THE STATE OF DECENTRALIZED IDENTITY

INDUSTRY REPORT

tykn

Today

The adoption of Decentralized Identity technology, also known as Self-Sovereign Identity, is rampantly growing around the world. In this report we bring you its most notable implementations in different verticals: Government, Banking, Higher Education, Healthcare, Human Resources, Humanitarian Aid and even the Travel Industry.

As you will see in this report, the direct benefits of this technology are staggering. Users are able to access digital services more frictionlessly than ever before; without passwords, without accounts. All while keeping strict control over their personal data, with minimum sharing of this personal data and the assurance that this data cannot be leaked or breached by third parties.

Decentralized Identity is reducing governmental bureaucracy, enabling access to digital services across borders, paperless travel and the secure storing and sharing of healthcare data. It is creating a better banking experience, making human resources more efficient, providing quicker access to humanitarian aid distribution and even helping tenants avoid ID theft.

In the next 10 to 15 years, our ID cards and personal documents will not be for daily use anymore; they will be backups, safely stored away at home. The credentials we use in our day-to-day lives will be digital, stored in our mobile wallets in the same way we now carry our debit and credit cards on our phone to pay for groceries. Decentralized Identity technology will pave the way for this digital transformation without compromising on security or privacy.

Lets dive into the State of Decentralized Identity.

Germany and Spain...

...are building an ecosystem of decentralized digital identities.

"We have already launched a national SSI-based digital identity ecosystem which now involves more than 60 stakeholders from the private and public sectors (...) We are pleased to take the next step through our partnership with Spain to show the whole of Europe the potential of user-centric, decentralised identities“, emphasised Germany’s Minister of State Dorothee Bär.

This partnership to develop a cross-border digital identity based on the principles of self-sovereign identity will allow “citizens to verify their identity and access digital services in both countries.”

"Citizens should be able to have control over their data and their identity. The cooperation we are starting today with Germany on a self-sovereign digital identity is another step on the European path towards data sovereignty" said Carme Artigas, Secretary of State for Digitalisation and Artificial Intelligence in Spain.

Finland & The Netherlands also join the initiative

“More and more countries in Europe are embracing our vision for user-centric, decentralised identity. We are thrilled that after the announcement of our partnership with Spain in July, we are now taking the natural next step through our partnership with Finland to show all of Europe the potential of self-sovereign digital identity,” says Minister of State Dorothee Bär.

The European Self-Sovereign Identity Network

The European Commission announced the creation of EBSI, the European Blockchain Services Infrastructure, a joint initiative of the Commission and the European Blockchain Partnership (composed of 29 countries). EBSI's vision is to "leverage blockchain to the creation of cross-border services for public administrations and their ecosystems to verify information and make services trustworthy."

One of the main EBSI use-cases is ESSIF, the EU Self-Sovereign Identity Framework. Its goal is to implement a "Self-Sovereign Identity model in Europe, allowing users to create and control their own identity across borders."

Among others, the problems ESSIF wants to solve are data silos, lack of data control, privacy issues, lack of universality and interoperability.

“The identity management technology is largely there. Centralized and federated approaches have existed for years. Decentralized and self-sovereigns are rapidly evolving and will become mainstream soon. So the roadblocks are largely conceptual – it’s about understanding how your program or business fits into a larger ecosystem. Two decades ago, during the dot-com boom, everyone was setting up their own servers, now nobody does that – it’s a cloud now. Soon identity, or self-sovereign-identity will be available as a utility and controlled by the users.”

- Tim Bouma, Senior Policy Analyst for Identity Management at the Treasury Board Secretariat of the Government of Canada.

Turkey pilots Decentralized ID

The Turkish Ministry of Foreign Affairs, the United Nations Development Programme and Tykn piloted Decentralized Identity in Turkey. With more than 3 million refugees in the country, Turkey wants to use this technology to help increase refugee employability and financial independence.

In Turkey, entrepreneurs need to complete a Work Permit application in order to hire refugees. Currently, this process is lengthy and paper-based.

Using Decentralized Identity, Syrian Entrepreneurs were able to request a Verifiable Credential from the Istanbul Chamber of Commerce attesting that they own a registered business. They stored that Verifiable Credential in a digital identity mobile wallet on their phones and, without leaving the mobile wallet, the Entrepreneurs were able to start a Work Permit Application with the Ministry of Labour and use their Verifiable Credentials to prove their identity and that they own a registered business. Making the process digital, efficient and quick.

In this case Tykn used Decentralized Identity to:

- make the credentials issued by the Chamber of Commerce become digital, tamper-proof and verifiable anywhere, at any time.
- establish a secure and digital peer-to-peer connection between the Chamber of Commerce and the Entrepreneur. Not even Tykn can see what is exchanged between them.
- allow the Entrepreneur to prove their business ownership to the Ministry of Labour and request a work permit in 2 clicks.

Thailand moving towards Self-Sovereign ID

Thailand’s Electronic Transactions Development Agency (ETDA) is "currently working on legislation that would replace physical ID cards with the Digi-ID", says Dr Karndee Leopairote, Supervisory Board member of the ETDA.

Dr. Leopairote mentions that Thailand is moving towards a “self-sovereign” digital identity management system, where users can "manage and control" their own identity.

The country's National Digital ID platform, NDID, uses blockchain technology and "was initiated due to the government sector's emphasis on the application of digital technology to provide services to the people and business sector efficiently". It aims "to be the country’s infrastructural digitization that can help building new creative services and businesses in the digital economy".

The Dutch Self-Sovereign Identity Framework

The exchange of information between customers and service providers has been increasingly problematic. A common example in The Netherlands is found in the housing market. To be able to rent an apartment, a prospective tenant has to send numerous sensitive documents to a realtor/landlord. Documents such as ID, financial history, proof of employment or pay slips.

This poses several problems. On one hand, landlords need to manually review those documents and check their authenticity. On the other, the tenant is left without knowing where their documents might end up, who might see them and if they could be stolen and abused for nefarious purposes such as ID fraud.

The Dutch Blockchain Coalition, in collaboration with the Dutch Government, Banks and Universities and others in the private sector, is drafting the The Dutch Self-Sovereign Identity Framework. A set of guidelines for administrators, policy makers and developers.

The framework states that "power over data should only lie with the data subject (human, organization or even machine) himself. This can be achieved by providing every person and every organization with a new tool: a digital assistant, also called an agent or wallet in SSI. That digital assistant – for people probably in the form of a smartphone app – makes it easy for the end user and ensures responsible management of identifiers, keys and data at all times. The data subject retains insight and control over data."

Decentralized ID in Singapore

Singapore is trialing Self-Sovereign Identity as an extension of its National Digital Identity platform.

sgID is a privacy-based authentication system created by the government of Singapore to help citizens be in control of their data. sgID does not store any of its users' data. All data will be stored on the users' mobile devices.

The government claims that each person shares their physical ID with businesses and organisations at least once a month and that exposes citizens to ID fraud and other security risks.

GovInsider Asia reports that "sgID will show users what personal data organisations are requesting and allow them to share only the specific details the business requires. The app then encrypts the data and sends it to the business (...) The sgID app enables citizens to verify their identity without sharing their identity number. It creates a unique ID for every business citizens authenticate with, making it harder to trace what they do online. "

The European Union Announces EU-wide digital wallet

Although this announcement does not pertain to Decentralized ID, this denotes a trend towards the mass adoption of identity wallets which will inevitably impact the decentralized identity space.

“The European Digital Identity will be available to EU citizens, residents, and businesses who want to identify themselves or provide confirmation of certain personal information. It can be used for both online and offline public and private services across the EU.”

According to the EU, this digital identity will enable access to public services (such as requesting birth certificates, medical certificates, reporting a change of address), opening a bank account, filing tax returns, applying for a university (at home or in another Member State), storing a medical prescription that can be used anywhere in Europe, proving your age, renting a car using a digital driving license and checking in to a hotel.

One of its key principles is to give “full control to users to choose which aspects of their identity, data and certificates they share with third parties, and keep track of such sharing” (source). Common values shared with Decentralized Identity.

“Every time an App or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data in reality. That is why the Commission will propose a secure European e-identity. One that we trust and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data is used and how."

- Ursula von der Leyen, President of the European Commission, in her State of the Union address.

Cutting Red Tape by The Government of British Columbia

The government of British Columbia, Canada, is using an open-source blockchain framework, Hyperledger Indy, to streamline their services and cut red tape.

Canadian companies claim they waste more than 6 billion dollars (CAD) every year on unnecessary bureaucracy. This governmental project – The Verifiable Organizations Network – believes decentralized identities and trusted credentials are the solution.

Each Canadian business owner has to use three different tax numbers and navigate three different levels of governmental bureaucracy: local, provincial and federal.

Using Decentralized Identity, one trusted organisation within the value chain – such as the provincial government – can issue a digital Verifiable Credential to the business owner and the other organisations – such as the federal government or a financial institution – can verify that credential and trust the attestation made by the first organisation.

According to Product Lead John Jordan, their team wanted to show that this innovative technology can even be applied to more than just identity.

Use cases such as “professional associations that register members like doctors, nurses, or engineers; standards groups that certify food as organic or kosher; or businesses that need to prove their facilities have been inspected”. It can be used “to support private and secure P2P connections where verifiable credentials can be used to build trusted relationships. This can help streamline any process that involves trust.”

The Pan-Canadian Trust Framework

The Digital ID & Authentication Council of Canada (DIACC) has identified at least $15 billion (CAD) of potential benefits for the Canadian economy as a result of improvements in the digital identity infrastructure.

A “conservative estimate” considering $300 billion CAD worth of transactions are done on Canada’s payment network. That’s according to Joni Brennan, President of the DIACC, and whose career has been focused on Identity and Access Management innovation and digital identity standards development.

The problem is that “digital identity was not built for the digital economy”. It currently costs organisations $236 per user to solve password reset related issues. Users spend up to 600 hours recovering from identity theft and a company whose data is breached incurs in losses of 5.68 million dollars.

What the DIACC is working on is a framework of industry standards and practices to enable “interoperable networks that will have verifiable data requesters ask for particular attributes to be verified and attribute verifiers to provide that verification".

This interoperable framework – The Pan-Canadian Trust Framework – could enable citizens to start businesses and not deal with so much bureaucracy and have trustworthy transactions online.

As an example, one trusted organisation in the value chain (such as the Provincial Government) could issue a digital verifiable credential to the business owner, and the other organisation (such as the federal government or a financial institution) can verify that credential and trust the attestation made by the first organisation.

“Governments create data about us that we should be able to use in the economy and in the ecosystem. Just the same as banks and telcos also create and manage data about us. We need to have access to that data and we need to get it into an ecosystem that we can use securely, simply and with privacy by design (...) This is not only login. This is a new data strategy for Canada." said Joni Brennan.

In Banking & Human Resources

Seven Korean Banks went live with Decentralized ID with nine more banks to follow until the end of 2021. Users will undergo KYC with one of the banks and will be able to store that verified KYC data, as Verifiable Credentials, in a digital Wallet in their smartphones. Users can then re-use those credentials with the other banks that joined the initiative.

Since 2016...

...Rabobank, one of The Netherlands' biggest banks has been researching Self-Sovereign Identity. Rabobank believes that with their extensive "Know Your Customer" – KYC – and due diligence processes, they could provide "directly verifiable data" that the customer could provide to third parties or use verifiable credentials in order to onboard new customers.

Another use case that Rabobank believes can bring added value to customers is in regards to Mortgages. Mortgage flows require a lot of time and documents from several different sources. Most of those documents are not verifiable. Decentralized Identity would allow for the direct verification of that data and its source.

On the Human Resources side, Rabobank wants their employees to be in control of their own data. Reusing "certificates or assessments they achieved or did at Rabobank everywhere else. Therefore we do projects in order to save certificates, diplomas, trainings and employment credentials". They believe Decentralized Identity would "drastically improve employee onboarding times''.

From South Africa

For the past four years, the South African bank Absa has been working with BankServ, the country's Bankers Association, "to set up an industry-wide governance framework for self-sovereign identity".

Absa is excited by the potential of Self-Sovereign Identity as "it lowers the cost of opening accounts, which has the potential to make small business financing more accessible, deepen savings and credit for under-banked customers, and in future even reduce the harm caused by fraud and identity theft,”

They consider that financial institutions are in a prime position to build decentralized identity ecosystems because of the volume of personal data they handle.

Absa believes that this technology "provides a quick and highly secure way for people to store and update their own identity data on a personal mobile device, and share proof of it through a secure digital verification system, without having to share actual copies of their documents,”

Good Health Pass

The Good Health Pass 125 members include IBM, Mastercard, SITA and Tykn.

This initiative aims to create “an interoperable, trusted framework and ecosystem for the issuance, use, and management of COVID-19 test and vaccination credentials for international travel.”

The coalition is not building a digital health pass product but establishing principles and open standards for these digital health passes.

“Good Health Pass solutions must allow individuals to own and control their health and identity credentials. They must provide transparency over how user data is collected, used, and shared. Individuals must be able to determine where, when, with whom, and for what purposes their data is shared.” Solutions should be decentralized, built on open standards and interoperable across institutions and geographical borders.

The Digital Credentials Consortium

This Consortium is a university-led effort whose founding members are the MIT, Harvard University, Delft University, among 9 others. They are exploring the use of public key infrastructures, public ledgers, and blockchains to develop a learner-centric digital credentialing ecosystem.

This technology will streamline the issuance of academic credentials and transcripts to students and greatly reduce the risk of diploma fraud. The process will be digital, safe, and allow students to keep a verifiable record of their academic achievements. One that they could share with prospective employers, or others, any time, without the need to contact the University to attest for the authenticity of the credentials.

Kim Hamilton Duffy, Architect of the Digital Academic Credentialing Infrastructure at MIT, believes that "the learner side often gets deprioritized in existing credentialing systems, resulting in limited ability for learners to access, store, and use their credentials across systems (as an example, credential exchange protocols are still in early phases of development). This initiative is positioned (and committed) to drive these standards and requirements forward – and even develop reference implementations if the market is not providing them."

“72% of users want to know how their data is processed when they use social media accounts. 63% of EU citizens want a secure single digital ID for all online services."

- Eurobarometer Survey.

Humanitarian Cash-Based Aid

121 is an Initiative of the 510 Data Team of The Netherlands Red Cross. 121 believes a digital identity creation will speed up Cash Based Aid in the future, by allowing people affected to access aid digitally and safely.

Tykn led the development of the 121's Digital Identity Backend. Built on the principles of Decentralized Identity technology, it utilizes the W3C's Decentralized Identifiers (DIDs) standard and consequently offers an interoperable identity management system back-bone.

Known Traveler Digital Identity

Canada and The Netherlands are piloting ePassports based on decentralized digital identity. The KTDI initiative, led by the World Economic Forum, aims to enable paperless travel for transatlantic flights between Montreal and Amsterdam.

KTDI consortium partners will be able “to access verifiable claims of a traveller’s identity data so they can assess their credibility, optimise passenger processing and reduce risk”.

ePassport holders will be able to store Verifiable Credentials of their personal data. This data is encrypted and securely stored on the travelers’ mobile devices. Passengers will be in control of what data they share, with whom and when.

“This project offers a solution. By using interoperable digital identities, passengers benefit from a holistic system for secure and seamless travel. It will shape the future of aviation and security.” said Christoph Wolff, Head of Mobility, World Economic Forum.

The IATA Travel Pass

Because of the pandemic, this initiative believes that the key to give governments the confidence to open borders is to enable travelers to “share their [COVID] tests and vaccination results in a verifiable, safe and privacy-protecting manner”

The IATA Travel Pass is a mobile app, built on Decentralized Identity technology, that allows passengers “to store and manage their verified certifications for COVID-19 tests or vaccines”.

Amongst the airlines trialing this Travel Pass are Emirates, British Airways, Etihad, Air France and 50 others.

"Global Blockchain Identity Management Market to Reach $21.8 Billion by 2027."

- Research and Markets report.

Who is Tykn?

Tykn is an award-winning Dutch startup developing decentralized identity tools for impact. Our innovative technology allows organisations to issue cryptographically tamper-proof credentials which are verifiable anywhere, at any time. Users can prove their ID to access services while remaining in full control of what personal data is viewed, shared & stored. We envision a world where identities are portable, private and secure, so that no one has to lose access to their identity ever again.

Having raised €1.65MM in private funding Tykn has led the development of the digital identity backend of the 121 consortium, an initiative of The Netherlands Red Cross for Cash Based Aid, is abstracting away the complexities of Decentralized Identity through its API platform, and is also developing a project for the Turkish Ministry of Foreign Affairs and UNDP, aimed at improving the livelihood of Syrian refugees by enhancing their employment opportunities.

Our team is composed of subject-matter experts formerly holding positions at Thomson Reuters, the Dutch Ministry of Interior, Telefonica and many more, all driven by tech innovation for good. The efforts of this team have lead Tykn to being published in The Guardian, NOS, NRC, Thomson Reuters, EU-Startups and several other international publication, as well as winning multiple prizes and awards, including "The Netherlands Chivas Venture Award 2019" (Best Dutch Social Enterprise), whereafter Tykn placed Top 5 in the global competition among a 1000 startups; The Spindle Innovation Awards (powered by Partos and Accenture) and the MENAFIF Innovation Prize from the Asia Financial Institutions Forum.

tykn