Deloitte.
Insights

A report from the
Deloitte Center for Government Insights

The future of government rests on the future of identity

The blending of digital and physical worlds opens up new possibilities for public services—but a new vision of identity is required to improve trust and deliver on those possibilities.

About the authors

Ryan Galluzzo | rgalluzzo@deloitte.com

Ryan Galluzzo is a specialist leader in Deloitte & Touche's Cyber Risk practice. With over 10 years of experience, he has provided cybersecurity and identity management subject-matter insights to multiple federal agencies, including the Internal Revenue Service (IRS) and National Institute of Standards and Technology (NIST), where he contributed to NIST Special Publications (i.e., federal standards) and international privacy and security efforts.

Tim Li | timli@deloitte.com

Tim Li, principal at Deloitte & Touche LLP, is the Government & Public Services industry Strategic Growth Offering leader for cyber. In this role, he is leading growth initiatives for the firm's Cyber solutions and capabilities for federal government, state and local government, and higher education clients. Li has more than 20 years of experience in cyber across both the public and private sector, helping to drive the strategy, implementation and operation of comprehensive cyber and risk management programs.

Badri Nemani | bnemani@deloitte.com

Badri Nemani is a managing director in Deloitte Risk & Financial Advisory, where he is the cyber identity leader for Deloitte's Government & Public Services practice.

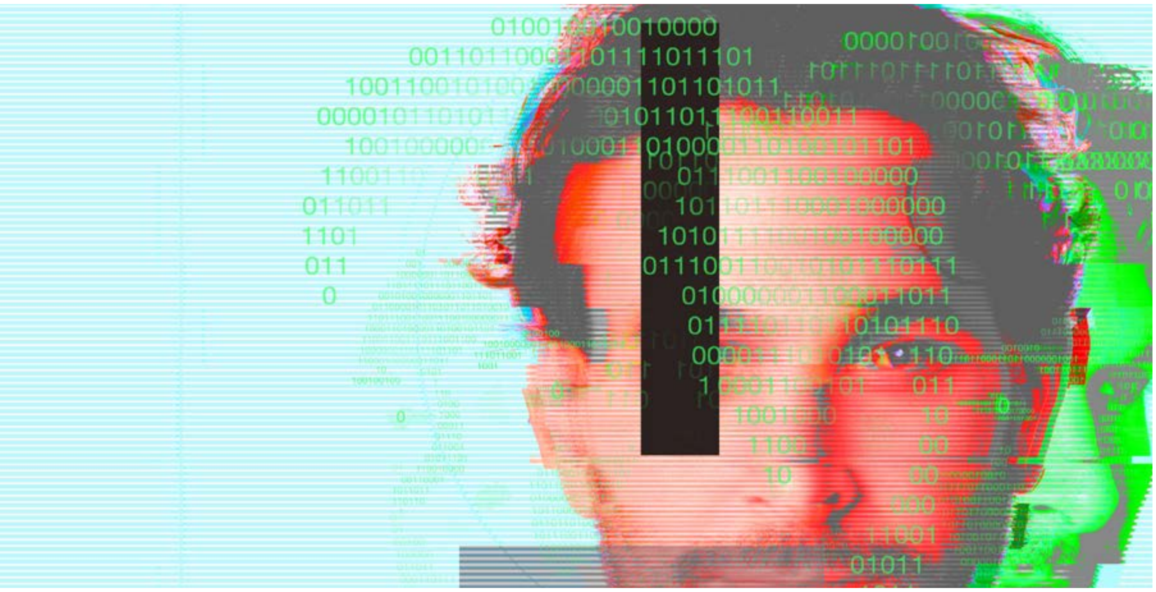
Dr Colin Souter | csoutar@deloitte.com

Dr. Colin Soutar is a managing director in Deloitte Risk & Financial Advisory. He leads cyber strategy within the Government & Public Services practice, helping organizations develop and execute their cybersecurity risk management strategies. Soutar has more than 25 years of experience in biometrics, digital identity, and cybersecurity technologies, and was previously the CTO of a public company in Toronto, Canada. He currently serves on the World Economic Forum Global Future Council for Cybersecurity.

Joe Mariani | jmariani@deloitte.com

Joe Mariani leads the government and emerging technology research program for Deloitte's Center for Government Insights. His research focuses on the intersection of culture and innovation in both commercial businesses and government organizations. Mariani's work has appeared in publications including the *National Academy of Sciences*, *World Economic Forum*, *US News & World Report*, *Wall Street Journal*, *Cyber Defense Review*, *The Marine Corps Gazette*, and more. His previous experience includes work as a consultant to defense and intelligence organizations, high school science teacher, and Marine Corps intelligence officer.

Contents



AROUND THE WORLD, government services are changing. Countries such as Australia, Austria, Estonia, Singapore, and the United Kingdom are already offering life event–triggered or proactive government services. These services could be automatic enrollment in retirement benefits or receiving your child's birth certificate without having to submit forms. These new types of government services offer fundamentally new and better interactions between government and its citizens.

However, these new services often require new forms of identity. Take the birth certificate, for example. The issuing agency needs to know that the digital identity in the hospital records corresponds to a physical identity living at X address, has rights to citizenship and so on. People no longer live in just the physical world; we live, work, and play in the physical and digital worlds—and identity also *to work seamlessly across both*.

But for years, governments have been using a patchwork of systems to identify people: physical ID cards like drivers' licenses and passports to identify physical individuals and generic logins and passwords to identify digital users online. But there were few solutions that could identify both physical and digital identities to the level of accuracy needed for government services. While the pandemic accelerated the adoption of many tools and approaches to identity like digital travel credentials, adoption was uneven. The result is a fractured ecosystem without the cohesive national strategy, policy, legislation, or leadership needed to unify it.

A common vision for identity is needed: a vision that protects user privacy and at the same time makes transactions easier regardless of your preferred channel, whether that be in the physical world, the digital, or even some combination like virtual reality. A common vision can help coordinate the innovation of the large number of players in the identity ecosystem, helping everyone move independently toward a common goal. We have termed that vision "agile identity."

Many approaches and technologies can help realize this vision, but government needs to build trust in that vision to begin unifying the identity landscape. The services that citizens want tomorrow could depend on having the identity solution we need today.

The identity landscape is evolving

IF THE NEW world of proactive, life event–based government services requires identifying individuals in both physical and digital worlds, it also adds additional layers of complexity. Rarely do our lives stand still. We move houses, get a new email address, get married, and so on. Our concept of identity must be similarly agile. If I file a tax return online, my digital identity must be able to verify that I am the physical person entitled to that return, as well as more changeable information like my status as a parent or business owner.

This trend exists for a reason: The digital services emerging today require agile identity. Over a decade ago, commercial companies discovered that by combining experiences across both physical and digital customer experiences, they could improve sales.[1] This concept of omnichannel marketing was a first step on the journey of linking the physical and digital worlds and has driven much of the progress to date. Well beyond just analyzing the contents of online carts, companies can now gather data from browsing habits, location, and more, to provide customized experiences and tools like apps and digital wallets to allow those digital experiences to work in the physical world. We can search for a flight online, buy it on a mobile app, get a boarding pass delivered to our mobile phone, and use that pass in the real world to board the flight. In fact, with the emergence of nonfungible tokens and other assets in virtual or augmented reality, physical identity can be important to transferring ownership of purely digital assets. Just as seamless service delivery in the commercial world rests on the foundations of omnichannel, the next revolution in government service delivery requires a new concept of identity and the tools to make it a reality.

This trend exists for a reason: the digital services emerging today require agile identity.

The emerging needs for modern identity

Historically, identity solutions were static. Both physical credentials like social security cards and digital ones like a usernames and passwords, once issued, stayed the same until renewed/replaced. Digital credentials are becoming more dynamic, with zero-trust schemes for access to computer systems using additional context like IP addresses, geolocations, device IDs, and so on, to continually update a user's risk. But now, the twin pressures of new technology and shifting social expectations are changing the context of identity. We live and work in physical and digital environments. Therefore, we need a form of identity that is *portable* between the physical and digital worlds, between different transaction types, and across different properties.

But the relevant attributes of identity can also shift rapidly as we move between those environments, requiring identity to be more dynamic than just printed plastic cards or usernames and passwords. If users are to understand what information is being used where and when, modern identity will need *transparency* in how data is collected, how the technology works, and how an individual's data is treated in order to protect privacy.

Further, shifting social expectations also have implications for identity. The ability of users to control digital data—whether by accepting/rejecting cookies, using ad blockers, or controlling how apps access data—has increasingly created an expectation that users should be able control use of their data in other contexts as well. Modern identity, in turn, needs to be governed by *individual choice*.

Technology and social trends have altered the context of the world. The nature of identity must shift to match this new context. The modern world needs a system of identity that is agile—identity built on **portability**; **transparency**; and **individual choice**.

But the fractured landscape hinders progress

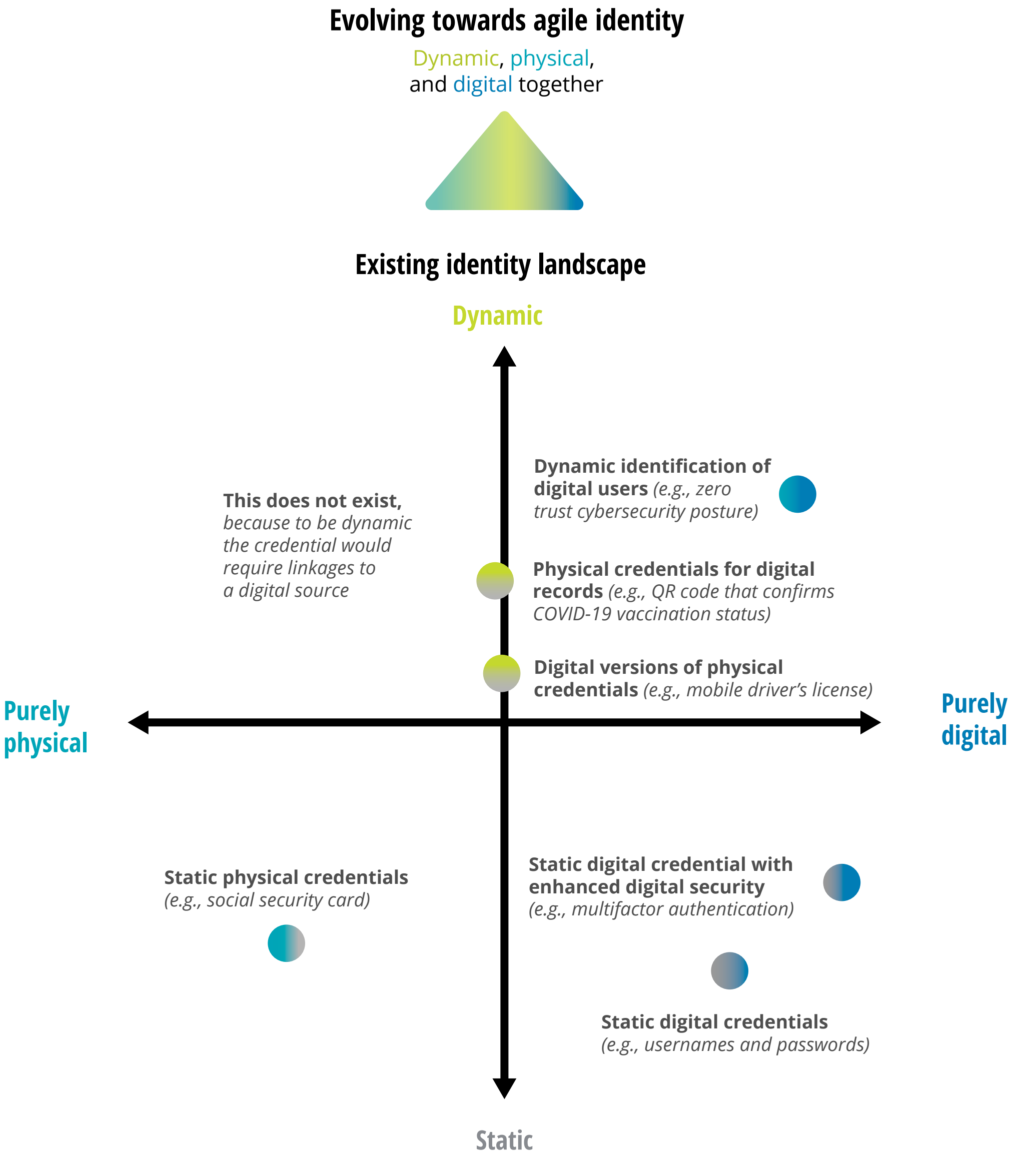
Governments and companies use a variety of identity solutions today with a wide array of capabilities. We can visualize the fractured, but evolving, identity landscape by categorizing existing identity solutions based on whether they are physical or digital and dynamic or static (figure 1).

The problem is that digital identity requires several different roles, each with different incentives pushing and pulling on the players. While omnichannel marketing may involve just a company, a customer, and a service provider, identity at a minimum requires an issuer (who creates the credential), a holder (the individual who uses that credential), a verifier (who views the credential to verify the holder), a relying party (who relies on the verified identity to provide a good or service), and a governing authority (who sets rules for the system).[2] Further complicating matters is the fact that organizations may play multiple roles depending on the transaction in question. For example, the federal government issues physicians with an identifying number to allow them to prescribe controlled substances, but it may also act as verifier in verifying that identity during investigations. Add on top of that the variety of roles that technology and service providers are likely to play, and there is a wide variety of players, all with different goals and incentives. As a result, different solutions can go in radically different directions depending on who created them or for what purpose. With many players, each pursuing their own solutions according to their own incentives, the identity landscape lacks the cohesiveness needed to support new services and promote the interests of individuals.

To realize a revolution in citizen experience, government has a unique ability to bring clarity to this fragmented identity landscape.

FIGURE 1

The existing identity landscape is fragmented, but slowly moving toward the dynamic, physical-digital nature needed for future government services


Evolving towards agile identity
Dynamic, physical,
and digital together
Existing identity landscape
Dynamic
Static
Purely physical
Purely digital
Dynamic identification of digital users *(e.g., zero trust cybersecurity posture)*
This does not exist, *because to be dynamic the credential would require linkages to a digital source*
Physical credentials for digital records *(e.g., QR code that confirms COVID-19 vaccination status)*
Digital versions of physical credentials *(e.g., mobile driver's license)*
Static physical credentials *(e.g., social security card)*
Static digital credential with enhanced digital security *(e.g., multifactor authentication)*
Static digital credentials *(e.g., usernames and passwords)*

Source: Deloitte analysis.

A new vision of identity

WITH SO MANY different players pushed by so many different incentives, it is unlikely that one dominant, interoperable solution is going to emerge on its own—nor is this necessarily desirable. Instead, we need a common vision for *agile identity* towards which different players can work independently. That way, whether you are an issuer of credentials like a state Department of Motor Vehicles (DMV) or a verifier of credentials like a web service provider, you can understand the future goals and requirements of the identity ecosystem.

Agile identity is a user-controlled identity that enables individuals to selectively manage the exchange of their personal attributes and data to securely interact with commercial and government services, in both the digital and physical domains. This vision has three hallmarks: portability, transparency, and individual choice.

Portability. For identity to work at scale, it needs to work across a variety of platforms and be accepted for a variety of services. This means that citizens can access their identity on a phone, computer, or in person, and use that identity to verify their age at a liquor store, board a flight, or pay their taxes online.

- **How would it work?** To achieve this level of seamless portability requires a curated ecosystem of issuers and verifiers, all working to common standards and linking to a core identity from a governing authority. Keys on a ring are a helpful metaphor for this ecosystem (figure 2). The governing authority establishes the rules for how a core identity that functions like a keyring is created. Then issuers can create different credentials that can be tied to that core identity like keys on a ring. This ecosystem is also dynamic, with credentials being added as they are issued or removed as they expire. An individual may have multiple core identities depending on the communities they choose to participate in. Such efforts require the harmonization of standards across different technologies (e.g., ISO's 18013 for mobile driving license (mDL) and World Wide Web Consortium's (W3C) Verifiable Credentials).

We need a common vision for *agile identity* towards which different players can work independently.

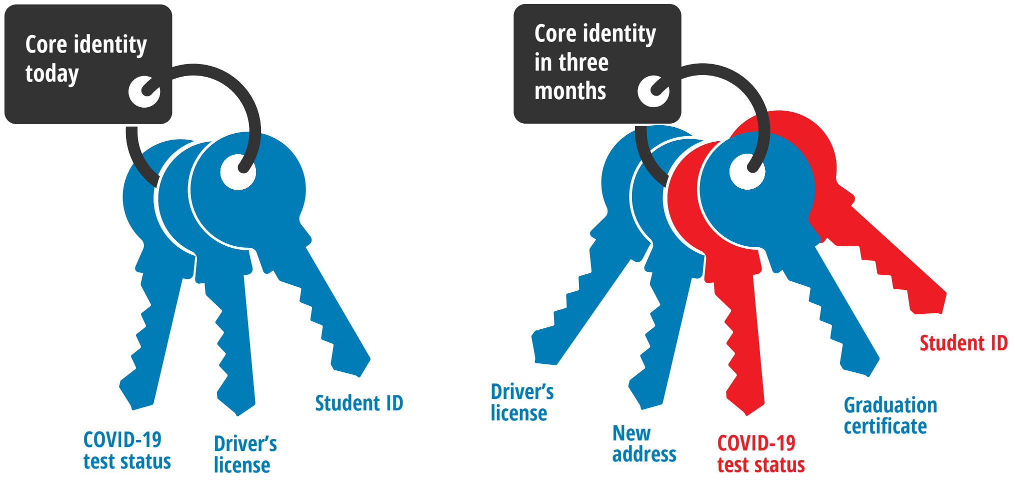
Transparency. With so many players, transparency is needed to help ensure trust at every step. Transparency about the tools, technology, and methods used in establishing identity would give issuers and verifiers solid assurance that transactions can be trusted. When paired with transparency about what data is collected and available to whom, this can also help individuals have confidence that their personal information is not being lost or misused.

- **How would it work?** Transparency starts from the very beginning. An "Identity Bill of Rights" should spell out what constituents can expect from every player involved in handling their identity. The bill of rights should lay out guiding principles like ensuring users have control on their data, demanding easy-to-understand statements of what data is being used and by whom, and so on. These high-level principles can then be developed into specific rules by federal, state, and local governments with enforcement mechanisms to ensure that everyone—government organizations and companies

FIGURE 2

A core identity token and additional credentials function like keys on a keyring to allow for portability of identity

🟦 Valid 🟥 No longer valid



Source: Deloitte analysis.

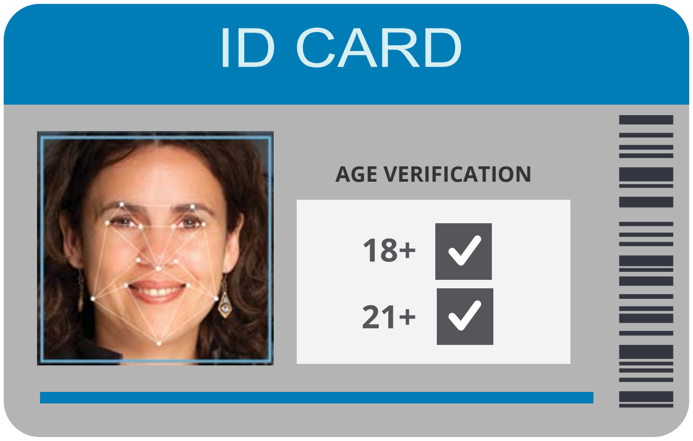
alike—follow them. One example of such a transparency effort is the cybersecurity labeling of Internet of Things devices (IoT) in the US. The effort began with the *Executive Order on Improving the Nation's Cybersecurity* (EO 14028) that laid down the requirement to better educate consumers about cybersecurity risks. This requirement is being turned into guidance from National Institute of Standards and Technology (NIST) for labeling consumer IoT products for cyber and privacy information and possible enforcement mechanisms by the Federal Trade Commission (FTC).[3]

Individual choice. With transparency comes the opportunity to control your own data. Individual choice is the ability of individuals to control which credentials to use, which data they release, and to whom they release that data. With physical IDs, the individual has no choice but to reveal all the information on the card to whomever they show it. With an agile identity solution, individuals can choose which credential to use and even what data to reveal, allowing them to show only the data needed for a particular transaction. When dealing with such sensitive data as identity information, the principle of individual choice could help build trust among individual users, and also reduce the compliance burden for many agencies as they would have to protect less personally identifiable information (PII).

- **How would it work?** Models of individual control of identity already exist, albeit on a small scale. Take mobile drivers' licenses. Although the license contains such sensitive information as date of birth, height, weight, and home address, a user can verify their age at a liquor store without ever having to reveal that information, merely showing the clerk a verifiable assertion that they are over 21 (figure 3). This is a significant privacy improvement over paper IDs where all of that information is permanently visible to anyone who sees the card for any purpose. That may seem like a minor inconvenience but consider government programs that require income validation. Users would not have to reveal their full pay statements, but instead merely verify to the clerk

FIGURE 3

Individual choice allows users to control who sees what information, such as verifying age without exposing date of birth



Source: Deloitte analysis.

that they qualify. Clearly communicating this improvement would be critical in helping win over a hesitant public.

A single vision, lots of possible technologies

The three hallmarks of agile identity should be present in any future identity solution, and there are many ways to achieve those hallmarks. Each approach has its own strengths, weaknesses, and supporting technologies:

- **Centralized**. One party, such as a government or agency, is an identity provider that transfers citizen attributes to relying parties. The advantages of this approach are that they allow more direct control for governments and accountability to citizens. The disadvantages are that they can be difficult to create—especially for large, federally organized nations—difficult to administer given the large volumes of PII collected, and difficult to upgrade technologically when needed. They also often create "honey pots" of data attractive to attackers and are often difficult to protect. Centralization also creates privacy concerns as a limited number of central authorities hold large volumes of user data.
  - **See it in the real world**. Estonia maintains a centrally managed identity system that allows users to identify themselves both in person and online via PKI-enabled (public key infrastructure-enabled) identity cards.[4]
- **Federated**. Established identities are accepted across connected communities or similar services. Federated systems are similar to centralized identity systems, except that a variety of brokers provide the digital identities to relying parties, often entities with similar missions (e.g., government agencies). This enables portability between different applications and services since one identity can be used in different locations. The advantage of this approach is that there are robust existing standards, meaning that new services can be set up quickly. Federated systems can also provide greater convenience for individuals since they can reuse existing identities at new services. However, due to the complexity of federation

rules and disparate regulatory environments, the full portability of such solutions has been limited. The market has also been slow to take shape, resulting a few core players dominating the scene and introducing similar risks to fully centralized identity models.

- **See it in the real world**. Canada's Verified.me is an example of a federated approach to identity. The system allows users to log in to online services from government and private sector using credentials that they already have from one of several major banks rather than having to use a different username and password for each service.[5]

An agile identity does not only support the different transaction types that a user may encounter, but also operates across different communities and implementation models.

- **Decentralized**. Fully decentralized identity systems connect many identity providers to many relying parties—distributing data and pushing control to the individual. This type of system sets citizens up with a digital "wallet" that serves as a login to multiple websites and applications as well as a sort of "personal data" vault. Generally, these systems are privately held and rely on common operating standards rather than a governing body. As such, decentralized approaches offer citizens the most control over their data. But lacking any centralized authority, they can also be the most difficult to create, administer, and scale.

  - **See it in the real world**. MemberPass is a decentralized identity service for credit unions. MemberPass allows credit unions to issue a credential to customers stored on a Sovrin blockchain.[6] Users can then control that credential in a digital wallet, allowing them to authenticate themselves using the same credential whether online or in the bank branch.

How would it work?

Ultimately, the approach chosen will come down to how different communities wish to navigate the trade-offs of the different models. In fact, the likely path forward for many communities will be a mix of all three approaches, depending on the risk, use cases, and transaction types they support. This further emphasizes the dynamic nature of agile identity. An agile identity does not only support the different transaction types that a user may encounter, but also operates across different communities and implementation models. This is particularly critical as the identity ecosystem continues to evolve.

The fictional vignette below, for example, lays out one future where individuals use their mDL License issued by a central state authority acting as their "core" identity that binds additional verifiable credentials or attributes from other issuers operating in a decentralized model. A truly agile ecosystem will harmonize standards and different technology implementations of different identity models to provide individuals with the greatest degree of choice and portability possible. Centralized, decentralized, and federated ecosystems can coexist to support the different interactions and personas we reflect in our lives.

Jamie, a 21-year-old college senior, is due for a license renewal. On the day that she visits the local DMV, the clerk asks her if she wants to download a secure wallet application to her smart phone that can act as her digital driver's license. Seeing the potential convenience of having her driver's license stored on her phone, she chooses to enroll. After downloading the application, Jamie has her identity verified by the DMV clerk, who then provisions the identity in her application. Jamie now has all the personal information usually stored on her licenses at her fingertips encrypted and digitally signed by the DMV on her device.

A few months later, Jamie graduates from college with a degree in engineering. During her last few days at school, the registrar offers students an electronically verifiable credential of their diploma. Because Jamie's secure wallet application leverages multiple open standards, she is able to sign into her school's online account, scan a QR code with her wallet application, and populate a cryptographically verifiable version of her transcript. She then links this to her LinkedIn account when applying for jobs online, allowing employers to independently verify her skills without ever having to directly contact the school.

After getting a new job with an engineering firm, Jamie needs to file her state income taxes online. Navigating to the state tax administrator's web page, she sees that she can sign in and file her taxes directly using her state-approved secure wallet. She selects "sign-in with your mDL," scans a QR code presented by the page, and consents to the release of her information. The personal information she requires to establish an account is automatically populated directly from the issuing source at the DMV. Later, she receives a push notification from the tax administrator with an update on the status of her refund. Jamie uses her phone's biometric authentication capabilities to log in seamlessly without a password.

The recent growth in popularity of digital wallets on smartphones and the adoption of "mDL" in states such as Arizona, Colorado, Delaware, Oklahoma, and Louisiana, as well as the continued advancement of verifiable credential standards make a story such as this increasingly likely in the near future.[7] But regardless of the approach a jurisdiction chooses, the ultimate success of any identity solution will depend on how well it is trusted.

How to make it a reality

THE STAKES OF identity are incredibly high. For citizens, identity contains their most sensitive and personal information. For governments, identifying citizens and delivering services are core functions of the state. With the consequences of failure being so high, every stakeholder needs to trust that the entire system will work as designed and protect their interests. But as we have seen, those interests vary with each stakeholder and the role they play. Therefore, government needs to help build trust in an agile identity ecosystem—regardless of the technology used—if it is to be adopted at scale. Our research on public trust suggests that this can be achieved in three parts: by building trust in the competence of the solution, building trust in the humanity of the players, and trust in the integrity of the system.

First, government should build **trust in the competence** of the solution. Issuers, verifiers, and relying parties in particular need to trust that the technology will work as advertised, because without it, their businesses and missions will suffer. Whether a nation uses a distributed, federated, or centralized approach, the technology stack that makes agile identity work needs to be trusted by those creating and checking credentials. They need to know that the system will work as advertised and deliver the promised benefits. On the one hand, this means demonstrating reliability, so that verifiers know that transactions will go through quickly and easily under any circumstances. On the other hand, it means demonstrating security so that verifiers know that the credentials they issue cannot be hacked or forged. Balancing these needs for trust requires an entire ecosystem of collaboration across federal, state, and local governments, as well as commercial companies.

BUILD TRUST OR LOSE TRUST

Government needs to build trust in an agile identity ecosystem to provide the services that citizens need. Without that trust in identity, trust in government itself may suffer as a result. Citizens already live and work across physical and digital worlds, so government services are provided there as well. Without identity solutions that can keep up, those services are more at risk of fraud than ever before. Often, that fraud is due to an inability to identify real, physical human beings from purely digital data. Our research on trust suggests that these type of missteps may be **especially damaging to citizens' trust** in many government organizations.[8]

But a trusted technical system only works if there are users willing to participate. For citizens to willingly entrust their personal data to an identity solution, they need to trust more than just the technology—they need to **trust the humanity** of the implementors. Most citizens will not have deep technical knowledge about how an agile identity solution works. Even if they hear terms like blockchain or PKI, most will not have a sense of how those technologies truly operate and where risks may lie. Therefore, citizens' trust of complex technology solutions will be driven by their trust of the individuals and organizations operating it.[9] If they trust the motives of the government agencies and companies involved, they are more likely to trust, and therefore use, the solution. If not, adoption could lag, and the solution may fail. And this trust in humanity must be two-way: Federal, state, and local leaders can harness digital technologies to solicit the input of constituents to help ensure that any identity systems meet their needs. The freer and more open this communication is, the more it helps companies and agencies see users as individuals and not merely as means to profit.

Finally, in an ecosystem as crowded as identity, it is not sufficient that only government be trustworthy. Every issuer, verifier, technology, or service provider must adhere to the same standards of trustworthy behavior. To achieve this, government should **build trust in the integrity** of the system, implementing rules, establishing measurement, and creating accountability structures to enable a network of trust.[10] In ecosystems working on sensitive topics, it only takes the failure of one player to cast mistrust over the whole system. Therefore, government should gather data about citizens' trust, put in place enforceable standards of conduct, and communicate through real people the mission and transparency of the identity solution. This can look like common privacy labeling on tools that use identity that describes what data is collected and how it is used but can and should vary with the needs of the public. Government also needs to function as a backstop to the identity ecosystem. Just as the federal government builds trust in the integrity of the banking system by backstopping it with deposit insurance, governments should take similar steps to backstop the identity system should leaks or compromises occur—by providing redress and protection for individual users, enforcing accountability to expected standards, and providing incentives to organizations that uphold the principles of the ecosystem.

Building trust may sound like an abstract concept, but trust can be seen at work every day in use cases like payment processing—a very similar ecosystem—where different public and private players work together on highly sensitive use cases. First, vendors and payment processors must trust the reliability and security of the system. Banks want to know that transactions are unlikely to be fraudulent and to gather data that can help them identify if that is the case. Vendors on the other hand need transactions to be processed quickly every time. Delays can not only cut into sales but can also encourage workarounds that are more prone to fraud. And, as is likely for agile identity, modern payments processing is a mix of centralized, decentralized, and federated approaches. Take mobile payment apps for example. These are federated platforms that link to the centralized bank accounts that house most individuals' money but can also allow the transfer of fully decentralized cryptocurrencies. Also, like identity, most citizens have very little knowledge about how payment processing works behind the scenes. Rather, our trust in the system rests on our trust in our banks and the government regulators and insurers whom we trust to secure our savings and backstop them in case of loss. Much as this ecosystem exists in payments processing today, it needs to be recreated in identity if stakeholders are to trust the technology.

A roadmap to trust

AGILE IDENTITY IS needed today. Every day without a scaled agile identity ecosystem increases the risk of fraud, compromise of personal data, and inefficient government services. We have seen ersatz and half-realized identity solutions in the past, and they often lead to more problems. For example, the use of social security numbers as a de facto national identity number has created significant opportunities for fraud since those numbers and their simple paper cards were never designed to fill that role.

The path to agile identity is not a straight line, however. Like payment processing, no single player can create a successful ecosystem. Collaboration and coordination will likely determine success.

Due to its importance to the identity ecosystem, government at all levels has an important role to play in ensuring that agile identity gets moving. Since the successful adoption of agile identity rests on building trust in the solution, the players, and integrity of the system—it can be a useful way of organizing the immediate next steps for each player to help make agile identity a reality (figure 4).

Agile identity offers the technology-agnostic way ahead on digital identity that government services need, and citizens want.

Figure 4

What each stakeholder can do to begin building trust in agile identity

Federal government	State and local government	Industry	Constituents
Build trust in competence of the solution			
• Convene stakeholders and provide consistent, unified leadership • Advance and promote consistent digital identity vision, strategy, and standards • Create incentives for states and industry to align to those standards such as grants, contracts, access to federal identity ecosystem, fines for misuse of identity, and more • Improve measurement, testing, and accreditation of new technologies to determine if they meet those standards	• Unlock the power of government data by making it accessible to other stakeholders, consistent with privacy/security safeguards • Invest at all levels—from basic technology to service providers—and engage with efforts at the national level • Orchestrate fraud and threat signal–sharing to improve the overall ecosystem's ability to detect risks or threats	• Develop tools and technology based on consensus standards and protocols • Engage in certification and measurement of technologies through approved mechanisms • Build technologies that promote individual ownership and determination • Invest in innovation	• Provide feedback on features desired in an identity solution
Build trust in humanity of the players			
• Advance a clear national agenda on digital identity • Identify a single leader to be point person for the public on identity issues • Build values and expectations into contracts and other transactions • Create an "Identity Bill of Rights" that lays out what citizens can expect of government and companies providing identity services	• Solicit input from citizens on their desires for an identity solution • Work through networks of real individuals in local communities to build trust in proposed identity solutions	• Regularly engage with customers to understand their values and expectations • Regularly communicate company's goals and role in identity ecosystem • Label every app or use of data with a short, plain-language descriptor that people can understand and approve/reject quickly	• Provide feedback on values desired in an overall identity solution
Build trust in the integrity of the system			
• Establish rules for transparency on data use that can be easily understood by citizens • Create mechanisms for accountability to hold all players to the standards established in the "Identity Bill of Rights" • Serve as a backstop to the ecosystem by services in the event a constituent's identity is compromised or lost	• Use public input to craft rules and standards consistent with federal guidelines, but meeting the unique needs of the state • Publicly commit to adhere to all standards • Pass privacy and transparency legislation at the state level consistent with an "Identity Bill of Rights"	• Publicly commit to adhere to all standards • Demonstrate adherence to standards with annual public evaluations	• Hold public leaders and private companies accountable for failures to uphold standards

Source: Deloitte analysis.

Agile identity offers the technology-agnostic way ahead on digital identity that government services need, and citizens want. But if we are to realize the transformational government services of tomorrow, we should begin building the infrastructure of agile identity today. Our future selves might literally depend on it.

Endnotes

1. Savannah Louie, “A brief history of omnichannel marketing,” Nectarom, January 5, 2015.
2. W3C, “Verifiable credentials data model v1.1: W3C recommendation,” accessed May 26, 2022.
3. National Institute of Standards and Technology, “Cybersecurity labeling for consumers: Internet of Things (IoT) devices and software,” May 24, 2022.
4. Estonia Information Security Authority, “Electronic identity eID,” accessed May 26, 2022.
5. Verified.Me, “Your digital identity in your control,” accessed May 13, 2022.
6. MemberPass, “FAQ,” accessed May 26, 2022.
7. Chris Velazco, “Digital driver’s licenses take the sting out of forgetting your wallet. Here’s how they work,” *Washington Post*, March 24, 2021.
8. William D. Eggers, *Rebuilding trust in government: Four signals that can help improve citizen trust and engagement*, Deloitte Insights, March 9, 2021.
9. John O’Leary, Angela Welle, and Sushumna Agarwal, *Improving trust in state and local government: Insights from data*, Deloitte Insights, September 22, 2021.
10. Jesse Goldhammer et al., *Using “trust networks” to address the trust deficit in government: Orchestrating the government trust revival*, Deloitte Insights, August 10, 2021.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Industry leadership

Tim Li
Cyber Strategic Growth Offering leader | Government and Public Services
Principal | Deloitte & Touche LLP
+1 571 814 7679 | timli@deloitte.com

Tim Li, principal at Deloitte & Touche LLP, is the Government & Public Services industry Strategic Growth Offering leader for cyber.

William D. Eggers
Executive director | Deloitte Center for Government Insights
Deloitte Services LP
+1 571 882 6585 | weggers@deloitte.com

William D. Eggers is the executive director of Deloitte's Center for Government Insights, where he is responsible for the firm's public sector thought leadership.

The Deloitte Center for Government Insights

Joe Mariani
Deloitte Center for Government Insights | Senior manager
Deloitte Services LP
+1 571 882 6585 | jmariani@deloitte.com

Joe Mariani leads the government and emerging technology research program for Deloitte's Center for Government Insights. His research focuses on the intersection of culture and innovation in both commercial businesses and government organizations.

About the Deloitte Center for Government Insights

The Deloitte Center for Government Insights shares inspiring stories of government innovation, looking at what's behind the adoption of new technologies and management practices. We produce cutting-edge research that guides public officials without burying them in jargon and minutiae, crystalizing essential insights in an easy-to-absorb format. Through research, forums, and immersive workshops, our goal is to provide public officials, policy professionals, and members of the media with fresh insights that advance an understanding of what is possible in government transformation.

Deloitte Cyber

As a recognized leader in cybersecurity consulting, Deloitte Cyber includes thousands of dedicated cyber professionals, across numerous industry sectors, who help clients better align cyber risk strategy and investments with strategic business priorities, improve threat awareness and visibility, and strengthen their ability to thrive in the face of cyber incidents. In the realm of Cyber Everywhere, the ubiquity of cyber drives the scope of our services. Deloitte Cyber advises, implements, and manages solutions in strategy, defense, and response; data security; application security; infrastructure security; and identity management.To learn more, visit Deloitte.com.

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Ramani Moses, Aparna Prusty, Aditi Gupta, Arpan Kumar Saha, and Aishwarya Iyer
Creative: Sonya Vasilieff and Rishwa Amarnath
Audience development: Maria Martin Cirujano
Cover artwork: Sonya Vasilieff

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.