Business Roundtable

Building Trusted & Resilient

DIGITAL IDENTITY

JULY 2019

Business Roundtable CEO members lead companies with more than 15 million employees and $7.5 trillion in revenues. The combined market capitalization of Business Roundtable member companies is the equivalent of over 27 percent of total U.S. stock market capitalization, and Business Roundtable members invest nearly $147 billion in research and development — equal to over 40 percent of total U.S. private R&D spending. Our companies pay $296 billion in dividends to shareholders and generate $488 billion in revenues for small and medium-sized businesses. Business Roundtable companies also make more than $8 billion in charitable contributions. Learn more at BusinessRoundtable.org.

Building Trusted & Resilient DIGITAL IDENTITY

JULY 2019

CONTENTS

Introduction

The ability of individuals to recognize and trust each other plays a fundamental role in economic and social interactions.

Before the digital age, identification systems relied upon physical documents and face-to-face interactions. The internet and the proliferation of internet-enabled devices have dramatically changed the interplay between individuals and institutions — from the way we bank and shop to the way we communicate with each other. At the same time, the internet has made disguising, hiding or misrepresenting their identities substantially easier for malicious actors, forcing us to find new ways to confidently interact with one another online.

Personal information is a lucrative target for theft. Misusing it to create illegitimate digital identities is one of the simplest methods for committing online fraud. Indeed, identity fraud costs the U.S. economy billions of dollars annually — in 2018, $14.7 billion was stolen from U.S. consumers online.[1] Malicious actors also exploit fraudulent identity information to illegally collect government benefits, such as food stamps; unemployment assistance; and Medicare, Medicaid and Social Security payments. The surface area available for attack will significantly expand as we increasingly interact with internet-connected devices across all aspects of life.

While service providers and cybersecurity firms work to keep up with evolving threats, criminals use creative and sophisticated tools to stay a step ahead. As a result, illegitimate identity may well be the likeliest path for fraud and other cybersecurity intrusions.

Yet having a digital identity is more than a data protection and security mechanism — it enables individual users and institutions to establish an appropriate level of trust to transact and interact in the digital world, including activities ranging from banking to health care to social media. And in a world in which boundaries among sectors are increasingly blurred, the relationship of a user and a company is no longer always directly owned or governed by the company. With digital identity being a key enabler for participation in digital interactions, it must not only be secure but also convenient so it can be used across sectors and in daily interactions.

To continue to reap the benefits of the online world, it is imperative that the U.S. government and the private sector work together to strengthen digital identity without sacrificing the speed or convenience that today's society demands. Meeting this goal would strengthen the entire online ecosystem — from e-commerce to health care, employment, supply chains and more.

This paper presents an approach to digital identity that would reduce identity theft and fraud without creating undue costs or burdens for users or service providers. It describes the current state of play, offers a vision for the future, and then puts forward a realistic action plan for how the private and public sectors can bolster digital identity.

Digital Identity Today Promise & Challenges

While anonymity is a fundamental and cherished aspect of the internet, some services require at least partial knowledge of an individual's identity to function properly.

Digital identity is the online persona of a subject, and a single definition is widely debated internationally.[2] Digital identity proofing and authentication are the two primary methods of establishing verifiable identity attributes, and opportunities exist to improve both, which may represent one's physical and online personas. (For a "Primer on Digital Identity," see the Appendix.)

Identity Proofing

Identity proofing establishes that a subject is whom he or she claims to be.[3] Service providers conduct identity proofing early in a transaction, such as opening a bank account or applying for a student loan. In a brick-and-mortar establishment, the service provider can check a customer's driver's license or passport to prove the person's identity. This process is more difficult online, however.

Digital identity proofing consists of three steps: resolution, validation and verification. Resolution often involves using records available from public sources to ascertain the identity of an individual. Validation confirms the authenticity and accuracy of the identity information by checking an authoritative source, and verification relies on information that only the individual and the party doing identity proofing should know — such as transaction history — to confirm ownership of the claimed identity (see the Appendix).

The resolution and verification stages have historically involved individuals confirming personal information. In the digital world, however, knowledge-based proof is no longer sufficient for many purposes. Data breaches and the increased sharing of sensitive data via online platforms such as social media mean that this method is no longer as trustworthy as it once was. Additionally, this method of identity proofing may unintentionally favor certain portions of the population, such as those with longstanding accounts and credit histories.

New technologies have created opportunities to increase confidence in the authenticity of identity evidence. For example, a bank could remotely match identity documents and biometrics — such as a photo — from a digital driver's license with the individual presenting the evidence. These approaches can be done remotely with mobile phones and personal computers and are effective for many users.

IDENTITY PROOFING VS. AUTHENTICATION

IDENTITY PROOFING: The process by which an organization collects, validates and verifies information about a person, often occurring at the time of enrollment.

AUTHENTICATION: The process of determining the validity of one or more credentials presented by a party as a prerequisite for granting access to a system or information.

These new technologies are a step toward the future; thanks to the digitization of government-issued identification, users with a driver's license and a passport have a high likelihood of being able to prove their identity online. However, an individual without these forms of identification — or without a smartphone — will struggle with (or be unable to use) these solutions. The individual will often have to fall back to inconvenient alternatives, such as visiting a brick-and-mortar location, which increases the effort to the user and costs the service provider time and money. While progress has been made, much work remains to be done to improve identity proofing.

Authentication

Authentication factors include things users **know** (namely passwords), **have** (namely credentials) or **are** (namely biometric identifiers). Knowledge-based authentication, commonly used today, has inherent weaknesses. Strong authentication relies on the robustness of identity information available at the time of the presentation of the identity claim. Often, improving the robustness of this information involves multifactor authentication (MFA), in which at least one factor is not knowledge based. Companies and governments are increasingly offering, and in some instances requiring, MFA. MFA can include asking a user to present his or her biometrics (verifying who the user *is*) or sending a code to a smartphone (verifying what the user *has*).

MFA solutions may have some residual user friction. For example, if MFA options are specific to each service provider, second-factor authenticator fatigue could set in on top of existing password fatigue. If adopted broadly and implemented well, smartphone-based authentication, biometrics and other promising technologies could mitigate this risk.

The application of data analytics, artificial intelligence, machine learning and multimodal biometrics to authentication is also increasing the availability of trusted authentication solutions.

Identity Federation and Decentralized Identity

When two or more traditional identity systems (e.g., a government entity and a bank) establish mutual trust — either by distributing components of proofing and trust or by mutually recognizing each other's proofing and trust standards — a federated identity system results.[4] These systems are prevalent in some day-to-day activities. For example, consumers know they can get cash at virtually any ATM (while paying a fee to do so), rent a car using a driver's license from another state, and log in to a third-party service through their social media or email accounts.

At the enterprise level, identity federation has seen widespread adoption. For example, many companies federate an individual's corporate identity to allow easy access to benefits information, such as health care claims and retirement planning. Federation has also found success in the defense, aerospace and automobile industries, with the government and/or industry partners taking a shared approach to employee vetting, such as security clearances. The benefits of federation have long been clear to participants in those industries, where trust is established among multiple

DECENTRALIZED IDENTITY SYSTEM PILOTS

MALTA: The government of Malta is piloting a program in which educational institutions use blockchain technology to issue credentials (such as diplomas and 15 professional certifications) to individuals, who can access and manage them through a mobile application.

ANTWERP: The city of Antwerp has piloted a system for individuals to create and manage a through-life identity on a mobile application employing blockchain technology, starting with identity attestations at birth from doctors, hospitals and the government birth registry.

organizations or where a single organization has individual trust relationships with other organizations such as a trusted intermediary. Federation may create efficiencies by accepting the identity proofing and authentication conducted by a different trusted institution. However, a federated model is based on individual agreements between institutions to trust and accept the digital identity of another. While the user may be required to remember one fewer set of login credentials per federation agreement, the digital identity often is not accepted more broadly and depends on established governance between institutions.

For broader consumer adoption, decentralized identity systems, which are mostly in pilot phases, offer some intriguing alternatives to central and federated identity schemes. Instead of partners relying on a data owner, a set of owners or a trusted intermediary to establish and manage identities, consumers could use their digital devices to hold attestations from several trust anchors, such as governments, banks and employers. The individual could choose which attestation or data attribute to share and with whom to share it.[5] Therefore, in a decentralized identity system, a user often would have greater control over his or her own identity and identity data. Decentralized identities, however, would still require large or complex governance and liability models and are currently being explored as this landscape continues to evolve.

A Vision for the Future

Objectives for Improving Digital Identity

To take full advantage of advances in technology, an appropriate mix of policy and process needs to be in place.

Businesses, governments and individuals should be able to securely, intuitively and easily execute digital transactions that respect privacy, are free from fraud, have relatively low costs, and present choices that have very little friction for both individuals and organizations. To meet this goal, the U.S. government and the private sector must work together to establish digital identity systems based on:

1. Strong identity proofing that reduces identity fraud by discouraging reliance solely on knowledge-based techniques.
2. Strong authentication, with effective options for MFA that are free to consumers, and strong fraud detection capabilities to protect against unauthorized release or access to personal and account information.
3. Use of identity federation and decentralized identity to reduce unnecessary repetition of identity proofing and authentication, while providing more transparency and control of identity data to users.

These systems should achieve the following goals:

Strengthen and Sustain the Security and Privacy of Digital Services

Policies should promote user confidence in online services — from financial transactions and accessing health care benefits to requesting government services. To reduce the risk and impact of identity theft, digital identity solutions must embed robust security and privacy that consumers can trust and must be able to introduce new security techniques as the threat landscape evolves.

Insure Digital Identity with a Safety Net

For a digital identity to be resilient, organizations must not only provide security to prevent a breach from occurring but also be prepared for *when* a breach occurs. Users will put more trust in a digital identity if a "safety net" insures the users against the harm done when identity data are stolen and enables continuity of service. When liability is clearly assigned and an ecosystem of trusted participants helps hold

the safety net, users can continue to transact business even when an individual organization's digital identity system — and trust in it — has been breached. These factors create a truly resilient digital identity.

Enable Convenient Access to Digital Services

Individuals should be able to conduct online transactions quickly and easily. Future solutions must reduce or replace the number of usernames and passwords required and prevent a confusing proliferation of second-factor options required of users.

Provide Transparency and Choice

Greater transparency and choice will require organizations to design privacy risk management into their products and empower users to take an active role in the management of their personal information. Users should have informed consent regarding the information they share, the ability to revoke that consent and control access to information, and the ability to access their information throughout their relationship with the service.

Enable Wide Availability of Authoritative Attribute Sources

Industry and federal, state and local governments are among the stewards of information that can assist in authentication and in identity proofing an individual. Organizations that maintain verified and accurate information should provide services to support attribute verification. This information must be accessible only by service providers meeting defined security and privacy protection standards, which are critical to outline in the terms of use agreed to by ecosystem participants. If done properly, this approach can reduce the number of times identity proofing is necessary by sharing specific pieces of verified information with user consent.

Increase Digital Literacy and Awareness

Users should be well educated in how their information is collected, used and shared — and the potential implications of those actions. Consumer awareness programs should help individuals understand how to create, use and maintain their digital identity, in addition to their other options and responsibilities as a digital citizen. Helping all stakeholders understand the value of stronger identity solutions and how they function will increase security while encouraging widespread adoption.

An Action Plan
to Establish Trust & Resiliency in Digital Identity

The action plan that follows will promote strong and resilient digital identity systems and help reach the aforementioned goals.

Industry will lead the development, delivery and adoption of digital identity solutions that are meaningful, convenient, secure and privacy enhancing. Government will play a supportive role to remove barriers, while also adopting industry-proven solutions for its own services.

ACTION 1
Reduce Dependency on Passwords to Provide More Intuitive and Secure Authentication

Industry and government should not create a greater authentication problem than the one that currently exists. To avoid exacerbating password fatigue by requiring additional authenticators (also known as tokens), industry and government should:[6]

- Transition from issuing authenticators to accepting authenticators a user already has and likes through decentralized identity. For example, allow users to register to their account a verified and secure authenticator, such as a mobile app or the biometric sensors available on a mobile device.
- Adopt open standards, such as Fast Identity Online, to strengthen authentication solutions that provide a path to password-less options.
- Maintain risk-appropriate levels of friction for the user — make authentication as intuitive and user friendly as possible, and as secure as necessary, for a given transaction.
- Adopt and enhance strong fraud detection capabilities where possible; robust authentication and fraud detection should go hand in hand.
- Develop and adopt authentication technologies that correspond to the current maturity of attack techniques, adapting as the threat landscape evolves.
- Offer the option to enable MFA everywhere and require MFA for services that maintain information or for services of significant value to users.
- Develop and offer national metrics, testing and reporting programs for better identity and MFA solutions, including comparability, efficacy and compliance with standards.

ACTION 2
Eliminate Identity Proofing Solutions That Are Solely Knowledge Based

Industry and government must work to adopt and encourage the development of identity proofing solutions that are both more secure and less onerous. Multiple solutions must be available that work for all segments of the population and that are able to prove comparability to other solutions. Industry and government should ensure that everyone has a chance to successfully prove their identity online.

To that end, government should encourage industry to:

- Eliminate identity proofing based solely on knowledge of information (e.g., Social Security number [SSN], password and answers to personal questions).
- Develop and adopt approaches to support identity proofing across demographic and economic boundaries, including individuals with little to no financial history.
- Partner with government at all levels, including internationally, to develop responsible information sharing agreements to expand the types of evidence that can be used to identity proof an individual.
- Collaborate across sectors to reduce repetitive identity proofing and provide services to validate the authenticity of information.
- Collaborate to deploy solutions that can facilitate more accurate detection of potential fraudulent behaviors.
- Develop and offer cross-industry metrics, testing and reporting programs for identity proofing solutions, including comparability, efficacy and compliance with standards.
- Adopt standards to share validated and verified attributes without requiring a complete identity proofing instance when minimal personal information is needed to deliver the service.

ACTION 3
Change the Use of SSNs

The SSN is an identifier, not an authenticator. Knowing a given SSN does not prove that it is the individual's SSN. As an identifier, the SSN is highly effective. It helps to delineate among, for instance, multiple people with the same name and birthdate. The SSN is a helpful tool to find key information about an individual, but the individual must prove his or her identity through other means.

As the authoritative source for SSNs, the Social Security Administration (SSA) is uniquely positioned to correct one of the greatest weaknesses in digital identity. Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018 establishes a means for organizations to validate the SSN against authoritative SSA data.[7] This process is a great step forward to thwart identity fraud.

Congress and the Administration should:

- Fully implement Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018, which empowers the SSA commissioner to expand the definition of permitted entities to include other organizations that have a need to validate an SSN.
- Discourage the use of SSNs as an authenticator within both government and industry but continue to allow the use of SSNs as an identifier.
  - » In providing identity verification services to permitted entities, SSA should specify that the information is used only for verification and identity proofing purposes and not for authentication purposes.
  - » The Administration should prohibit the use of SSNs for any authentication services offered by agencies.
- Provide options for individuals to configure how service providers can leverage their SSN and to receive alerts if their SSN has been verified by the SSA for a third party.

All entities, including government, the private sector and academia, must find new ways to authenticate individuals and adopt innovation as it becomes available to further deter SSN-related identity theft.

ACTION 4
Improve Government Support for Validating Identity Attributes and Verifying Identity Claims

Comprehensive identity proofing solutions will need to validate an individual's attributes from multiple data sources, including those managed by federal, state and local governments. Whether the source is a driver's license, passport, military ID or financial account, strong digital identity relies on access to authoritative data sources to determine that the information exists, is correct and is authentic.

To support enhanced identity proofing solutions, Congress, the Administration, and state and local governments should:

- Update laws, regulations and policies that currently prohibit government agencies from sharing data regarding identity attributes of individuals with the private sector and other public agencies. Specific attention should be paid to agencies such as SSA, the Internal Revenue Service, the Department of State, the Department of Defense and the Department of Veterans Affairs.
  - » Government attribute validation services should be limited to validating claims rather than revealing personal information. In other words, the government should, with proper privacy protections in place, offer "yes" or "no" responses to organizations' inquiries.
- Increase federation of identity across the federal government. For example, the Transportation Security Administration and Customs and Border Protection issue Pre-Check and Global Entry credentials based on rigorous identity proofing. That background check could be incorporated into federal job applications and other federal benefits and services.
- If an individual has successfully completed the Pre-Check process, he or she should not need to repeat similar portions of the process for volunteering in a child care setting or working in a health care environment.
- Develop solutions and services to validate identity claims that bind documents to document holders — for instance, use biometrics to verify that a document belongs to the person providing the document.

ACTION 5
Reduce Barriers to the Adoption of New Technologies

New categories of information (e.g., device intelligence, biometrics, behavioral analytics) can be used to assist in proofing and authenticating individuals. However, current legal and regulatory regimes may impede some companies from adopting these innovative technologies.

In consultation with private-sector and consumer groups, Congress, the Administration and state governments should:

- Provide clarifying guidance to reduce legal uncertainty around the use of new categories of information or technologies and to avoid conflicts across jurisdictions. For example, as biometrics have become near-ubiquitous, some states and countries have specified appropriate use and storage of biometric data.
- Create a communication network and repository for federal and state governments to learn about and adopt each other's technology and implementations.
- Expand guidelines, such as the National Institute of Standards and Technology (NIST)

Special Publication 800-63, that outline acceptable use and standards of care for identity proofing via digital means. These guidelines, if enacted through law or regulation, should offer states options and should not stifle innovation.

- When updating regulatory regimes, ensure that regulators work with industry to incorporate best practices in digital identity while allowing flexibility in specific implementation. This action will promote alignment of regulatory regimes, resulting in a safer, more efficient regulatory environment while allowing room for innovation.

ACTION 6
Establish a Public-Private Partnership to Focus on Implementation of Digital Identity Solutions at Scale

Digital identity affects all users of the internet and will continue to do so for the foreseeable future. To develop requirements, test and pilot solutions, and transition them into the market, the Administration should:

- Direct the Department of Commerce's NIST to advance international standardization of Special Publication 800-63 to an international standards development organization.
- Direct the National Cybersecurity Center of Excellence and IT Modernization Centers of Excellence in the General Services Administration (GSA), in collaboration with other federal agencies, to develop a "proving ground" for identity proofing solutions. NIST and GSA should leverage their existing capabilities to engage the private sector, assess the effectiveness of market innovations and rapidly transition successes throughout government agencies.
- Direct the National Science Foundation, the Networking and Information Technology Research and Development program, the Department of Homeland Security, and other research agencies to promote long-term evolution in digital identity through R&D activities in authentication and identity proofing.

ACTION 7
Enhance Privacy Through Digital Identity

Advances in digital identity must preserve and, wherever possible, enhance the current state of individual privacy. Business Roundtable supports a national consumer privacy law that champions privacy and accountability, fosters innovation and competitiveness, harmonizes regulations, and facilitates interoperability.[8]

To champion privacy in digital identity solutions, industry should:

- Build solutions that empower users with choices related to how their personal data are collected, used, processed, transferred and shared and that clearly define obligations and accountability.
- Build solutions that maximize global interoperability and enable compliance with privacy regimes.
- Take a technology-neutral, principles-based approach to allow different types of organizations to adopt appropriate risk-based privacy protections.

Policymakers should:

- Support state and municipal pilots that test decentralized identity systems to enable greater user trust and control of data. Decentralized systems can support a more appealing digital consumer experience since individuals increasingly expect and can manage greater personalization and transparency. These systems can also facilitate interoperability between existing, isolated systems through verifiable claims.[9]

ACTION 8
Bolster Digital Identity Education and Awareness

All stakeholders, including individuals, business leaders and government officials, should understand the basics of how digital identity works and what happens when users make the decision to share their information online. It is critical that users understand their rights and what companies and third-party entities intend to do with their data. Increased understanding of digital identity and its role in the digital world will encourage more widespread adoption of stronger, privacy-enhancing solutions.

The Administration and state governments should:

- Create a digital identity education and awareness initiative for individuals. The program should improve digital literacy and increase understanding of how the digital identity ecosystem works, the role of various stakeholders and how improved solutions can benefit all Americans. Many stakeholders have not yet embraced next-generation solutions because they do not understand how they function. Increased adoption of next-generation digital identity solutions will require greater understanding of the risks associated with continued usage of legacy identity proofing and authentication solutions as well as the benefits of transitioning to new approaches.

Congress should:

- Fund and direct law enforcement agencies, agency offices of the inspectors general, the Department of Homeland Security and NIST to develop outreach programs in collaboration with the National Cyber Security Alliance to educate the public and raise understanding of digital identity and digital citizenship.

Education and awareness programs are needed to promote shared understanding of digital identity challenges and solutions and enable dialogue among all stakeholders in the ecosystem.

Conclusion

Improving the state of digital identity is a national imperative.

The United States needs solutions for digital identity that are proactive and that support the enterprising and entrepreneurial spirit of the American digital economy. Governments and industry must collaborate to build a better path forward for the digital ecosystem.

This action plan builds on the lessons learned from the past and augments meaningful progress in the market. Execution of these near-term and attainable actions will bring together the necessary efforts of many entities that have a shared vision of strengthening digital identity. All organizations, large and small, public and private, can reap the benefits if these actions are taken.

Real progress requires decisive action and meaningful collaboration. Doing nothing is the biggest risk of all. By embracing this plan as a collective mission, the U.S. government and private sector can reduce fraud, protect individuals, and improve security and privacy for all.

APPENDIX

Primer on Digital Identity

This section explains the primary components of digital identity: identity proofing, authentication and federation.

Digital Identity

Digital identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service means that, for instance, every username is a unique digital identity, but the real-life identity behind the username may not be known.[10]

For the purposes of this document, there are two critical takeaways from this definition:

1. Digital identity as an online persona means that an individual can have any number of digital identities to interact online; and
2. A digital identity is always unique in the context of the service being accessed.

Digital identity also offers similar benefits to the offline world. When paying with a credit card, the store needs to know a verified attribute — that the credit card is valid. It does not need to know the user's name, address or birthdate.

Over time, most online services have trended in the opposite direction. Individuals tend to share a lot of personal information to transact — yet this broad sharing of personal information does not have to happen. With a good digital identity, an individual can assert identity (sometimes via an online third party, a credit card number, an address or a birthdate, all validated) to obtain a benefit or service without giving away more information than necessary.

In fact, digital identity can reveal even fewer attributes than transactions in the physical world, if done right. Simple technical approaches exist that allow age validation without giving away all of the information on a driver's license. A common trusted source can simply assert, for instance, that the user is older than 25 without sharing the entire date of birth — let alone name, address, height and weight.

These methods, however, have experienced slow adoption. The technological capability exists, but legal, policy and institutional barriers remain.

Identity Proofing

Some online transactions require a subject to prove identity. This requirement is no different than in physical transactions, such as walking into a bank to open an account. The process has three parts: resolution, validation and verification.

In person, a representative of the bank will typically take the applicant's driver's license and enter it into a system that looks for other accounts with that information. This process is called *resolution*.

More commonly, stores are scanning driver's licenses to *validate* them — a digital process. The difficulty comes mostly in *verification* — proving that the person presenting the evidence is actually the owner of the evidence. In the physical world, this is usually accomplished by looking at a picture on a form of identification and comparing it to the person in front of the verifier. Digital service providers have a particularly difficult time determining exactly who is on the other side of the screens, Wi-Fi and fiber optic cables.

The generic identity proofing process is depicted in Figure 1. These days, even in a physical setting, resolution and validation are typically done through digital means by the company or service provider, though the process includes physical checks such as making sure the driver's license looks and feels right.

Two forms of fraud involve identity proofing: traditional identity fraud, which involves impersonating a real-life individual (usually called identity theft), and synthetic identity fraud, which involves combining different individuals' personal information (e.g., address, birthdate and Social Security number) into a new, fictitious person. Collecting and validating personal information, or identity evidence, goes a long way toward combating synthetic identity fraud. But it does not solve traditional identity fraud. One must prove that he or she is the rightful owner of the information to stop the traditional form of fraud.

Authentication

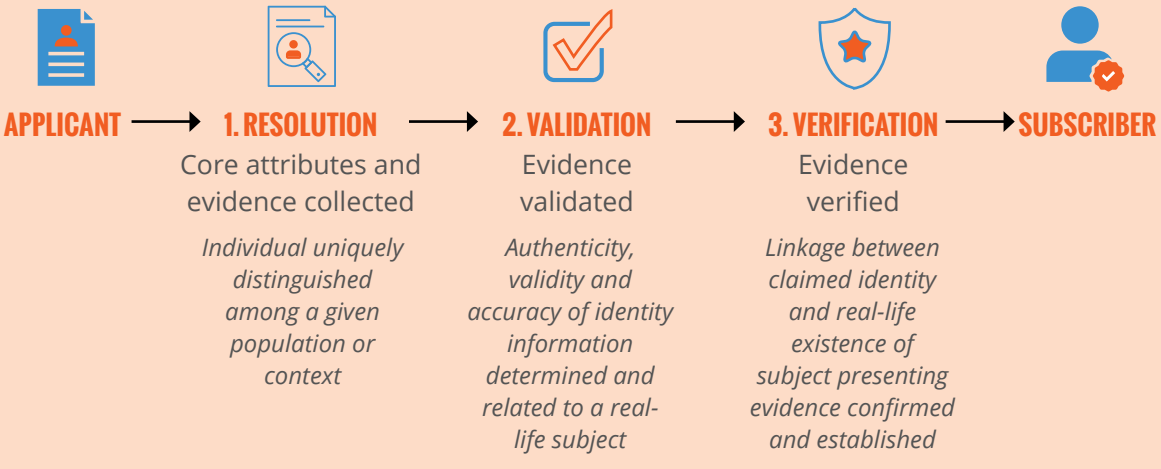
Authentication provides a means for a returning user — and only that returning user — to get back to his or her previous work. When an individual registers for an online service, he or she is usually given one or more authenticators to use from that point on. Authenticators are tools for the user to provide reasonable assurance that the same user is coming back.

Historically, the authenticator of choice has been a password. Now, organizations are moving toward multifactor authentication (MFA). MFA is familiar to Americans, though they may not know it by name. The use of an ATM with a debit card (something a user has) and a PIN (something a user knows) is a form of MFA individuals have been using for decades.

While strong authentication practices have grown at steady rate, they have not become ubiquitous. For example, widespread adoption of MFA comes with a set of challenges:

- Asking a user to download a free login application before checkout, such as an app that generates a time-based one-time code. This process adds significant user friction.
- Asking a user to purchase authentication hardware or the organization issuing that same hardware to the user. With issuance comes delay in service accessibility because the hardware, such as secure USB keys, must be shipped to the user.

FIGURE 1
GENERIC IDENTITY PROOFING PROCESS



- Creating an overload of authenticators by requiring users to have a different password and hardware or software authenticator for each site with which they interact.

Digital Identity Federation

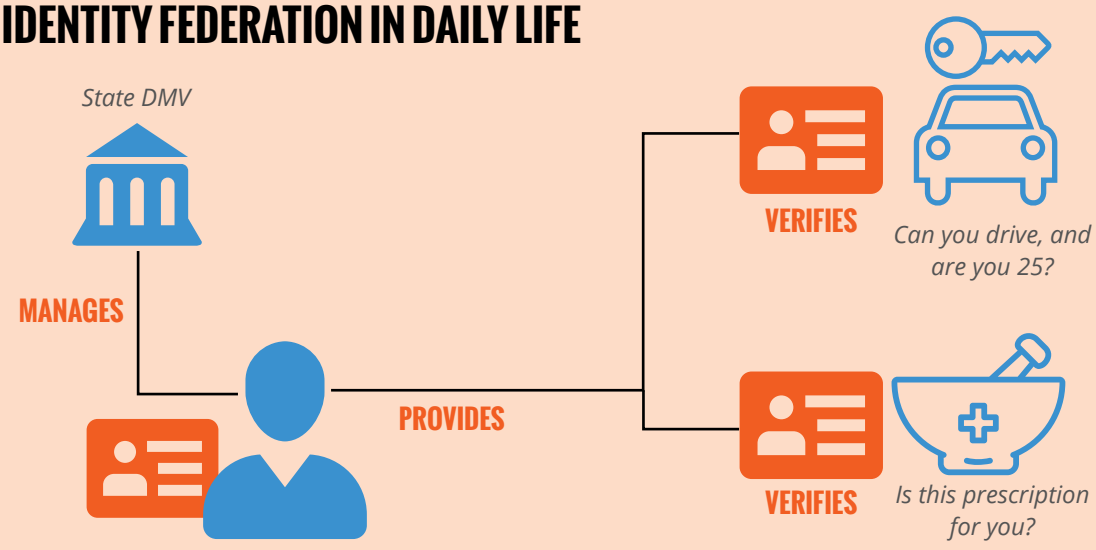
Digital identity federation allows identity information and authentication mechanisms to be shared and trusted by organizations that did not originally proof the identity or issue the authenticators. At a higher level of assurance, proofing organizations and those that establish and maintain authenticators with the user (credential service providers [CSPs] or identity providers [IdPs]) provide information on how they operate. Relying parties (RPs) or service providers (SPs), organizations that receive information from CSPs and IdPs, trust the proofing and authentication mechanisms used by the IdPs and establish rules and agreements for sharing information.

Federation is a mechanism that can reduce the number of credentials a user must remember and offers the promise of enhancing privacy by allowing a user to share verified information, but only the information deemed necessary to use a service — versus, for instance, a user needing to share a multitude of attributes with many organizations so that each organization may perform identity proofing and authentication processes. The techniques have existed for decades, but modern technologies, near-ubiquitous internet connectivity and widespread adoption of powerful consumer devices create an opportunity to bring these approaches into the mainstream.

Americans federate their identities every day. The driver's license is a great example of an individual being issued something (the license) by a third party (the Department of Motor Vehicles [DMV]) and it being accepted in many places. As depicted in the diagram below, a license asserts, "I can drive" and "I am of the required age to rent a car." The license also asserts, "I am me" and "I can buy a prescription written for me." The number of use cases for the driver's license beyond driving is vast.

The same approach is recommended for digital identity. An IdP establishes a digital identity for individuals who complete the identity proofing process. The IdP issues an authenticator to the individual or lets the individual link his or her own authenticator to the account. From that point on the individual can use that authenticator at any site that will accept it.

FIGURE 2
IDENTITY FEDERATION IN DAILY LIFE



A major consideration of federated identity approaches is managing privacy risk. Without proper protections, an IdP will know each time the user logs in to any given service. This approach could create a single entity that effectively knows everywhere a user goes on the internet. Technology measures exist that can mitigate this situation, but they must be built in from the start (often known as "privacy by design" or "by default"). Users must also be educated to understand how their personal information is being used. This situation, too, replicates the physical world, as the DMV does not know every movie theater and liquor store at which an individual shows a driver's license.

When implementing federation, it is also important to consider the potentially high governance overhead involved in setting up agreements between many parties. While some methods of federation allow dynamic registration of IdPs or SPs, each party involved — whether an IdP or an SP — must decide which organizations it trusts to either provide or receive information. The parties must also decide on the rules by which information is shared; the protocols and technical infrastructure to be used and implemented; and requirements for audits, testing and certifications.

In the consumer space, federation of digital identity for higher-risk services has seen low adoption. The solution provides clear consumer advantages — fewer logins and more personalized experiences — but businesses need to evaluate the value proposition based on their own circumstances. Traditionally, businesses claim that owning the account creation process is crucial to establish and maintain the relationship with the customer. However, that process does create a barrier for consumer acquisition. Alternatively, companies could outsource this function by adopting federated identity solutions in which they rely on credentials established through a third party. Federated identity is consumer friendly because it reduces login requirements, removes a barrier to customer acquisition, and enables customer-centric communications and marketing. It can also be business friendly by reducing the costs and effort associated with establishing and maintaining independent identity proofing and authentication. Instead, federated companies could amortize the costs across participating companies and remove the need to independently maintain specialized personnel and solutions for identity proofing and authentication. Organizations must also consider how liability is to be assigned among the parties and, critically, must develop mechanisms for redress.

Decentralized Digital Identity

Decentralized identity is an emerging archetype; unlike centralized or federated systems, decentralized systems do not rely on system owners to manage and control digital identity data. Rather, users, usually through a mobile app, are provided *attestations* of identity by various trusted organizations (trust anchors). In this way, the individual is able to control and manage his or her trusted identity data — including with whom to share the data. Decentralized identity systems are often built on distributed ledger technology and supported by a wide consortium of players.

Decentralized identity's strengths lie in giving the user more transparency and control over his or her own identity data, as opposed to traditional models in which the identity system owners generally manage not only identity management but also the relationship with the end user. Therefore, organizations must consider how a decentralized identity system changes the model for consumer engagement. Additionally, with the introduction of new technology, governance and legal models for digital identity will need to evolve.

This type of identity system is still being explored, though several pilots are ongoing across the globe.

ENDNOTES

1 Javelin Strategy & Research. (2019). Consumers increasingly shoulder burden of sophisticated fraud schemes, according to 2019 Javelin Strategy & Research study. Retrieved from https://www.javelinstrategy.com/press-release/consumers-increasingly-shoulder-burden-sophisticated-fraud-schemes-according-2019

2 Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017, June). *Digital identity guidelines* (NIST Special Publication 800-63-3). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

3 *Ibid*.

4 World Economic Forum. (2018, September). *Identity in a digital world: A new chapter in the social contract.* Retrieved from http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

5 *Ibid*.

6 Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., & Richer, J. P. (2017, June). *Digital identity guidelines: Authentication and lifecycle management* (NIST Special Publication 800-63B). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://pages.nist.gov/800-63-3/sp800-63b.html

7 Economic Growth, Regulatory Relief, and Consumer Protection Act, Pub. L. No. 115-174, § 215. Retrieved from https://www.congress.gov/bill/115th-congress/senate-bill/2155/text#toc-id300CF8635ABE45D48B8E289E6B95C4FA

8 Business Roundtable. *Framework for consumer privacy legislation.* Retrieved from https://s3.amazonaws.com/brt.org/privacy_report_PDF_005.pdf

9 World Economic Forum. (2018, September). *Identity in a digital world: A new chapter in the social contract.* Retrieved from http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

10 Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017, June). *Digital identity guidelines* (NIST Special Publication 800-63-3). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

300 New Jersey Avenue, NW
Suite 800
Washington, DC 20001

Telephone 202.872.1260
Twitter @BizRoundtable
Website brt.org

Printed on recycled paper