Digital Identities

Jennifer Morales (C)
Contingent Worker


DRIVER LICENSE
NAME SURNAME
ID
NAME
SURNAME
1234 5678 9012 3456
01/19

What are Digital Identities? (also known as Digital IDs)

Put simply, digital identity is a person's online profile. Digital identity is derived from web-accessible personal data that can be traced and connected to a given individual.

From a technical point of view, a digital identity is an online or networked identity adopted or claimed in cyberspace by an individual, organization or electronic device. These users may also project more than one digital identity through multiple communities. (i.e. it is likely that your banking digital identity is different from your social media digital identity.) In terms of digital identity management, key areas of concern are security and privacy.

Like its human counterpart, a digital identity comprises characteristics, or data attributes, such as the following:

- Username and password
- Online search activities, like electronic transactions
- Date of birth
- Social security number
- Medical history
- Purchasing history or behavior

A digital identity is linked to one or more digital identifiers, like an email address, URL or domain name. Because identity theft is rampant on the Web, digital identity authentication and validation measures are critical to ensuring Web and network infrastructure security in the public and private sectors.

Good digital ID is identification that is verified and authenticated to a high degree of assurance over digital channels, unique, established with individual consent, protects user privacy and ensures control over personal data.

Digital Identities – How do they compare with traditional identities?

Unlike a paper-based ID such as most driver's licenses and passports, a digital ID can be authenticated remotely over digital channels. McKinsey adopted this outcome-based

definition of digital ID, regardless of the ID-issuing entity. For example, a digital ID could be issued by a national or local government, by a consortium of private or nonprofit organizations, or by an individual entity. This definition also applies regardless of the specific technology used to perform digital authentication, which could range from the use of biometric data to passwords, PINs, or smart devices and security tokens.

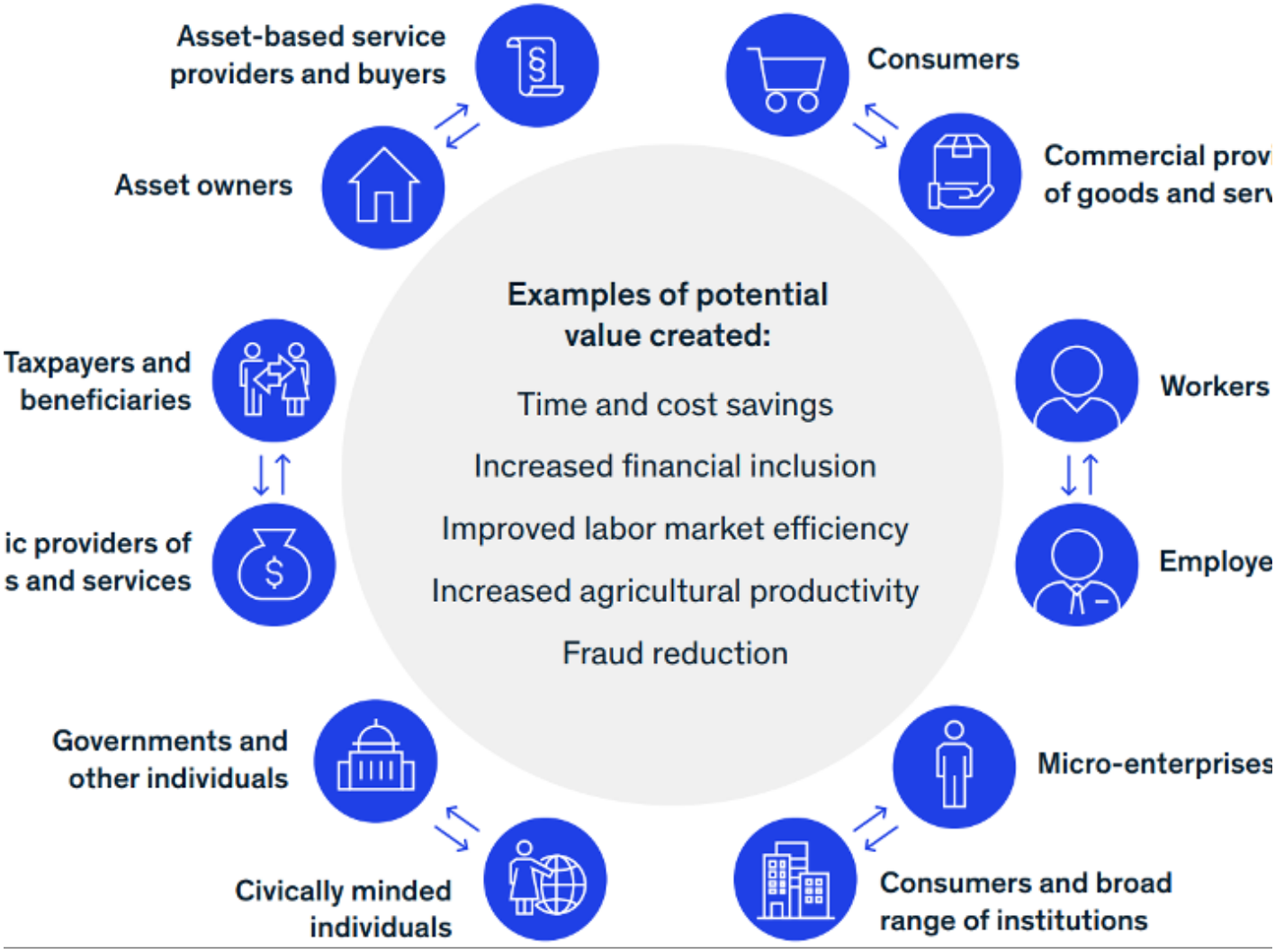
What are they good for?

Digital ID is a way of proving who we are and generating opportunities to carry out interactions in a simple and safe way in the digital world. Efficiency, cost reduction, fraud prevention and less bureaucracy are some of the benefits of using a secure digital identity.

Research by the McKinsey Global Institute finds that countries implementing good digital ID could unlock economic value equivalent to 3-6 percent of GDP on average by 2030, making digital ID a potential force for inclusive growth, especially in emerging economies.

According to McKinsey, Digital ID can unlock value by promoting inclusion, formalization and digitization.

- 45% of women aged 15+ in low-income countries lack ID while only 30% of men do.
- 1.7 billion people globally could gain access to financial services
- 90% of customer onboarding costs could potentially be reduced



Other Major Benefits of Digital Identities

In addition to the day-to-day facilities for users, a digital ID can also help create trust between the customer and the company while, at the same time, allowing companies to adapt the way they execute their processes. Knowing the customer is not only a security measure for organizations that helps to combat fraud, but it's also a way of orienting themselves to offer the best user experience and the best possible digital journey

How They Work

Different sources of digital identity create unique personas. An organizational identity is, for example, that of a business or government, or one of its employees. A personal

identity is that of a customer of a business, or a citizen of a country. An application or device identity is that of a mobile phone, computer or piece of industrial equipment.

A person's digital identity, and his or her interactivity with the world, will be multi-faceted and unique to each experience. For example, when an online banking service requires a password and other information from a customer and receives the correct information, the bank knows it is dealing with that customer and no-one else. The customer, meanwhile, knows it can trust that the bank's digital identity checks will prevent identity theft and the possible consequences associated with that.

Digital identity verification works by comparing a readily available proof of identity (e.g., a facial biometric or an ID document) to a confirmed data set (e.g., government-issued credential, such as a passport, or a biometric stored on a user's registered mobile phone). The purpose is to verify that a person is who they say they are.

A variety of identity verification methods help verify a person's identity, and each works in a distinct manner. Let's take a look at each of these methods:

1. ID Document Verification:
    a. Verifies the legitimacy of an ID document (such as a driver's license, passport, or government ID)
2. Biometric Verification:
    a. Selfies are used in biometric verification to ensure that the person presenting the ID is the same person whose portrait appears on the ID
3. Liveness Detection:
    a. Detects spoofing attacks such as face masks or doctored images to determine whether a selfie is genuine
4. Knowledge-Based Authentication (KBA):
    a. A type of authentication that relies on the user's knowledge, such as from the applicant's credit file to generate "out of wallet" questions
5. OTP (One-Time Passcode) Verification:
    a. During the verification procedure, the applicant receives a one-time passcode through SMS or email
6. Database Methods:
    a. Uses information from social media, offline databases, and other sources to verify the applicant's information

Digital Identity Use Cases

Due to the advanced methods used by fraudsters for nefarious actions, not a single industry is secure these days. Every industry needs digital identity verification checks, but the ones that require it the most are:

Online Gaming

Given the significant increase in e-gaming market revenue, this sector is more prone to criminal activities. Malicious users can be kept at bay with identity verification services. They can save gaming companies a lot of money by avoiding costly lawsuits and data theft.

Aside from the monetary considerations, safe identity verification is critical for fostering trust in the gaming community. Verified profiles not only aid in the identification of rogue actors, but they also enhance the overall online gaming experience.

Financial Services

Banks, crowdfunding platforms, insurance firms, and virtual payment systems are all working hard to make customer transactions as simple as possible. However, illegal activity has become a major issue.

Digital ID can alleviate systemic issues by reducing some of the barriers to participation in the digital economy for individuals with restricted access. To begin, a legally recognized, unique digital identity can be used in place of physical documents. You can leverage technology to meet regulatory goals such as validating proof of address using GPS. This process will enable an individual to meet the KYC standards for opening a transaction account, which will open up a world of financial possibilities.

Travel and Tourism

Fake travel agencies, fabricated identities used to escape, and a variety of other activities make it difficult for the travel industry to adhere to KYC standards. Fraudulent activities in the travel industry cost it almost $21 billion USD annually.

Face and other forms of identity verification can assist the travel sector in adhering to the rules while aiding in preventing fraudsters from fleeing with all of their activities.

Digital Identities Impacting Business

Huge growth in use of Digital IDs

According to a Juniper Research report, the use of digital IDs will increase by more than 50% over the next few years, from 4.2 billion in 2022 to 6.5 billion in 2026. In that way, accessing government services will likely be essential in this construction.

- The European Commission announced a proposal for a digital identity for all European citizens, allowing all official documents to be stored and managed through a digital wallet.
- E.g. is Estonia, a small European country of about 1.3 million inhabitants that has been using this system for many years. In the country, 99% of services can be accessed electronically: voting, opening a company and even issuing a birth certificate. Behind this is a digital ID ecosystem that connects people to these facilities. However, this technology not only makes the life of citizens easier; the country has managed to save 2% of its GDP by going digital.
- India implemented a national digital ID called the Aadhaar project. In addition to ensuring the reduction of costs and bureaucracy in the country, the digital ID also increased security by replacing physical documents—reducing fraud, inefficiencies and corruption. It became easier for citizens to hire private services, which attracted investment, increased competition, and led to better products and services at lower prices.
- In 2020, the Australian government announced that the development of its digital ID system would be the focus of its tech budget package of $800 million.

Impacts inside the business

Deloitte breaks down the internal impacts needed to implement Digital ID. They feel it should be at the heart of the effort to make the entire enterprise digital.

Startup Activity

Top Identity Management Startups – This is a hot market for startups. A quick survey of [Tech Crunch's Site]() for Identity Access Management yields this activity over the last 3 quarters for ConductorOne, Teleport, Silverfort, Spruce. Older startups, some with familiar names include Okta, Auth0, Ping, One Identity, OneLogin, ForgeRock, and Persona:

Jun 23, 2022 — ConductorOne is bringing automation to **identity** and **access management** with $15M investment ... The founders of ConductorOne, an **identity** and ...

- [ConductorOne is bringing automation to identity and access ...]()
- [https://techcrunch.com › 2022/06/23 › conductorone-is...]()

May 3, 2022 — Teleport, a **startup** developing a proxy-based

infrastructure **access** and **management** system, has raised $110 million in venture funding.

- Teleport nabs $110M to provide identity-based ... - TechCrunch
- https://techcrunch.com › 2022/05/03

Apr 12, 2022 — The company's platform is built both to work with existing **identity management** software providers, as well as provide a layer of security across ...

- Silverfort nabs $65M with a 'holistic' approach to protecting ID ...
- https://techcrunch.com › 2022/04/12 › silverfort-nabs-6...

Apr 20, 2022 — Web3 **startup** Spruce is developing "sign-in with Ethereum" to let users decide what they share with platforms.

- Decentralized identity startup Spruce wants to help users ...
- https://techcrunch.com › 2022/04/20 › decentralized-id...

Competitor Activity

Avalara

So far there are no obvious announcements of or references to what Avalara may be doing with regard to digital IDs.

Sovos

From their Website : Enforcing tax identity information reporting is a priority for governments to increase revenue and reduce the current $9B tax gap. Businesses must report employees' tax identification numbers (TINs) and names to government agencies to ensure that individuals and businesses are being reported in their database correctly and reconcile what's being reported on 1099 and annual income tax returns.

Thomson Reuters

From their website : Thomson Reuters CLEAR ID Confirm is the premium electronic identity verification solution infused with public records data. Customizable for your organization's needs, minimize the potential for fraud and meet regulatory requirements.

CLEAR ID Confirm can detect fraudulent identities quickly by incorporating risk flags –

such as passport MRZ verification, death records, redundant SSNs, OFAC listing, and other businesses linked to same FEIN - into searches. These flags provide an additional layer of protection against identity fraud and allow your organization to know when further investigative due diligence is necessary

CLEAR ID CONFIRM International : Access expanded identification verification for international and non-U.S. subjects, including identity confirmation within 35 countries. Know what information is incorrect while receiving scoring and transparent data sources information.

Conclusion

Key takeaways:

- Digital IDs are vital to successful digital habitation.
- Digital IDs are varied, proliferating quickly, and are not particularly interoperable making integration slow and prone to compromising security.
- The risks and defenses are evolving rapidly making it difficult but critical to stay ahead.
- The rewards lie in connecting everyone who wants to and agrees to be connected to information and the associated people, places, business and things.

Are Digital Identities Ready for Adoption?

Digital Identities are already being adopted so it's not a question of whether to adopt, it is a matter of joining in securely and setting the pace based on your skill in security and your budget.

Source articles for this page:

- Digital Identification Technology Promises Stronger Security
- *https://www.techopedia.com/definition/23915/digital-identity*
- Infographic: What is good digital ID?
- Digital identification: A key to inclusive growth
- The Future of Digital Identity
- The World of Digital Identity - Everything You Should Know
- Council Post: What Does The Future Of Digital ID Look Like?

- The Future of Digital Identity
- Tax Identity Management 101
- CLEAR ID Confirm | Electronic Identity Verification
- TechCrunch • Startup and Technology News