, and long-lasting change.

Appendix

Working of a Digital Identity Wallet

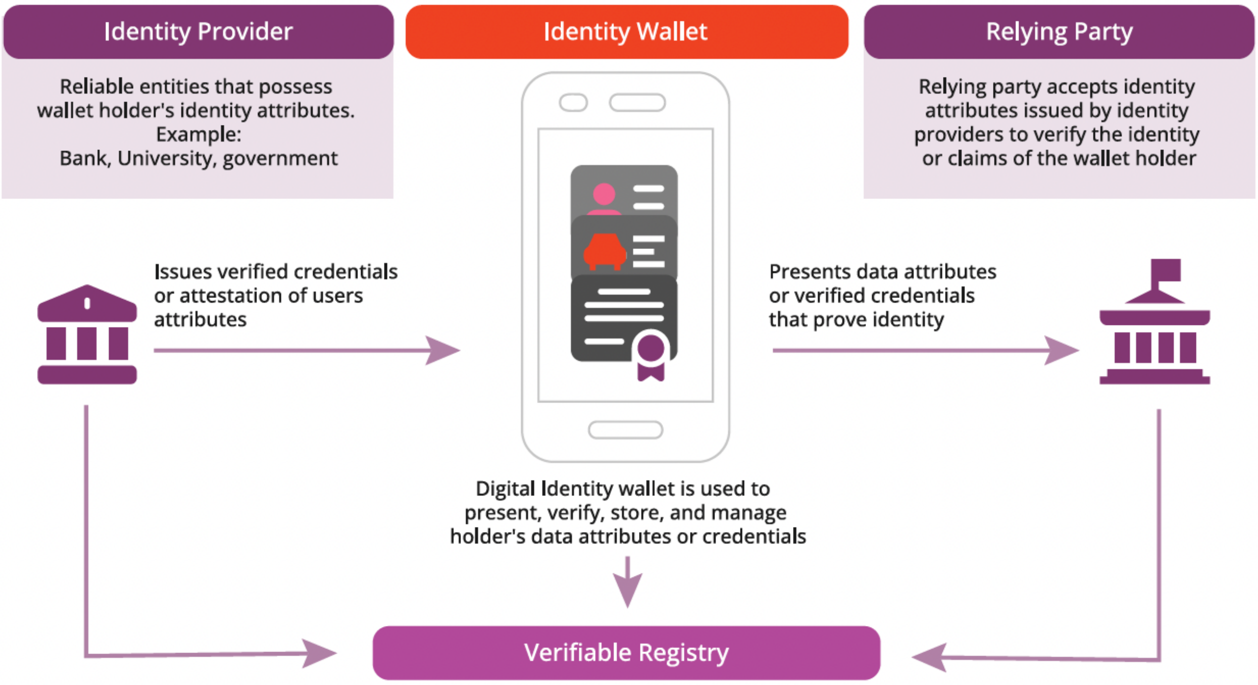
At a high level, there are three roles that facilitate a Digital Identity system built around a Digital Identity Wallet.

Identity Providers (IDPs) – Identity Providers are issuers of data attributes and/or verified credentials. These entities have completed a KYC process, based on which they are able to hold and attest to claims made by the wallet holder in the form of data attributes or verified credentials.

Relying Party (RP) – Relying Parties are entities that are interested in verifying claims made by the wallet holder. They accept and rely on the attestation provided by Identity Providers to verify the identity or claims of the wallet holder.

And finally, we have the Digital Identity Wallet. Ideally, a Digital Identity Wallet is capable of accepting and locally storing data attributes or verified credentials issued by an Identity Provider. In addition, it is also capable of presenting these stored attributes or verified credentials to Relying Parties that accept identity attributes issued by Identity Providers. This model, where there is no intermediary coming in between the wallet holder and the Relying Party, is called the self-sovereign model.

In the self-sovereign identity model, a verifiable registry is used to store the credential schemas, issuer public keys, credential definition, etc. that can be used by the Relying Party to verify the authenticity of the credential without contacting the Identity Provider or Issuing Party.


Identity Provider
Reliable entities that possess wallet holder's identity attributes. Example: Bank, University, government
Identity Wallet
Relying Party
Relying party accepts identity attributes issued by identity providers to verify the identity or claims of the wallet holder
Issues verified credentials or attestation of users attributes
Presents data attributes or verified credentials that prove identity
Digital Identity wallet is used to present, verify, store, and manage holder's data attributes or credentials
Verifiable Registry

Copyright © 2023 Mobey Forum

The wallet can also simply facilitate the exchange of the wallet holder's identity attributes between the Identity Provider and the Relying Party. In this model, called the federated identity model, the Wallet Provider acts as an intermediary between the wallet holder and the Relying Party. The presence of a trusted intermediary takes away the need to have a verifiable registry. (More information in a later section.)

Overall, the Expert Group believes that Identity Wallets should not be looked at in isolation as they are just part of the picture. Identity wallets should always be considered as part of a larger trust system (issuers, Relying Party, use cases, regulation, standards etc.).

Technical standards

Technical standards that relate to Digital Identity Wallets provide specifications and guidance regarding how credentials can be expressed, consumed, and verified in a manner that is secure, private, and seamless. Below is an overview of the technical solutions and standards that are being adopted or promoted by various entities.

1. W3C (VC): W3C Verifiable Credentials standard provides recommendations for a Verifiable Credentials Data Model and a mechanism to express credentials on the web in a way that is cryptographically secure, privacy respecting, and machine-verifiable[6]. This includes a core data model, guidance on how to issue and verify credentials, and use of decentralized identifiers to establish secure communications, to name a few.

2. OpenID Connect (OIDC): OIDC is an authentication protocol that enables identity verification by providing an identity layer over the OAuth 2.0 protocol (industry-standard protocol for authorization)[7]. This provision of an identity layer over the OAuth 2.0 protocol facilitates the requesting and receiving of identity information between clients and end users.

3. Mobile Driver's License (mDL): mDL is a digital version of the data encapsulated within a physical identity document such as a state-issued driver's license or identity card[8]. This digital representation of an identity document is stored on the end user's device with the ability to be updated when needed. mDL is based on the draft ISO/IEC 18013–5 standard which provides the framework for receiving and verifying attributes from an mDL3.[4]

4. Fast Identity Online 2 (FIDO 2): FIDO 2 is the most recent standard from the Fast Identity Online alliance that aims to create a stronger and more seamless authentication framework that reduces the reliance on passwords. FIDO 2 works towards this aim by incorporating the web authentication standard written by FIDO and W3.

[6] https://www.w3.org/TR/vc-data-model/

[7] https://openid.net/connect/

[8] https://www.mdlconnection.com/mobile-drivers-license-faq/

Around the world, different parties play a role in establishing standards. For example, the EU has established eIDAS (electronic identification and trust services) regulation aimed at setting standards for Digital Identity Wallets. BankID and Verified.Me are examples of Digital Identity Wallets where banks have built a consortium to set standards to issue one wallet to all people within a jurisdiction.

As identity standards are constantly emerging and evolving, some of them will be complementary while others may be in competition with each other. The Expert Group calls for banks to join together and lead the way in setting these standards. One example of this is Findy, a joint public-private sector initiative in Finland, that is working to build a Digital Identity Ecosystem beyond eIDAS. Other countries such as Norway and Sweden are following suit.

Regulatory Environment

As technology has quickly evolved to meet the identity verification needs of customers, so have the security and privacy risk implications. As a result, regulation is constantly playing catch up. This has led to uncertainty around regulation related to Digital Identity. With growing concerns about how consumer identity-related information or data is consumed, processed, and used, regulatory authorities working on Digital Identity are prioritizing legislation aimed at protecting customer information[9].

Europe: The Electronic Identification, Authentication, and trust Services (or eIDAS), established in 2014, provides regulation around electronic identification and trust services related to electronic transactions[10]. This framework has been in effect since July 1st, 2016 and is aimed at creating a user-friendly service that promotes the growth of cross-border public services and drives digital innovation in the EU.

However, a 2021 report from the commission to the European Parliament and the Council on the evaluation of eIDAS found that there was scope to improve the regulation to resolve differences among member states and different trust services, improve efficiency, meet user expectations, and meet market demand[11].

The regulation also seeks to establish a Digital Identity Wallet, which will be available to all EU entities (citizens, residents, businesses, etc.). EU Digital Identity Wallet program, a consortium of six European countries, has announced an initiative to launch a pilot cross-border payments system. The consortium has also been able to garner support from a number of public and private entities - highlighting once again, the increasing appetite for a Digital Identity Wallet[12].

Despite the momentum building from a regulatory standpoint from governments across the world, the Expert Group believes that overall, progress is slow and there are a lot of questions

[9] https://www.pymnts.com/news/ecommerce/2022/pymnts-intelligence-challenges-compliance-digital-identity-regulations/

[10] https://go.eid.as/

[11] https://www.eumonitor.eu/9353000/1/j4nvke1fm2yd1u0_j9vvik7m1c3gyxp/vljcg0sohcyk/v=n2p/f=/com(2021)290_en.pdf

[12] https://euroweeklynews.com/2022/09/14/eu-digital-identity-wallet/

Copyright © 2023 Mobey Forum

that need to be answered. Many of the regulatory frameworks such as eIDAS regulation, focus too much on the standards and technology and do not tackle more practical perspectives such as liability, level of assurance, and governance to name a few. As a result, in most countries, banks have taken the lead on Digital Identity and are far ahead of the governments. One of the leading regulatory frameworks on Digital Identity is Europe's eIDAS 2. While more clarity is needed on the regulation, it does mandate the provision of an Identity Wallet by member states to everyone who wants one.

Canada: While Canada hasn't yet come up with a nationwide regulatory framework for Digital Identity, there have been significant strides made by individual provinces in the Digital Identity space. Below is the current state of the Digital Identity landscape in some of Canada's provinces.

Ontario: Ontario has taken the approach of prioritizing the technology and standards that it will use for Digital Identity and is focused on enabling cross-Canadian standards, while strongly focusing on privacy as a core principle of its Digital Identity program. The province has partnered with its information and privacy commissioner, in addition to consulting with over 68 organizations and 100 industry experts to navigate this space[13]. Ontario's Digital Identity Program also has a provision for a Digital Identity Wallet with functionality to store, manage, and use identity credentials.

Alberta: In 2015, the province of Alberta launched MyAlberta Digital ID, a government-backed Digital Identity service that provides easy and user-friendly access to government services online without the need for in-person interaction or physical documents[14]. The service lets Albertans verify their identity online through a single account to access driver's license services, health records, etc. The government of Alberta also plans to launch a digital government identification app aimed at helping users present their credentials[15].

British Columbia: BC was one of the early adopters of Digital Identity and is one of the leaders in this space. The province launched BCeID, an account that provides secure and seamless access to online government services in 2002 and is constantly looking at how to evolve its Digital Identity strategy to meet the needs and challenges of the future. As part of this, the province is exploring how verifiable credentials can provide the foundation for the province's next Digital Identity strategy[16]. The Government of BC also provides a BC Wallet, which enables residents to receive, manage, store, and present their identity credentials.

Other provinces such as Quebec and Saskatchewan are also working towards building a Digital Identity strategy and solution that would make access to online services seamless and streamlined—while also prioritizing customers' privacy and security. Leveraging a Digital Identity Wallet for the provisioning, managing, presenting, and verifying of credentials is being considered.

United States: Like many other countries, the COVID-19 pandemic highlighted the urgency to have a robust Digital Identity system in the United States. This was especially clear during the execution of the US Cares Act, aimed at providing relief to American citizens during the COVID-19 pandemic.

[13] https://news.ontario.ca/en/release/1000787/ontario-releases-technology-and-standards-for-digital-identity

[14] https://www.westernstandard.news/news/alberta-hiring-digital-id-director/article_58fa69df-2ead-5819-a117-d41e9876e203.html

[15] https://www.albertaparty.ca/digital-id-2019

[16] https://www.itworldcanada.com/article/b-c-s-cio-says-verifiable-credentials-key-to-creation-of-national-digital-strategy/488677

The 'Improving Digital Identity Act of 2021'[17] was introduced by a bipartisan group of congressmen. The act creates a federal task force to establish a government-wide approach to enhance Digital Identity. In addition, it would entrust the National Institute of Standards and Technology (NIST) to put in place the standards and requirements needed to guide federal, state, and local governments when it comes to providing Digital Identity services and support. Finally, a grant will be awarded by the US Department of Homeland Security to states in order to help them upgrade their current Digital Identity systems.

Trust Over IP

Trust over IP Foundation is a project hosted at Linux Foundation with the mission to provide a robust, common standard and complete architecture for Internet-scale digital trust. The vision behind Trust over IP is to create the trust layer of the internet. This can be compared with the backbone of the internet today: the TCP/IP stack.

This trust layer needs to enable independent development of trust ecosystem that are peers in the global trust infrastructure. Each peer would be an instance of a standard "stack" of protocols, just as each device on the Internet runs an instance of the TCP/IP stack. Today, that vision, with its combination of technology and governance, is seen in the two-sided, four-layer stack that is called the Trust Over IP Stack.

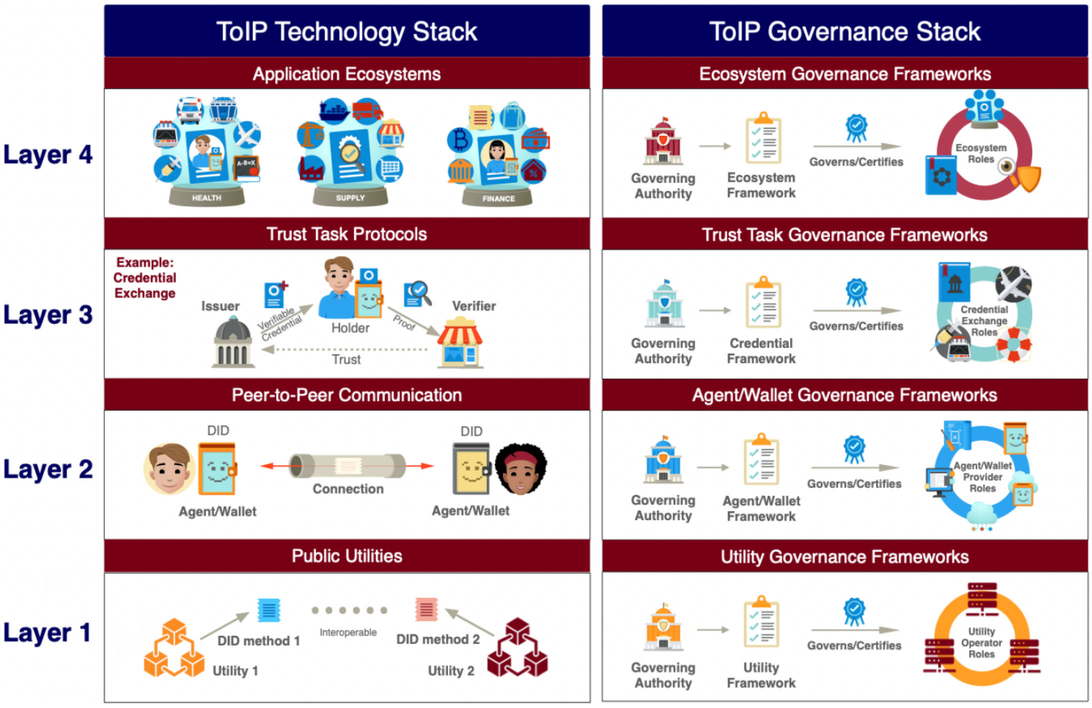


Image source: https://trustoverip.org/blog/2022/01/24/the-trust-over-ip-foundation-publishes-new-introduction-and-design-principles/

[17] https://www.congress.gov/bill/117th-congress/house-bill/4258/texts

Copyright © 2023 Mobey Forum

The Trust over IP stack divides trust infrastructures into four layers, each representing a functionality that is provided usually (but not always) by different actors in the ecosystem.

Layer 1 provides the trust support and public utilities for common functionality, like key verification and trust registries, for the purposes of enabling connectivity and verifications on the layers above it. Public utilities may be centralized or decentralized, but they commonly serve parties across different domains or wallet ecosystems. Examples of Layer 1 services are any ledgers that maintain DID Methods or additionally Government registries and EU Trust lists.

Layer 2 focuses on the connectivity of wallets and other end-devices using Decentralized Identifier (DID)-based keys. It spans the trust capabilities by being agnostic to connectivity protocols, like Bluetooth, NFC, HTTPS, etc. The purpose for this layer is to enable same trusted key-based communication for the layers above it, regardless of its used connectivity method.

Layer 3 describes the various trust task protocols that can be performed when trusted connectivity is enabled. Trust tasks are defined by the business needs of the layer 4. The most well-known trust task is generic verifiable credential exchange. Other trust tasks can be more granular, and business-focused, like provisioning, updating, and verification of Digital Identities, consent management, requesting and signing of digital documents, secure messaging or even digital payment or value exchange in any form.

Layer 4 is the application layer for any business application that needs to engage in trusted interactions. Layer 4 application ecosystems may use any number of Layer 3 Trust Task Protocols. Layer 4 can be any size, ranging from local, few-member business ecosystems up to global interoperability infrastructures for the financial sector.

By implementing the Trust over IP framework, we can ensure global interoperability, scalability, and innovative use of digital trust, while retaining end-user privacy and business benefits of decentralization.

Decentralized Digital Identity Models

With momentum building towards adopting or transitioning to decentralized identity, several players from governments, Big Tech, and banks to identity startups are looking at ways they can carve a niche in fast moving Digital Identity market. This has given rise to three leading models of implementing decentralized identity.

- Federated Identity: In a Federated Identity Model of Digital Identity, one or more entities rely on a single system or organization to provide their authentication needs[18]. In other words, the Relying Parties (those who need to perform the authentication) delegate identity verification to a trusted Identity Provider (IDP)[19]. The most common example of this model is how we can leverage our Google or Facebook credentials and profile to access third-party websites and

[18] https://securekey.com/wp-content/uploads/2020/07/VerifiedMe_OWIWhitepaper_APrimertoDecentralizedIdentity.pdf

[19] https://docs.microsoft.com/en-us/azure/architecture/patterns/federated-identity

services. In this case, Google or Facebook takes the role of an Identity Provider (IDP) and provides our identity/profile-related information to a Relying Party. This solves the problem of creating multiple accounts to access different websites and services. Another example of this model is Login.Gov, a sign-in service that enables access to several participating government agencies using a single Login.Gov account.

- Self-Sovereign Identity (SSI): The SSI model is one that most closely confirms with the idea of truly decentralized identity system. SSI enables individuals to own and fully control their identity-related information. Credential Issuers such as banks, governments etc. provide Digital Credentials to an individual, which they can store in their Digital Identity Wallet. However, individuals control who they share their identity information or Digital Credentials with. They can also choose how much of that identification information they would like to share with a Relying Party. Unlike the Federated Model, SSI does not delegate granting or tracking access this identification information or credentials to an administrative third party[20].

- Hybrid decentralized identity: A hybrid decentralized identity model brings together elements from the Federated Model and the Self-Sovereign identity model and is based an ecosystem where multiple Identity Providers such as banks, governments etc. come together to enable the identity verification needs of an individual. Unlike a Federated Model, it does not rely on a single Identity Provider to facilitate the identification of individuals but rather, involves multiple Identity Providers. Also, unlike an SSI model, the hybrid decentralized identity model does not emphasize sovereignly or possession of credentials[6].

  An example of a hybrid decentralized identity model is a Canadian Digital Identity solution called Verified.Me. This solution provides an ecosystem where several major banks in Canada come together to provide trusted and reliable identity-related information to Relying Parties to facilitate identity verification[21].

[20] https://sovrin.org/faq/what-is-self-sovereign-identity/

[21] https://verified.me

Copyright © 2023 Mobey Forum

Join Mobey Forum

This paper covers the main findings but is by necessity a summary. To get the full benefit of the Mobey Forum Expert Group, we strongly encourage you to join the organisation and actively participate in the work to gain the full range of insights.

Joining Mobey Forum also helps increase your international network and professional profile as an industry expert on Digital Identity or other topics in the industry.

The close community of experts at Mobey Forum allows you to bring forth your own questions and leverage decades of combined experience in navigating challenges and searching for opportunities.

For more information, contact mobeyforum@mobeyforum.org

mobey
forum

www.mobeyforum.org
January 2023