Global Insights

Digital ID

Verification is the Name of the Game

29 Mar 2023 11:43:53 ET

Executive Summary

Anuj Gangahar
anuj.gangahar@citi.com

Wenyan Fei
wenyan.fei@citi.com

Robert Garlick
robert.j.garlick@citi.com

With thanks to

Carol Gibson

Questions of identity lie at the heart of almost every interaction in our increasingly digitized lives. Proving that the person or company you're dealing with is who they say they are is difficult. And fraudsters are alive to the opportunities that identity authentication and verification provide. Making digital identity easier and more secure is an important key to unlocking the full potential of digital societies and economies for citizens and corporates alike. The march to digitization following the pandemic, coupled with the imperatives of supply chain efficiency and financial inclusion, mean an increased use of digital ID looks inevitable. The question now is what form will it take, and who will control it - citizens, governments, or the private sector?

Contents

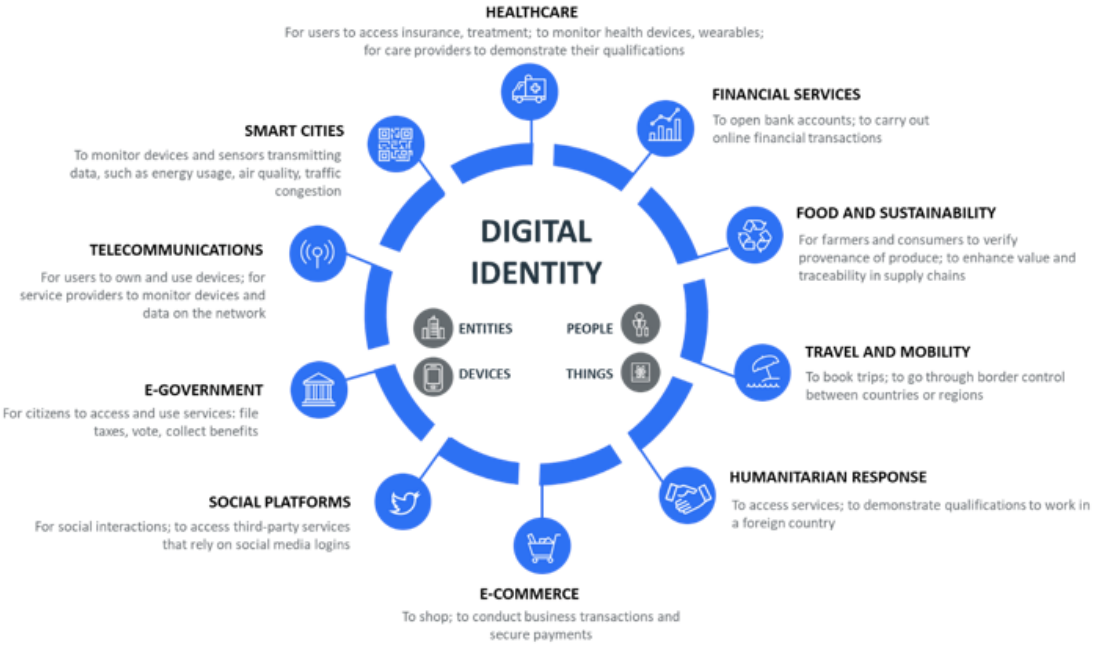
Digital ID: Who Are You? Who am I?

Questions of identity. They lie at the heart of almost every interaction in the digital age. Is the person or company you're dealing with really who or what they say they are? How can they prove it? How can you trust them?

These are fundamental questions of our time. And they're difficult but vital to answer.

It's not an overstatement to say that getting a handle on the answers to these questions - making digital identity and verification easier and more secure - is the key to unlocking the full potential of digital societies and economies.

Figure 1. The Centrality of Digital Identity



Source: World Economic Forum

Digital identity has the potential to create economic value equivalent to 6% of GDP in emerging economies and 3% in mature economies, according to McKinsey.[1] There's a huge opportunity to reach those who currently have no digital ID. The World Bank[2] says around 1 billion people worldwide have no form of identity at all, 3.4 billion have paper-based identities but limited access to digital services, and 3.2 billion have digital identity granting access to the digital economy but with differing levels of effectiveness.

Think about a world with no passwords. A world where you can automatically access and present relevant digital credentials from your digital wallet according to who's asking for them and what exactly they need. A world where you can access

[1] https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

[2]https://documents1.worldbank.org/curated/en/099437402012317995/pdf/IDU00fd54093061a70475b0a3b50dd7e6cdfe147.pdf

and use those credentials for any transaction or interaction you like as easily as pulling a bank card from a real wallet.

Imagine the impact that level of efficiency could have on your interactions with government departments, with the private sector, with your bank, with anyone you're transacting with.

You might not need to imagine much longer. Progress is being made on several fronts. And it's happening fast.

For the purposes of this report, we'll check in on developments in a few aspects of the global efforts around digital identity. This report follows our previous report, Digital Identity - Unlocking the Future, published last year.

We'll look first at governments, and the progress of existing and nascent digital identity schemes for citizens. Government still sets the tone for discussion of identity, so progress here has important implications not just for the relationship between citizens and the state, but also for corporates.

Then we'll look at exactly how the private sector is stepping up, and how it's playing a part in an area historically controlled by government. Increasingly, companies are concluding that digital identity can be a commercial imperative. They could save billions of dollars per year by streamlining their onboarding process or doing away with the need for old educational certificates and proof of address for example. Now at the click of a button, or the scan of a face, you can, in theory, verify that the someone claiming to be someone in the virtual world, is indeed that person in the actual world.

And lastly in this report we'll look at how AI might make an impact on digital ID and the relatively new concept of 'zero trust' approach to identity. This could, we think, pave the way for rapid advances in secure digital identity.

At the end of the report, we'll hear from several experts involved in the field of digital identity who through their insights and different perspectives will hopefully provide a rounded view of latest thinking. This section includes thoughts from an interview with Lord Hague, former U.K. foreign secretary and leader of the Conservative party.

It's worth saying up front that digital ID has immense power to drive change.

It could make financial services available to the world's unbanked - around 1.7 billion people according to WEF[3]. And it could save billions of hours standing in queues. Digital identity is at the heart of efforts to combat cybercrime, particularly identity threats. Indeed many of the corporates that provide digital identity solutions purport to combat precisely that problem.

The cybercrime problem is a huge one. Lexis Nexis Risk Solutions published its Global State of Fraud and Identity Report[4] in June last year. Based on a survey of 2,952 risk and fraud professionals, the survey found that businesses globally experienced a 38% increase in malicious bot attacks in the 12 months preceding publication of the report.

---

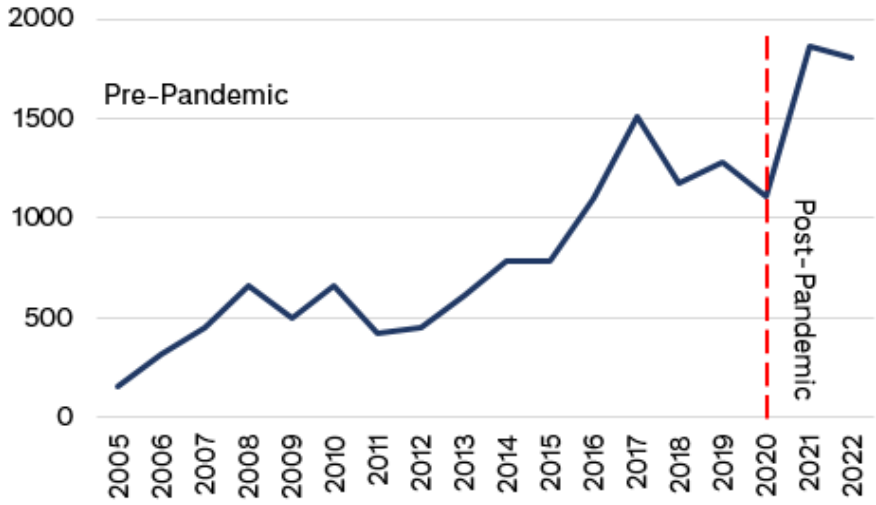
[3] https://www.weforum.org/agenda/2023/01/3-ways-global-access-financial-services-davos2023/

[4] https://risk.lexisnexis.com/about-us/press-room/press-release/20221205-global-state-of-fraud-and-identity-report-reveals

It also found that human initiated attacks grew 32% YoY globally. North America showed the highest YoY increase of 52%, followed by EMEA (19%).

The volume of cyberattacks has soared as the pace of digitization has accelerated following the pandemic. The chart below shows that the annual number of data compromises in the US jumped from 1,108 in 2020 to 1,862 in 2021, a nearly 70% increase. Globally, malware attacks rose by 125% in the first half of 2021[5], following a 358% increase in 2020[6].

Figure 2. Annual Number of Data Compromises in the US



Source: Statista

According to a report published by Liminal Strategy Partners[7], the reusable identity market size is expected to grow from USD 32.8 billion in 2022 to USD 266.5 billion by 2027, at a CAGR of 68.9%. As the market continues to focus on consumer identity, reusable identity will evolve as the natural next step to allow people and enterprises alike to create identity credentials that can be integrated across different use cases.

To facilitate reusable identities, Liminal said the current paradigm needs to shift to one that supports interoperable networks, public-private partnerships, and fully fledged ecosystems – with supporting standards, policies, and trust frameworks – that provide consumers with data mobility.

Initially, government-led initiatives will dominate the market, with a shift towards private-led reusable identities and growth across commercially-focused verticals. By next year, Liminal projects rising demand for public-private partnerships to support cross-border commerce and intergovernmental networks.

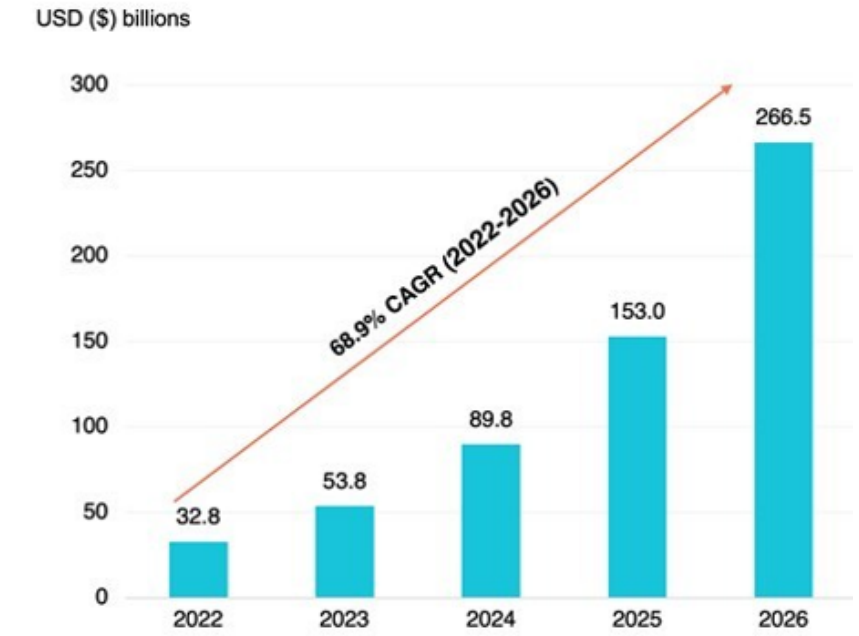
---

[5] Triple digit increase in cyberattacks: What next?

[6] Malware increased by 358% in 2020

[7] https://liminal.co/

Figure 3. Reusable Identity TAM (2022 - 2026)



Source: Liminal Strategy Partners

We think some of the factors driving digital identity can be broadly summed up as follows:

- Individuals are seeking ways to streamline their online presence and make it harder for fraudsters to take advantage of their fragmented digital identities.
- Companies are grappling with how to make their corporate digital identities interoperable across all the jurisdictions they operate in, across multiple geographies and regulatory frameworks, and across the entirety of their supply chains. And they're looking at the possibilities around KYC (know-your-customer), where digital identity holds potentially huge power to streamline fundamental tasks every organisation has to complete, like onboarding and background checks.
- Governments are trying to figure out how they play their part and whether national identity schemes are workable for them. Several ID schemes are already up and running across the world and more are set to follow.

National Digital ID Schemes: One Size Doesn't Fit All

Digital ID hit the headlines recently when former U.K. Prime Minister Tony Blair and former foreign secretary William Hague joined forces - not something the long-standing political opponents are accustomed to doing - on a report [8] highlighting the need for the UK to radically rethink its approach to technology. The call comes, they said, because we are "living through a 21st century technology revolution as huge in its implications as the 19th century Industrial Revolution."

The report, published by the Tony Blair Institute for Global Change[9],calls for a fundamental reshaping of the state around technology. "This is not about traditional left and right debates. It should lead to a more strategic state with an entirely new operating model," they wrote.

As part of that, they advocate for reorganising the centre of Whitehall to drive the use of data and AI across government, including digital ID for every citizen, alongside a national health infrastructure that uses data to improve care and keep costs down, and sovereign AI systems backed by supercomputing capabilities.

The debate over digital IDs has raged in the UK for decades. The Blair Institute report argues that in a world in which everything from vaccine status to air tickets and banking details are available on our personal devices, it is illogical that the same is not true of individual public records.

The report also points out that governments are the original issuers and source of truth for most identity documents, from birth certificates to passports.

"A well-designed, decentralised digital-ID system would allow citizens to prove not only who they are, but also their right to live and work in the UK, their age, and ownership of a driving license. It could also accommodate credentials issued by other authorities, such as educational or vocational qualifications."

The potential advantages it says are as follows:

- Cheaper, easier, more secure access to a range of goods and services, online and in person.
- Allowing government to understand user needs and preferences better, improving the design of public services.
- Easier access to benefits, reducing the number of people who are missing out on support they are entitled to.
- Help the government move to a more proactive model, meeting people's needs, tailoring services and reducing administrative burdens on both individuals and the public sector.

To date, the UK has made only tentative steps towards sharing data among public-sector organisations, either for policy-making purposes or delivering services.

---

[8] https://institute.global/policy/new-national-purpose-innovation-can-power-future-britain

[9] https://institute.global/policy/new-national-purpose-innovation-can-power-future-britain

Meanwhile, members of the European Parliament's (MEPs) Industry, Research and Energy Committee[10] have given their support to a new digital identity framework known as eID.

The framework would create an interoperable, EU-wide scheme, allowing all European citizens to use the all-in-one gateway to access public services.

Users will be able to identify and authenticate themselves online via a European digital identity wallet without having to go through commercial providers.

The idea is that the digital wallet will become a reliable, all-in-one identity gateway that puts citizens in full control of their own data and gives them the freedom to decide exactly what information to share, with whom, and when.

Further demonstrating how various governments and agencies are waking up to the need to address digital identity, The OECD's[11] Public Governance Committee and its Working Party of Senior Digital Government Officials have developed a series of recommendations on implementing and governing digital ID at the national and international levels.

Elsewhere, digital identity schemes are rapidly gaining popularity across the world. South Africa has a smart ID card. The United Arab Emirates recently rolled out a mobile-based national digital identity app, bundled with access to government services across the seven emirates under one unified registration and authentication process, allowing greater ease of movement across the region.

Meanwhile, Ministers from Australia's federal government have agreed to a deal with their state and territory counterparts to include digital credentials in the new national digital identity system, reports the Australian Financial Review[12].

The agreement paves the way for driver's licenses and occupational credentials to be recognized across the country and allows storage of credentials in a digital wallet[13], all based on international standards.

The new digital identity scheme is expected to make it easier for businesses to verify customer identities without collecting excess personal information.

It has been reported in the US that the federal government's Login.gov[14] digital identity service could be expanded nationally, according to the terms of a draft executive order.

Under this scheme, agencies that offer "high impact" services – such as tax schemes, passport renewal, Medicare, and the census, which are used by millions of Americans each year – would need to include Login.gov it as a sign-on and identity verification option.

---

[10] https://www.europarl.europa.eu/meps/en/home

[11] https://www.oecd.org/governance/eleaders/

[12] https://www.afr.com/politics/federal/new-identity-system-paves-way-for-national-sharing-of-drivers-licences-20230224-p5cn9t

[13] https://www.biometricupdate.com/tag/digital-wallet

[14] https://login.gov/

And India's Aadhaar[15] is the world's largest biometric digital ID system. Registration is linked to biometrics and demographics and can connect to SIM cards, bank accounts, and government aid, making financial systems more inclusive.

That said, some media reports have featured criticism of Aadhaar over privacy and data breaches.

For governments, digital identity can be a political hot potato, and some countries couldn't even begin to try to push them through, as citizens wouldn't stand for it. In any case, digital identity adoption is unlikely to throw up a eureka moment where everyone suddenly has an interoperable digital ID.

But over time, systems and structures will become more streamlined and efficient and in theory at least, we think, a force for good driving progress in our societies.

[15] https://uidai.gov.in/en/

Corporate Digital Identity: Efficiency to the Fore

For corporates, digital identity covers a few different things. One of these is that it can refer to electronic verification of the identity of a company or legal entity.

In supply chains, digital ID is increasingly important at every point of global trade to document, track, and monitor trade flows effectively and efficiently.

Another big thing for companies, looking more inwards, and particularly at the IoT proliferates, is machine identity. This is a big identity challenge because the average number of machine identities used by the organizations is set to continue to rise.

In both cases, getting a handle on digital identity can lead to significant efficiency and cost savings.

The table below shows the potential benefit of digital ID to corporates, including revenue generation enhancement, fraud reduction, and efficient digital authentication.

Figure 4. Savings and Revenues in Identification Systems for Private Sector

Feature	Description	Key Benefits
Digitization	transition from paper to digital-based systems, including of databases, credentials, data transfer, etc.	• *Direct:* reduces operating and transaction costs • *Indirect*: enables unique ID, integration, digital authentication
Unique ID	creation of a unique identifier –often biometric-based–for each member of the target population	• *Direct:* increases transaction efficiency; reduces fraud opportunities • *Indirect*: enables integration and queriability
Integration and Interoperability	connections between different identification systems, including their ability to exchange information	• *Direct:* increases transaction efficiency; facilitates queriability; reduces fraud opportunities • *Indirect*: incentivizes system adoption by incorporating a wider array of services into a given identity platform; encourages positive network effects
Queriability for Verification and Authentication	the ability of private sector companies to efficiently, securely, and consistently query and identification system for information	• *Direct:* increases transaction efficiency; facilitates effective private sector verification and authentication • *Indirect:* reduces private data liability costs; mitigates fraud opportunities; incentivizes value added services; encourages positive network effects
Public-Private Cooperation and Partnerships	the extent to which private sector companies are directly involved in the architecture and continued execution of identification systems	• *Direct:* enables private sector revenue generation for identity services

Source: World Bank

For SMEs, access to financial services can be enhanced by corporate digital ID since a corporate digital ID system can address information asymmetries.

According to the BIS[16], these are often more severe for SMEs than for large corporates, which typically have detailed accounting records and a long operating history.

As such, financial institutions tend to prioritise larger corporates, often at the expense of SMEs, even though the latter also contribute significantly to the global economy.

Micro, small and medium-sized enterprises account for around 70% of employment globally, the BIS says, with approximately a quarter of GDP in low-middle income countries, and over 50% of GDP in OECD countries.

Individual digital ID is now seen as a core tool for enhancing financial inclusion, with the lessons increasingly also being directed towards the challenges facing SMEs.

In many aspects of business and finance, customer identification and verification is a necessary first step. In financial services, it is not only driven by regulatory requirements, particularly around market integrity (such as anti-money laundering rules) and prudential objectives, but also by risk management and the need to avoid losses, prevent fraud, and better understand customers and counterparties.

Corporate digital ID has the potential to dramatically simplify the identification and verification of legal entities and, thereby, to reduce the risks and costs of customer acquisition, counterparty analysis, and doing business.

In essence it provides a quick means for a legal entity to access financial and non-financial services. Beyond providing certainty of identity, corporate digital ID is able to offer further benefits by digitally linking to other information and attributes about that legal entity.

This helps to facilitate KYC and other mandatory due diligence procedures, in addition to providing information about counterparties and customers central to the risks and opportunities being evaluated, whether business, finance, or related to broader sustainable development objectives.

Corporate digital identity offers a range of potential benefits, according to a note[17] from Citi's Treasury and Trade Solutions unit, and a means to tackle a multitude of entrenched problems.

Global trade features multiple parties including exporters, importers, banks for each party in a transaction, customs, freight forwarders, shippers, and insurers. Establishing identities across this chain is critical in ensuring trade security and efficient access to finance throughout the life of the transaction. As supply chains have come under severe strain due to the coronavirus pandemic, so corporate digital identity has quietly become part of one of the biggest global stories of our time.

Also, Citi TTS points out, now that companies tend to operate around the clock and around the globe, they must be able to transact across borders and establish identities when time and geography make that impossible through physical or traditional methods. The direction of travel for most companies is to have ever-smaller physical footprints as technology and digitization continue apace.

---

[16] https://www.bis.org/publ/bppdf/bispap126.htm

[17] Corporate Digital Identity: Big Challenges and big rewards

At the heart of the challenge is, of course, the increasingly onerous set of rules around KYC. Complying with these regulations in and across multiple jurisdictions can be challenging, and can lead to delays that are often expensive for banks, and inconvenient and costly for companies. Financial services firms are eager to find ways to make KYC more efficient in order to avoid false-positives, and to distinguish between similarly named companies or multiple entities within a group. Corporate digital identity is widely seen as key to improving how KYC works.

As such, corporate digital identity can be seen as a foundation for operational efficiency, market integrity, financial stability, and inclusion.

Indeed, a legal entity may be part of a complicated corporate structure whose attributes may change frequently. Data privacy has very different implications for “legal persons” than for natural persons, in particular since most data protection regimes differentiate explicitly between personal and non-personal (e.g., company) data.

That said, individual digital ID is a very significant complement to corporate digital ID, due to the need of external users to identify and authenticate individuals that claim to represent a company and to enable interlinking of data and identities between companies, their representatives, owners, and controllers.

AI and Digital Identity: Zero Trust

Companies are clearly becoming increasingly dependent on their digital infrastructure.

As digital IDs proliferate, the constant threat of data breaches is causing mounting concern. Now, thanks to Artificial Intelligence, a new way of protecting networks is becoming possible.

Until now, most network security has relied on a firewall that separates outsiders from insiders. This perimeter-based architecture works like a fence.

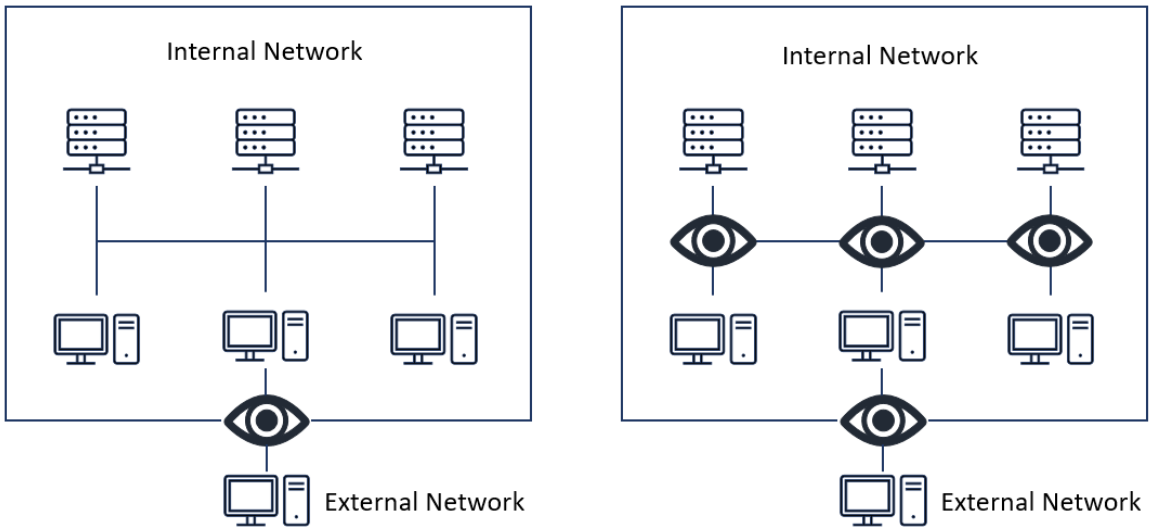
Once bad actors sneak their way inside of the network, or worse, they are themselves insiders, they are trusted by default. This means that they can wander around the network, even across departments, systems or servers, often facing zero obstacles.

Just like a fence, the entire network is only as strong as its weakest point, meaning these networks are vulnerable to attacks.

Now a huge shift is happening. In short, it involves never assuming trust - even for insiders - but rather verifying their identities all the time.

The “zero trust” idea sounds simple but has been barely implementable until the current AI coming of age because of the high granularity required in the governance and policymaking process of digital ID and access management.

Figure 5. Latency Network Security (Left) vs Zero Trust Network Security (Right)



Source: Citi Global Insights

The first step in zero trust authentication is known as endpoint analytics.

Cisco's AI Endpoint Analytics product uses machine learning to analyse endpoints based on 250 different attributes[18] (e.g., name, physical location, device type, time, IP address, and protocol utilization).

An AI model will be able to classify users into high/medium/low risk categories and determine whether to grant them access to a specific segment of the network. This essentially automates the digital ID and access management process.

In addition to granularity, AI also introduces flexibility. AI-enabled data pattern recognition is contextual- and behaviour-based.

AI can also tell whether the users are bad actors by analysing human movements, for example. Take Cursor Insight - it can verify whether the user behind the screen is the same person as they should be. They achieved an accuracy rate above 90% in a cybersecurity test.[19] With continuous verification of user identities and intentions, even insider attacks can be effectively identified and fended off.[20]

The AI solution provides an integrated one-stop platform for companies to gain full-scale vision to digital IDs connected to their network in real time. It's essential to have a complete vision of real-time connections – you cannot protect what you cannot see. However, a survey from Tanium suggests that in 94% of enterprises, up to 20% of all endpoints remain unknown.[21]

---

[18] Cisco AI Endpoint Analytics: A New Path Forward White Paper

[19] Cursor movement based user identification, ad targeting and signature verification – interview with Tamás Zelczer CEO at Cursor Insight

[20] An Insider Threat Detection Approach Based on Mouse Dynamics and Deep Learning

[21] Point Solutions Can't Protect You From Today's Problems — Here's Why You Need Converged Endpoint Management

Many organizations are still using siloed network security policies across different departments, making internal data sharing inconvenient.

AI automation of digital ID can help eliminate human errors from the process. According to IBM's Cybersecurity Intelligence Index, "human error" contributes to over 95% of cybersecurity incidents investigated.[22] Zero Trust Architecture (ZTA) is already adopted in some cases where network security is of paramount importance – all US government agencies are required to adopt ZTA.[23]

And many companies are now offering AI-enabled zero trust solutions as a service.

The market is already big – six independent research estimates[24] indicate that the average total addressable market of zero trust security in 2022 reached $27.7 billion and will grow at a 5-year CAGR of 16.3%, reaching $59.1 billion in 2027. As AI is an indispensable pillar of ZTA implementation, we expect to see a proliferation of AI in ZTA.

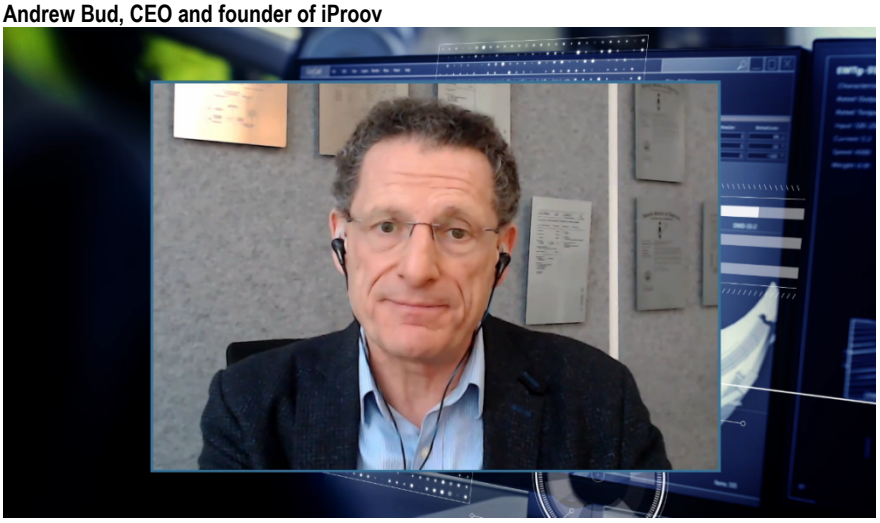
[22] IBM Security Services

[23] Federal Zero Trust Strategy – The White House

[24] Expert Market Research, Allied Market Research, Grand View Research, MarketsandMarkets, Research Dive and Future Market Insights

Digital I View: Andrew Bud, CEO and founder of iProov

Andrew Bud, CEO and founder of iProov



Source: Citi Global Insights

Andrew Bud, a veteran tech entrepreneur with over 40 years of experience founded iProov in 2011. The company provides the Genuine Presence Assurance identity platform that is used across the world by governments and corporates.

Among the company's key goals: To ensure that organisations can trust that the digital identities are provided and controlled by the real human beings to whom they belong.

"That is to say that we're very much in the business of ensuring the genuine presence of a real person. There's a lot of confusion between identity and authentication. For me digital identity is like a file, or a dossier, or information about you," he says.

Andrew thinks of digital identity as this file sitting on a desk somewhere that contains things like your name, social security, and other information. But he points out that there's a point at which human beings need to assert that digital identity. And that, he says, is where problems often arise. "The moment of authentication can be tricky and that is the point that many attackers go after. What we do at IProov is that we tie real human beings to the dossier of information that is their digital identity."

He points out that we're now moving into an age when almost every transaction and interaction people have with an organisation will happen over the internet. These transactions or interactions cannot take place effectively unless there is a high degree of trust between the two parties. The establishment of trust over the internet is an expensive and high-risk business. But he adds that establishing digital identity is an initial investment that can then dramatically reduces transaction risk and transaction costs. It's the concept, he says, of using one digital ID to reduce the cost of setting up another. Robustness is fundamental. As Andrew puts it, "It's a chain of trust and if that's broken it causes a break in the trust and erosion in the fundamental fabric of commerce and public discourse across a society,which is obviously very serious."

There are two moments, he says, at which a human being interacts with their digital identity. There's the moment they establish it - that's called enrolment or onboarding - and then there's the moment that they assert it - that is when they come back to use it. The moment at which they create it is also a moment of enormous danger. Because if a criminal or foreign power can create an identity in the name of somebody else - either real or synthetic - then they can undertake things without any fear of accountability or retribution. In government issued ID, the one thing that ties the government issued-ID to the bearer, is the photograph. As such, you have to check that the face of the owner is the same as the face of the person in the dossier. For a long-time people thought the challenge was, "how accurately can you match the face?" But in fact that's not the challenge anymore, he says. Rather, he adds, it's about determining if the face you are matching is of a real and genuine person, or not.

Quickfire questions for iProov's Andrew Bud:

How many people can you authenticate in a day?

On one day last year, we authenticated 1 million people.

Is one digital ID what everyone wants?

There is, I think, a world in which people would want to assert multiple, and in some ways unconnected, digital identities. There's no real reason why people would need just one. The importance of biometrics is to ensure the integrity of each of those digital identities. There are many countries in the world where it would be politically and socially unacceptable to have one verifiable credential. But verifiable credentials are interesting because there are degrees of freedom built in there. Your wallet can contain lots of facts about you. But you can choose what to disclose about you, and how to disclose.

So it's all about trust?

The question of who is going to be entrusted with running digital ID systems will be as much about convenience as it is about trust, actually. When people are doing low cost, low-risk transactions, they want them to be quick and easy. When they are doing things that they understand are important and are higher stakes, they want ceremony. If you give them that too easily, it actually frightens them.

What do digital ID solutions look like 10 years from now?

I think any citizen who has access to the internet will have a verifiable credential wallet. They will contain credentials issued by governments and others.

The challenge of authentication will have been met by a suite of different solutions and several biometric solutions. We won't have passwords anymore. Cloud-based biometrics will be one of the key factors. One by-product is that it will enable society to hold people accountable for what they do on social media.

How do you actually make sure someone is who they say they are?

It starts with something our company calls Genuine Presence Assurance (GPA) which uses a patented technology that delivers secure and passive face biometric authentication. GPA protects against a full range of attacks, including highly scalable digital injected attacks: replayed or synthetic imagery such as deepfakes that bypass the device camera or are injected into the data stream.

How does AI help?

Our Liveness Assurance (LA) is a patented 3D passive face biometric verification technology that combines camera imagery and contextual data from the authentication process. Deep learning AI methods assure accurate face matching and determine liveness. LA has these benefits and delivers a simple, passive, and low ceremony user experience.

icg.citi.com - Digital Identity with iProov

Digital I View: Lord Hague, former leader of conservative party and former U.K. foreign secretary

Lord Hague

Source: Lord Hague

Lord Hague, spoke to CGI's Anuj Gangahar about his recent call, alongside former UK prime minister Tony Blair, for what amounts to a fundamental remodeling of the state around science and technology, to ensure Great Britain's continued competitiveness on the global stage.

In a recent joint report, they proposed the idea of a secure digital ID for all citizens. "It goes with treating data as a competitive asset and raising national productivity," he says.

If you want to improve public services, Lord Hague says, you have to improve productivity. And digital identity is at least a part of how you could potentially do that.

That said, he also accepts that pushing through digital identity in the U.K. would be very difficult politically, for both the political left and right, stressing that the proposal is made in the spirit of moving the debate about an important topic along. He points out that people are used to proving their identity in different ways to different parts of government and to the private sector. So the issue now is more about how governments could look to introduce digital ID in a sensible and reassuring way.

"The government has to some extent be mindful and sensitive to the fact that people don't generally want government departments sharing data about them that could mean that they can build up a picture of how you are living your life," he says.

Digital I View: David Walker, head of public sector, EMEA Citi

David Walker, head of public sector, EMEA Citi

Source: Citi Global Insights

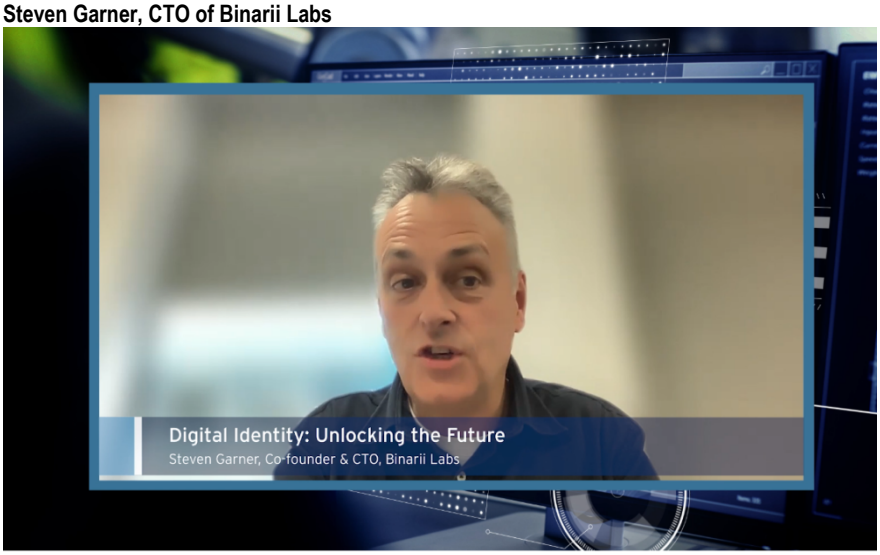
Citi's head of public sector for EMEA David Walker points out that digital identity has been a long running area of debate and fascination for all manner of public agencies and governments. "It starts really with the sheer complexity and scale of government. For them, digital identity is seen as the cornerstone of efficient service delivery," he says.

David points to recent financial programmes spurred by the pandemic, for example. "The ability to get things out in a very targeted way quickly without huge amounts of administration and without huge amounts of fraud coming in via that channel is the key."

He also highlights why, for many governments and sovereigns, digital identity is increasingly important, given that for most, their levels of sovereign and sub-sovereign debt are far higher than before the financial crisis. So governments, he says, need to deliver much more efficiently. "That's why digital identity is potentially so important."

Digital I View: Steven Garner, CTO of Binarii Labs

Steven Garner, CTO of Binarii Labs



Source: Citi Global Insights

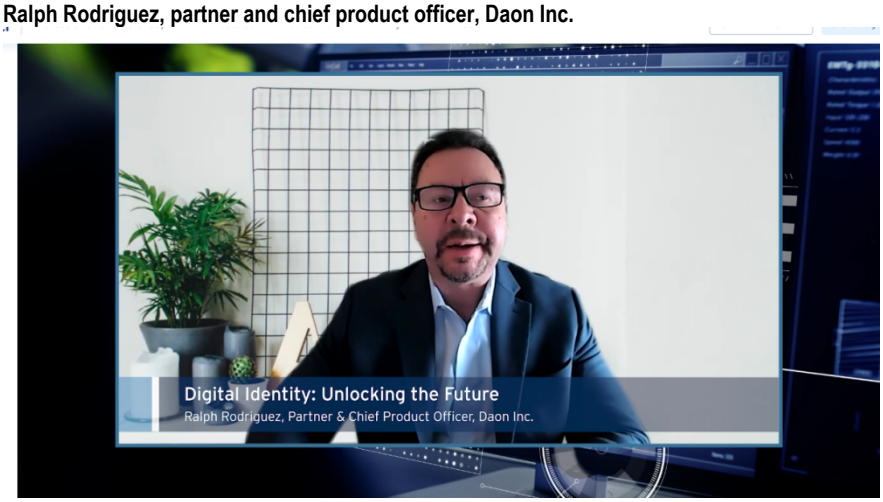
Steven Garner says companies should care about digital identity for one big reason: Cost.

"A lot of time and effort is expended on KYC. It's clear a lot of information is siloed that should really be shared by everybody." Steven says the blockchain is the perfect repository for digital identities. "It's very easy to pull information from the blockchain, very inexpensively. It's there forever. And the person that put it on there has full control over the data." As such, he says, the blockchain will be useful exactly because it will allow individuals to control what data they want to share and, crucially, with which people.

He adds that the biggest challenge for interoperable digital ID is not technology. "You can create a global database; you can create digital identities on a blockchain that are available to everybody. The challenge is more policy driven. Do countries, do governments want to give over information about their citizens to other countries and other global bodies?" He adds that over the time, the government will likely address digital identity through solutions created by the private sector. "The challenges we face are around political will and social will."

Digital I View: Ralph Rodriguez, partner and chief product officer, Daon Inc.

Ralph Rodriguez, partner and chief product officer, Daon Inc.



Source: Citi Global Insights

Ralph Rodriguez says his firm's Identity X platform is about the notion of establishing trust on day zero. How do you ascertain that person is who they say they are? The Daon platform does it using biometrics - finger, voice, or face - to allow consumers anywhere to, in a friction-free way, gain access.

"In ten to fifteen years from now, I would think that alpha-numeric passwords will finally be gone. And I think using the cloud or the blockchain will provide a very fast way to verify things."

If you are visually impaired and would like to speak to a Citi representative regarding the details of the graphics in this document, please call USA 1-888-800-5008 (TTY: 711), from outside the US +1-210-677-3788

Disclosures