WHY DIGITAL IDENTITY IS CRITICAL TO POST-PANDEMIC SOCIETY

Whitepaper

1.1 Introduction

The concept of digital identity and how it can be applied has been discussed for many years. These often-philosophical discussions are beginning to crystallise into the 2020s. The concept of digital identity is less about presenting a digital persona and more about sharing verified identifiable data. However, this is not to say that a digital version of 'you' does not have a place in the wide-scale, multi-use ecosystems being built today. With the versatility inherent in many modern identity systems, life events and portable identities take on new meaning.

Digital identity is about much more than creating an online account. Data drives transactions and, more and more, we are seeing a requirement to add weight to justify the use of identifying data. Beyond registration for an identity account, verified data sees a place in post-registration or even non-registered (third-party) verifiable, assured, transactions.

As we carry on into an unknown future, disrupted by the pandemic, this interwoven nature of identity-security-privacy will play a vital part in making sure our internet, workplace, government services, and banking are safe havens.

Digital identity systems or 'ID Networks' are no longer an island; isolated from anything else going on around them. ID Networks are multi-faceted, multi-component ecosystems facilitated via APIs, open standards, and protocols. The players within the expanded ID Network ecosystem are focusing their efforts and fast becoming best-of-breed solutions; adding vital pieces to wider, whole, often extended, API-enabled ecosystems.

Security and privacy are an integral part of this. Digital identity is unique, in that it both needs security and privacy, and at the same time, when done well, enhances security and privacy. Issues like synthetic identities and other identity-based fraudulent activities have a chance of being tackled by modern robust options in ID that draw in those best-of-breed ID Network components.

This whitepaper will give an overview of the current trends in the digital identity space, as well as our definitions and our forecast outlook for digital identity app use.

1.2 Definitions & Scope

Juniper Research considers digital identity to be a digital representation of an entity; this can be one or more individual pieces of identifying data, an event, or a 'signal,' such as an assurance indicator and similar, yet to be determined, items defined by the industry. This latter statement is important, as ideas such as decentralised identities, IoT identities, robotic IDs, etc take shape. This data can be used as authorisation signals, grant rights, access or privilege, on the basis of that representation.

1.2.1 Identity Tasks

ID Networks, even decentralised IDs, may be reliant on multiple components, each doing a job within the larger engine of identity. Which of the myriad requirements are applied, and at what point in a user journey, depends on the use case and remit of the ID system. Wider adoption of ID networks requires omnichannel support, facilitated by the re-use of ID verification and authentication to add assurance to transactions. The result

is a rich ecosystem of contributing components. Typical tasks in an ID Network include:

- Authentication – A proof of an assertion (ie identity data). This is typically done through credentials such as usernames, passwords, PINs or biometrics, single or multiple factors in that authentication process. In addition, rules-based/risk-based authentication has a place in making ID-enabled transactions more granular.
- Authorisation – Association and assertion of rights with a given identity/role/transaction. This is typically done through assigning roles, independent of a given end user. But this can be done at a transaction or device level.
- Verification – Check of an identity or piece of identity data (eg an identity document such as a passport).
- Anti-fraud – Increasingly, anti-fraud checks are being used during registration or transactions that have an identity element.
- Attribute Enrichment – If required, additional attributes can be requested from external or internal sources. These may require further verification.
- Rules of Engagement – A rule applied to an identity event (eg under condition X, user Y can perform action Z).

1.2.2 Forms of Digital Identity

Juniper Research classifies digital identity under three categories:

- Centralised – Digital identity credentials are held in a single place, and each credential is used for a single purpose.
- Federated – Digital identity credentials are held in a single place, and applied to multiple contexts; allowing a single set of credentials to act for multiple systems.
- Decentralised – Digital identity credentials are typically created and managed directly by the credential owner, and stored in a decentralised manner, eg on a mobile device. This has broadened in meaning from SSI (Self-Sovereign Identity) to encompass multiple different types of credential frameworks.

Note: All three categories can be used within a wider ID network.

1.3 Why Digital Identity Is Critical to Post-pandemic Society

Thanks to the lockdowns introduced to contain COVID-19, companies all over the world have been forced to turn to home working to stay productive. This has created challenges for enterprise IT teams, particularly in the area of cybersecurity. Cybercriminals have taken advantage of vulnerabilities in highly complex networks where Shadow IT is common, which has been stretched further by working from home. Shadow IT is where systems are deployed by departments other than the central IT department. This is combined with the now massive variety of devices and networks that users are working on, driven by an explosion in remote working. The advent of the malicious ‘remote insider’ only adds complexity to the needs of traditional enterprise IAM (Identity & Access Management) systems.

Providing robust and effective access control in an environment that is outside the direct control of the enterprise requires a change in approach.

The August 2020 NIST Special Publication 800-207 update on implementing a ZTA (Zero Trust Architecture), defines a process to create an effective ZTA with an emphasis on monitoring, NIST states that:

'When balanced with existing cybersecurity policies and guidance, identity and access management, continuous monitoring, and best practices, a ZTA can protect against common threats and improve an organisation's security posture by using a managed risk approach.'

The situation surrounding online consumer accounts has reached a tipping point. It is becoming extremely difficult to manage the credentials, usually, a password, required to access the many accounts users hold. Coupled with this, many people reuse credentials to avoid remembering multiple passwords. The result has been an onslaught of credential stuffing attacks, fraudsters using stolen credentials to hack into online accounts. In the year to December 2019, there were 88 billion such attacks recorded.

This issue is not just a consumer problem. The phenomenon of work from home, coupled with Shadow IT and BYOD (Bring Your Own Device), means that the issue of credential stuffing could potentially leak over into enterprise access: users re-using cloud login credentials for personal accounts for convenience.

Federated identity provision, seen in its simplest form, provides the reuse of social provider login federation, as well as in enterprise SaaS (Software-as-a-Service) provision. This is a useful device for improving usability. SSO (Single Sign On) is sometimes associated with federated login for even easier resource access. Tokenisation is used via standard identity protocols, SAML (Security Assertion Markup Language), OIDC (OpenID Connect) and OAuth (Open Authorisation).

Federation of identity, or 'identity reuse' can provide a mechanism to reduce the burden of credential management and recall. However, federation has some implicit problems, namely which existing identity providers to support. The use of standard protocols such as OIDC allows easier onboarding of federated ID support. However, some existing ID systems, such as decentralised wallets (see later) may use proprietary standards. The W3C project, 'Decentralised Identifiers (DIDs) v1.0' is updating this situation by developing the DID standard so that:

'DID methods can also be developed for identifiers registered in federated or centralised identity management systems. Indeed, almost all types of identifier systems can add support for DIDs. This creates an interoperability bridge between the worlds of centralised, federated, and decentralised identifiers.'

The development of 'hubs' or an orchestration layer, to handle protocol translation, onboarding and offboarding of relying parties and services, as well as federated identity providers (IDPs), offers a more versatile and manageable way to create federated identity networks.

However, federation in and of itself is not the answer to securing access. The whole system requires other components to verify and check access events. For example, verification of additional attributes may be required. Other checks such as machine-learning based UEBA (User and Entity Behavioural Analytics) and AML checks can also be used to augment identity networks that utilise federation.

1.4 Market Trends Affecting Digital Identity

This section will outline two further trends which are shaping the future of digital identity.

1.4.1 Governments Leading?

A wide variety of countries have tried, failed, or are planning to bring, digital identity to citizens. The move to a digital government is largely dependent on a mechanism of identifying yourself in an assured manner. The government also has control over a number of identity documents, such as passports. This should be simple, but is often more complex.

Online government services are often the main touchpoint for consumers wishing to connect to local and national governments. These services can be crucial in delivering benefits and tax options. The level of assurance required to transact online with government services is a key requirement of these systems.

In the UK, this same requirement became an obstacle for the smooth running of digital government identity. The UK Verify service was a vanguard service that shaped the ideology of digital government. The identities were provisioned by a number of UK brands, including the Post Office, Royal Mail, Experian, and Barclays Bank. The system was based on a SAML 2.0 'hub,' in this case acting as a conduit to the citizen; allowing them to pick a brand to provision their government ID. The level of assurance started off as low (LOA1); allowing a small number of these brands to quickly on board for the scheme. A second procurement was put out to market but these new IDPs were required to start at an increased level (LOA2), eventually, retro fitting to an LOA1, as the project progressed. Issues with match rates plagued the project, as to achieve an LOA2, users had to be taken through fairly onerous steps to prove their identity; providing identity documents and being asked identifying questions from a number of Credit File Agencies and aggregators at the backend of each IDP. Match rates were low, typically below 50%. Most IDPs left the scheme due to government funding issues; leaving only the Post Office and Digidentity to run the IDPs (note: The Post Office IDP technology is provided by Digitdentity). Match rates for 2020 are around 45% of users successfully being issued an identity. Of the expected 25 million UK citizen signups, by February 2019, only 3.6 million people had successfully signed up for Verify.

A number of different approaches to digital identity for G2C (Government-to-Citizen) transactions are shaking out. Australia has launched the MyGovID which is a smartphone-based ID that is based on a granular point system (you can gather up to 100 points to prove your identity). Card or wallet-based IDs remain popular in a number of countries in the EU, including Estonia, who are innovators in the space. The Canadian government is active and innovative in the digital identity space. DIACC (Digital ID & Authentication Council of Canada), headed up by Joni Brenan, ex Kantara Initiative, is working toward an interoperable relationship between the public and private sector to build a Canadian digital identification and authentication framework.

Figure 1: Specimen Estonian eID Card

Source: Republic of Estonia Police & Border Guard Board

The US continues to battle with citizen acceptance of a federal identity scheme. This will play out in the coming years.

Citizen identity has the potential to bridge the gap to consumer identity. Schemes around borders and airports such as WorldReach's 'Know Your Traveller' app has allowed the successful processing of more than 4 million applications to the UK Home Office EUSS (EU Settlement Scheme).

Government use cases continue to drive certain aspects of the identity market and test the waters around high assurance IDs and consumer usability.

1.4.2 The Evolution of Identity Wallets

An ID in a user's pocket is a compelling idea. The use of smartphones to carry out day-to-day life activities has proven highly successful. We use our smartphones for music, contacts, notes, emails, banking, messages, so why not identity? The market for mobile ID/identity wallets has evolved over recent years to bring a number of solutions to the market.

Identity wallets are a form of decentralised identity. Some are based on proprietary protocols, some on standards. Some identity wallets are based on SS architecture and are therefore built on a backbone of a blockchain. Some are centralised but with the ethos of user-controlled decentralised actions using a mobile wallet. Evernym's decentralised wallet, Connect.me, uses the Sovrin blockchain. Connect.me manages all of an individual's verified (and non-verified) identity data from a mobile device. Connect.me supports the privacy-enhanced sharing of these data via a zero-knowledge proof methodology (ZKP). Another mobile solution is CULedger's MyCUID, which creates a KYC checked, decentralised digital credential based on Evernym's Sovrin decentralised ledger.

The digitalisation of ID documents is growing at fast pace, especially with the introduction of new ID wallets which can be point solutions, such as a mobile driver licences, or which can aggregate various documents (digital identity, driver licence, health care credentials, etc) in a single app.

Others such as Infobip, use mobile ID as a way to improve the user experience of using a digital identity. The Infobip solution verifies a user's phone number and, in doing, so protects customers against SIM Swap attacks. This is done in an unobtrusive manner – a key requisite of ID solutions, with friction often being a barrier to uptake.

The verified attributes that a digital wallet can present on request are those same attributes that other digital identity systems present. The party requesting the identity check then must decide if the details required are sufficient to authorise the transaction.

1.5 Digital Identity: Movers & Shakers

Eve Maler

ForgeRock

CTO

Eve has had a varied career to date. As a former linguist, it was perhaps a natural home to move into the area of standards and protocols. Eve has co-invented XML and SAML, and over the last ten years or so, she has worked diligently with her team at Kantara Initiative on the User-Managed Access protocol UMA.

Eve has held positions at Sun Microsystems, PayPal, and, more recently, as a Senior Analyst at Forrester Research. Eve joined ForgeRock in 2014 to become their VP of Innovation and Emerging Technology. In 2020, she was made interim, then permanent, Chief Technology Officer.

Emma Lindley

Truststamp

Chief Commercial Officer

Emma Lindley is Chief Commercial Officer for Truststamp, a provider of revolutionary privacy protecting technology for biometrics, she is also co-founder of Women in Identity, a not-for-profit organisation focused on developing talent and diversity in the identity industry.

Emma previously held positions at GB Group and has worked in the identity industry for 17 years. She has an MBA from Manchester Business School and completed her thesis in Competitive Strategy in the Identity Market.

Joni Brennan

President

DIACC (Digital ID & Authentication Council of Canada)

As President of the DIACC (Digital ID & Authentication Council of Canada), Joni builds on 15 plus years of experience in digital identity innovations and standards development. Previously, Joni headed up the Kantara Initiative.

Joni has extensive experience in the standards space and is viewed as a key member of the identity industry. She has participated in committees and initiatives around the world including OECD-ITAC, ISOC, IEEE, OASIS-SSTC, ISO SC27 WG5, and she has testified before the US ONC HITSP (Office of the National Coordinator for Health Information Technology Security and Privacy).

Kim Hamilton Duffy

Co-Chair W3C Credentials Community Group and Architect of the Digital Academic Credentialing Infrastructure at MIT (Digital Academic Credentials Initiative).

Until recently, Kim was previously the CTO & Principal Architect at Learning Machine.

Kim is the co-chair of the W3C Credentials Community Group. The mission of the W3C Credentials Community Group is to explore the creation, storage, presentation, verification, and user control of credentials. It focuses on a verifiable credential (a set of claims) created by an issuer about a subject—a person, group, or thing—and seeks solutions inclusive of approaches such as: self-sovereign identity; presentation of proofs by the bearer; data minimisation; and centralised, federated, and decentralised registry and identity systems.

Kim also works at MIT and in W3C to help forge the way for usable, interoperable SSI. Kim is also an active proponent of women working in the software development space.

Alvina Antar:

Okta

CIO

Alvina was the former CIO of subscription management company Zuora and also spent time at Dell. She joined Okta as CIO in September 2020.

Alvina has over 20 years' experience at high-performing IT organisations at both Fortune 50 companies and high-growth startups. Alvina is a Speaker at Executive Briefing Center and Technology Conferences promoting M&A integration strategy and transformational solutions driving business evolution from hardware company to end-to-end solutions provider.

Cheryl Stevens OBE:

DWP Digital Group

Director for Shared Channels Experience

As a career civil servant in the UK, Cheryl has held a variety of leadership posts; gaining operational insight, spearheading transformational change and developing an in-depth knowledge of customers. She has recently been promoted to the position of Director for Shared Channels Experience at DWP Digital Group. In this role, she has had to deal with the massive challenge of manging government benefits during the COVID-19 pandemic.

Cheryl holds the vision of all citizens being able to access digital services, with those services able to operate securely with proportionate, tailored Identity and Trust solutions that meet both customer and service needs, whilst ensuring that the person, the data and the transaction are protected. Cheryl is passionate about lifting other women in digital and identity.

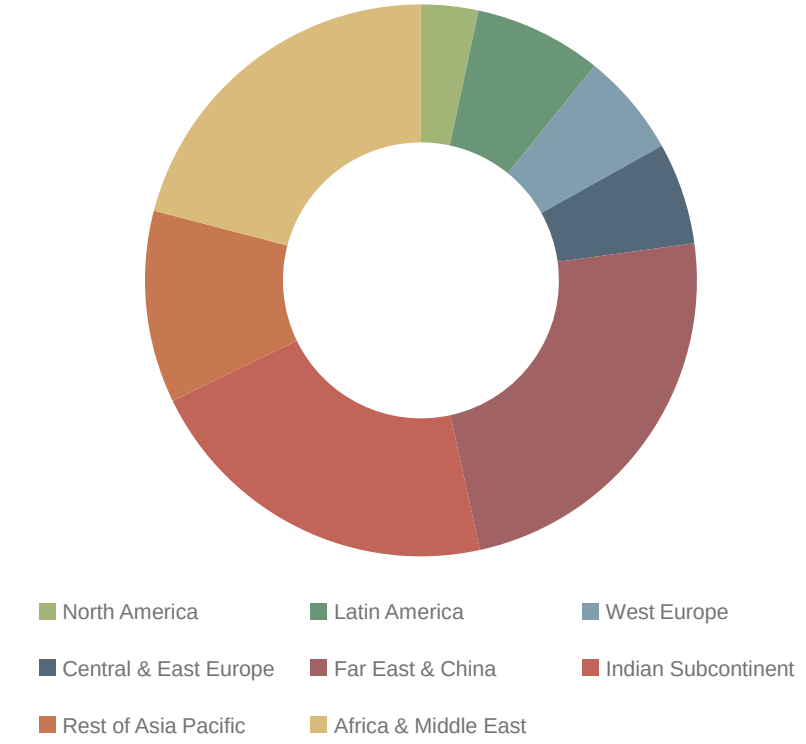
1.6 Forecast Summary

The number of digital identity apps in use will exceed 6.2 billion in 2025, from just over 1 billion in 2020. Civic identity apps, where government-issued identities are held in an app, will account for almost 90% of digital identity apps installed globally in 2025; driven by the increasing use of civic identity in emerging markets and the lasting impact of the pandemic.

The unprecedented shift to digital services during the pandemic across the world will stimulate rapid growth in civic identity; growing by 467% between 2020 & 2025, as robust onboarding and verification for digital services becomes vital.

- Civic identity apps will overtake the number of digital identity cards in use in 2023, with the number of apps in use 41% higher than cards by 2025. While digital identity cards are still growing, apps are much easier to scale and better support increased involvement in digital commerce, which will be critical to digital identity's future use.
- Blockchain will be important to the future of digital identity, with blockchain-based third-party digital identity apps accounting for 16% of all installed third-party identity apps in 2025. However, this is not necessarily the much-lauded self-sovereign model, where numerous parties such as banks, identity providers and mobile network operators work together to provide identity as part of a wider network. Blockchain will be an effective way to secure federated access to data; injecting trust and transparency.

Figure 2: Number of Digital Identity Apps Installed (m), Split by 8 Key Regions: 6.2 Billion, 2025



Source: Juniper Research

Order the Full Research

Digital Identity's new research features a massively expanded forecast; delivering an exhaustive guide to this rapidly changing and highly complex landscape. Discover valuable insights into vendors' digital identity strategy and a fine-grained analysis of the current competitive landscape; supported by interviews with key vendors in the field.

Key Features

- **Digital Identity Trends Analysis:** Detailed analysis of each digital identity segment, plus insights on market trends, challenges and our future outlook for the market.
- **Regulatory Analysis**: In-depth discussion on how legislation and cultural factors are impacting digital identity solution deployment across over 20 country markets.
- **Juniper Research Leaderboard**: 14 leading digital identity vendors compared, scored and positioned on the Juniper Research Leaderboard, including Experian, Okta and WorldReach.
- **Interviews:** 9 leading digital identity stakeholders interviewed, including Mitek, Okta and Thales.
- **Benchmark Industry Forecasts**: Market forecasts covering digital identity prospects across a number of areas including:
    - Digital Identity User Base
    - Digital Identity Civic App User Base
    - Mobile Biometrics User Base.

What's in this Research?

1. **Deep Dive Strategy & Competition** – Strategic analysis of market dynamics and opportunities, together with a detailed investigation of the regulatory frameworks in numerous countries, as well as player analysis through the Juniper Research Leaderboard (PDF).
2. **Deep Dive Data & Forecasting** – Future digital identity prospects analysis, together with 5-year forecasts for key metrics, including civic identity apps and digital identity cards (PDF).
3. **Interactive Forecast Excel** – Highly granular dataset comprising nearly 8,000 datapoints, allied to an Interactive Scenario tool giving users the ability to manipulate Juniper Research's data (Interactive XL).
4. **harvest Online Data Platform:** 12 months' access to all of the data in our online data platform, including continuous data updates and exportable charts, tables and graphs (online).

Download a summary of the table of contents and forecasts above, or request a detailed list of every table and chart via info@juniperresearch.com.

Publication Details

Publication date: October 2020

Author: Nick Maynard and Susan Morrow

Contact: For more information contact info@juniperresearch.com

Juniper Research Ltd, 9 Cedarwood, Chineham Park, Basingstoke, Hampshire, RG24 8WD UK

Tel: UK: +44 (0)1256 830002/475656 USA: +1 408 716 5483 (International answering service)

http://www.juniperresearch.com