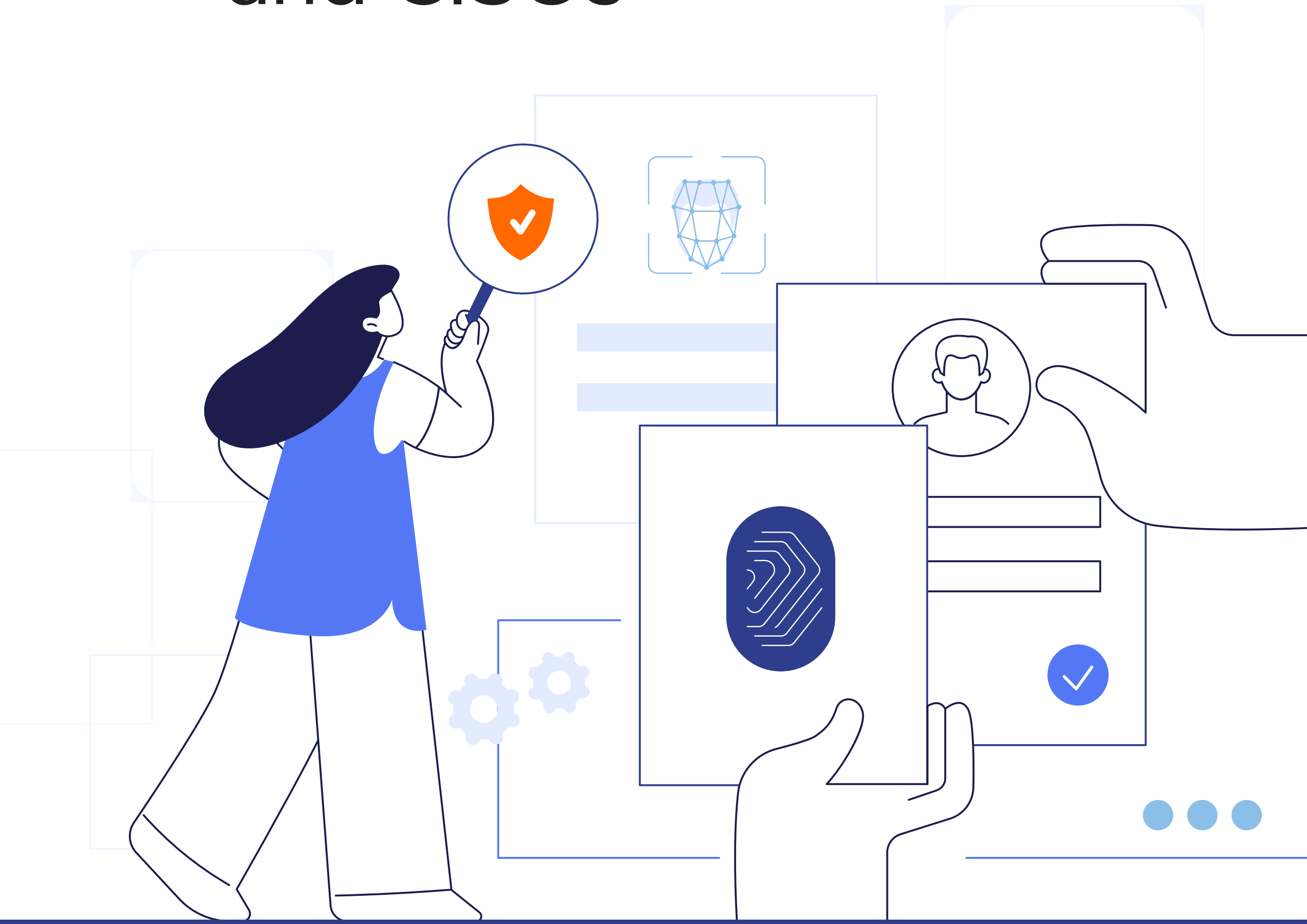
A **GOVERNMENT TECHNOLOGY** HANDBOOK | SOCURE

Digital Identity 101:

A Playbook for State and Local CIOs, CTOs and CISOs



CONTENTS

Introduction

Imagine this scenario: You apply for unemployment benefits but must wait months to receive help because your local unemployment agency can't verify your identity — even though you've sent them everything from your marriage and driver's licenses to your birth certificate as forms of verification.[1]

Or perhaps you've been displaced, and you learn your benefits are delayed because an agency can't confirm your new address, so you'll need to drive an hour to verify your identity in person.

Or maybe you work for an agency and discover that thousands of dollars in small business grants didn't go to legitimate recipients but to fraudsters who had stolen identities online.

All these scenarios are possible in state and local government today because agencies still grapple with how to create and manage digital identities.

This challenge is persistent at a time when threat actors are relentless.

Compromised digital identity is the number one attack vector in data breaches. During the pandemic, rampant fraud led to cyber criminals stealing millions in government dollars and benefits that should have gone to vulnerable constituents. In fact, there was a 2,920% increase in identity theft reports to the Federal Trade Commission (FTC) tied to government benefits during this time. In 2022 alone, identity-related data compromises across American organizations led to 422 million individual cases of stolen credentials.[2]

Synthetic identity fraud is also increasing. With this type of fraud, perpetrators use a combination of real and fake attributes to create a new fraudulent identity and access government unemployment benefits, tax refunds, stimulus checks and other funds.[3]

“As we think about government being more than a brick-and-mortar establishment — about it being a website and application that we interact with — we’ve got to think about the role of identity in that digital engagement.

— Matt Thompson, senior vice president and general manager of public sector solutions for Socure

In this evolving threat landscape — and with growing constituent demand for digital services — governments must holistically address digital identity.

The federal government realizes this. It has called for the development of a digital identity ecosystem in the latest version of the National Cybersecurity Strategy, released in March 2023.

“Enhanced digital identity solutions and infrastructure can enable a more innovative, equitable, safe and efficient digital economy. These solutions can support easier and more secure access to government benefits and services,”[4] the administration said in the strategy document.

The National Institute for Standards and Technology (NIST) maintains digital identity guidelines — NIST SP 800-63 — designed to help all levels of government properly frame and understand the technical requirements to stand up robust digital identity services intended for employees, contractors and the public.[5]

Additionally, over $1 billion tied to the American Rescue Plan Act is being used to build digital identity infrastructure, with a focus on improving data sharing, modernizing systems and increasing predictive analytics capabilities.[6]

There needs to be more movement on digital identity at the state and local levels. Identity infrastructure is now critical infrastructure, so state governments in particular must take meaningful steps.

“As we think about government being more than a brick-and-mortar establishment — about it being a website and application that we interact with — we’ve got to think about the role of identity in that digital engagement,” says Matt Thompson, senior vice president and general manager of public sector solutions for Socure, a leading provider of identity verification and fraud detection solutions.

Getting digital identity right is complicated. But if state and local governments can develop a robust digital identity strategy, they can forge a more trusting relationship with constituents and better serve them. ●

The Pressing Need for Digital Identity

Without a national standard for digital identity, state and local governments must work strategically to push digital constituent services forward.

Digital constituent services continue to be on the rise. As state and local governments digitize more services, they will need better ways to validate constituents' identities to make sure help goes to the right people at the right time.

But what exactly is digital identity?

"Digital identity is the representation of who someone is in an online ecosystem and a critical extension of their legal or physical identity," says Jordan Burris, former federal chief information officer and chief of staff at the White House Office of Management and Budget (OMB) and current vice president of public sector strategy at Socure. "It's the pieces of you, when evaluated online, that make up who you are."

A range of data points can make up a digital identity, including information such as email addresses, usernames, passwords, online search activities, and even purchasing history and behavior, says Lydia Payne-Johnson, a senior fellow at the Center for Digital Government with more than 40 years of experience in privacy, cybersecurity risk and data governance.

"Digital identities can be both a blessing and curse," Payne-Johnson adds. "Within the context of government, particularly in the U.S., we don't have a clear approach for how to manage people's information, particularly their most sensitive information. Governments are still in the 19th century in terms of some of their approaches, systems and how they handle identity."

Several other factors explain why the country hasn't matured its digital identity ecosystem.

✓ No national ID

The U.S. doesn't have a national ID, which means there isn't a government-endorsed identity system. Instead, the country has a patchwork of identity systems across federal, state and local entities.

The U.S. lags behind its counterparts in Canada, Australia, the United Kingdom, and the European Union that either have already established a digital identity ecosystem or are in the process of doing so. Australia, for example, has invested more than $600 million since 2015 on digital identity. The country has developed a "Trusted Digital

> **"We don't have a clear approach for how to manage people's information, particularly their most sensitive information. Governments are still in the 19th century in terms of some of their approaches, systems and how they handle identity.**
>
> *— Lydia Payne-Johnson, Senior Fellow, Center for Digital Government*

The public sector has traditionally focused on in-person service delivery, relying on government-issued photos and documents to verify constituents' identities.

Identity Framework," created its own digital identity system and released draft legislation that will govern this system.[7]

The Canadian government is now planning the creation of a digital credential ecosystem, which it argues is necessary to provide "easy, secure and trusted access to digital services."[8]

The gap between online and offline identity

Jeremy Grant, a leading identity expert, boils the country's identity challenges down to one fundamental problem, illustrated by a famous 1993 New Yorker cartoon featuring two dogs.

"There's two dogs on the computer and one says to the other, 'On the Internet, nobody knows you're a dog,'" Grant explains.

This message is largely still true today as more governments gradually integrate digital channels into their operations. The public sector has traditionally focused on in-person service delivery, relying on physical government-issued photos and documents to verify constituents' identities.

"We've never had the government come up with any way to close that gap between the nationally recognized authoritative credentials that exist in the physical world and the types of transactions where you often need to prove who you are in the digital world," says Grant, who formerly served as the senior executive advisor for the National Strategy for Trusted Identities in Cyberspace (NSTIC) at NIST.

With the internet revolution in the early 2000s, the public sector implemented new processes to establish identity online. These methods included one-time password tokens (OTP), SMS,

text-based pin codes and knowledge-based authentication (KBA) methods, where someone answers a series of questions related to their personal history, such as previous places they've lived and worked.

In recent years, organizations have used methods such as single sign-on through Facebook or Google to develop a federated identity via social media or email, as well as intrinsic identifiers that rely on networks to match against known values of behavior, geolocation, IP addresses and device IDs.[9] Some states have also adopted mobile driver's licenses or other portable digital credentials. Although these methods make identity transferable across a range of services and interactions, they can be exploited if implemented poorly.

This surfaces another critical issue — as the methods used to establish and verify identity online have evolved, so has the threat landscape. Brute force attacks have made OTP tokens more costly to implement and less effective. KBA methods can lead to high false rejection rates and high false acceptance rates (60%), meaning constituents who actually need access to services are denied and potential fraudsters are authenticated.[10]

"Fraud has never been more difficult to identify and stop," says Mike Cook, vice president of commercialization at Socure. "Where fraud patterns used to change annually in the 2000s and monthly in the 2010s, the 2020s have brought us intraday behavioral changes and massive fraud attacks."

✓ Identity verification is a weak link

It's clear traditional identity approaches are no longer viable in an environment where data breaches regularly happen and hackers can easily access a variety of personal information online. Identity verification is quickly becoming one of the weakest links in the chain of trust for organizations.

"Almost all government services require us to validate your identity. A digital identity gives us that level of confidence to provide services to the right people," says Ajay Gupta, chief digital transformation officer of the California DMV. "Without doing identity verification correctly, the cost of making a mistake is very high for states. It hurts not only the people who need services but also our economy."

Ralph Rodriguez — an MIT fellow, expert in applied identity intelligence, former research scientist and former head of identity verification at Facebook — says the public sector faces several challenges with identity verification. These challenges include a lack of standardized identity verification procedures, limited technological capability to detect fraudulent identity documents, and siloed databases and systems that make it difficult to verify identity across agencies.

"Identity verification frequently necessitates coordination across multiple agencies and databases, which can be complex and time-consuming to implement," Rodriguez says. ●

> **“A digital identity gives us that level of confidence to provide services to the right people.**
>
> *— Ajay Gupta, Chief Digital Transformation Officer, California DMV*

How to Build a Digital Identity Program

As agencies develop a digital identity system, they should anchor their strategy on the foundational building blocks of digital identity.

The 8 Foundational Building Blocks of Digital Identity

1. **User onboarding:** The initial phase when you collect a constituent's information, such as biographic and biometric data, to begin the enrollment or account opening process. Also known as identity verification.

2. **Progressive profiling:** The gradual collection of more information about a user as they engage with a website or application, which helps build a robust user profile.

3. **Authentication:** How an agency verifies a user's identity to grant access to systems or applications. Can involve passwords, PINs, biometric data, digital certificates, etc.

4. **Single sign-on:** An authentication method that allows a user to login into multiple applications with a single ID.

5. **User profile management:** The process by which an agency manages a collection of user profiles and oversees each user's specific permissions and access privileges for a given system or application. This component involves the complete life cycle of an identity record.

6. **Fraud detection:** Leverages artificial intelligence and machine learning-based models to identify behavioral patterns and detect anomalies that could indicate compromised identity or risk of fraud.

7. **Consent and privacy management:** The process by which an agency allows users to understand or determine what personal information they share and for what purpose.

8. **Omnichannel support:** Integrated customer service across multiple channels, including in person, online systems or phone.

Several emerging technologies are paving the way for state and local agencies to modernize their digital identity infrastructure. Each of these technologies can be effective for certain use cases but also have certain limitations.

Biometrics

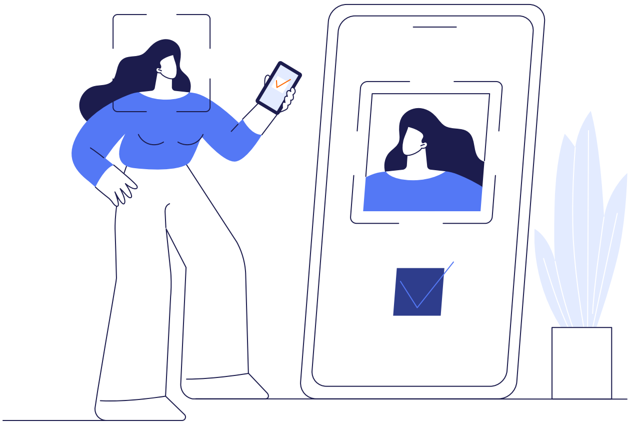
Facial recognition technology, behavioral biometrics and fingerprint scanning can be helpful to create secure digital identities and for constituents who lack a credit history. However, there are emerging bans around biometrics,[11] with concerns about impacts to privacy, ongoing surveillance, potential misuse, and the technology's ability to identify women and minorities.

Blockchain

Blockchain improves the security and accessibility of decentralized digital identities, where users have more control over their online identity, who has access to it, and with whom they share their data. Blockchain makes identity auditable, traceable and tamper-proof. One drawback of blockchain solutions, like privacy-enhancing cryptography, is the technology isn't always scalable and may negatively impact user experience.

AI and machine learning (ML)

AI/ML can accelerate verification and improve decision-making about whether to authenticate a specific individual based on specific data inputs or behavioral patterns. But there's a risk the underlying assumptions used to develop AI/ML models and algorithms may reflect the unconscious biases or preferences of the data scientists who create them, which can negatively impact equity.



Grant says technology isn't a cure-all for digital identity verification.

"Many tend to get passionate that biometrics is the answer or blockchain is the answer," he says. "I tend to look at all these things as different tools in the toolkit. Depending on what use case you're trying to solve, they may or may not play a role."

Rather than focus on technology, it's better to understand what an ideal digital identity program should look like — and how technology can help achieve this desired state.

✓ Inclusive

During *user onboarding,* the data sources used by your agency and identity verification providers should be inclusive. What authoritative and nonauthoritative sources will be used? Do these sources cater to a particular demographic or a broader range of people? For example, using credit history will unfairly exclude people who are credit-invisible, unbanked or underbanked.[12]

Moreover, user onboarding should be streamlined so that users don't have to go through the same initial proofing process multiple times. And remember that different communication channels (in

> **Your digital identity program should provide constant insight into who accesses your system and how much risk surrounds their activity.**

person, online and so on) should be designed with equity in mind for onboarding.

Research shows non-inclusive verification processes frustrate constituents and lead to high abandonment rates. In a poll of constituents from six states, more than 40% of respondents said they experienced cumbersome verification processes and had to provide additional information to confirm their identity, which led to delays in access. Two-thirds of respondents indicated government has made it difficult to verify their identity online. Thirty-five percent abandoned the verification process altogether, while 10-17% never got their identity verified when applying for benefits or services.[13]

It's not enough to make sure your verification methods are culturally sensitive and accessible to all populations regardless of race, gender, language, ability or socioeconomic background. Your agency must also consider the potential impact of identity verification requirements on marginalized communities, such as undocumented immigrants or homeless individuals, and take steps to ensure these communities are not unfairly denied access to essential public services, Rodriguez says. "When it comes to identity verification, agencies must consider equity from a variety of perspectives," he says.

Insightful

Your digital identity program should provide constant insight into who accesses your system and how much risk surrounds their activity.

Progressive profiling helps paint a clearer picture about a user. This process, which occurs after user onboarding, involves collecting information through new questions across screens as a user continues to interact with the system. Regardless of whether someone provides a Social Security number on one screen and an email address on another, you must take all these identity signals together to build a robust user profile. For instance, you can find out what device someone uses and whether that device has ever been associated with their email address.

As you collect more data, you can start evaluating behavioral patterns for risk of fraud. What if someone provides a gmail address but then quickly changes this to an email that has never been associated with the identity you've established? How much scrutiny should be applied in such a situation?

It's also wise to engage in *user profile management,* the continuous monitoring of digital identities throughout their entire life cycles. You need to regularly audit identity records, attributes and updates, as well as confirm whether accounts are dormant or deactivated. A reproofing event might need to occur if any unusual updates occur well after an identity is established.

Frictionless But Secure

Authentication — which occurs immediately after a digital identity is established through user onboarding and progressive profiling — is key to delivering a frictionless and automated user experience.

Here, a digital identity is linked to a credential (e.g., username/password or a user's smartphone) that a constituent can easily use to access services on an ongoing basis. Make sure to determine how a constituent may reengage with the system in case they lose access to the credential (i.e., a lost smartphone). And think about the implications of different multifactor authentication methods, such as a one-time passcode: A code can be phished or stolen, so verify the identity or device first and bind the identity when possible to phishing-resistant authenticators.

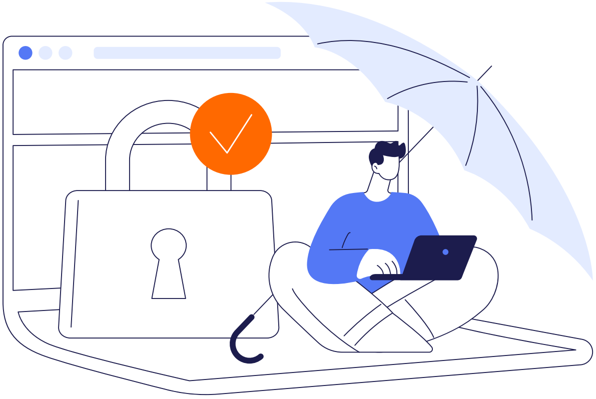
Single sign-on is also important for allowing the user to move seamlessly through a system of services. At the same time, single sign-on methods must be able to verify an identity across applications without triggering a higher risk of fraud. Single sign-on verification should not be a one-time event where someone can go anywhere they want, so identify the situations when users will need to provide further verification when accessing a new application or workflow.

Lastly, *omnichannel support* is critical to avoiding friction. Consider the linkages between online, in-person and phone experiences. Identify the ways you can verify or link identity across all three methods so that the process always leads you to the same person. It should be a fluid experience: Someone should not be told they are the right person on one channel and that they are the wrong person on another.

✓ Privacy-Focused

There is where *consent and privacy management* comes into play. No identity work should be done without the user being informed. There should be an explanation about why information needs to be provided and how it will be used. Consent should be established before data collection.

Think about what user data needs to be permanently stored for security reasons versus data that doesn't need to be retained. While some argue you don't want a database with PII, it's impossible to fight fraud effectively without some personal data.



Achieve a balance between the rights someone has to their data and the information your organization needs for practical purposes.

When crafting privacy and legal policies, chief privacy officers make great consultants. And make sure to understand what vendors are doing. Are they selling information? Are they using biometric tools, and if so, are people informed? What are the limits around storing data for fraud prevention?

Though there's no federal privacy law, agencies can anticipate potential privacy risks with digital identity solutions and craft new governance policies around data collection and storage to preserve privacy, Grant says. Grant gives the example of mobile driver's licenses, which some constituents fear states will use to track them. "There are ways you can

Include your program integrity and business teams in fraud detection. These teams will help you develop risk mitigation strategies for addressing fraud in the long run.

design it where constituents can digitally sign the data on a device that can be presented somewhere else," he says. "Identity can be validated without the state ever knowing that it was you or what it was used for. People rightfully get uncomfortable when you think about how you could be tracked, linkability between transactions or the potential for surveillance. But we know enough about how to design technology systems so that we don't have that problem."

✓ Fraud Responsive

Effective *fraud detection* involves identifying in real time when a digital identity might be under attack. The first step is to establish clear definitions for fraudulent and nonfraudulent activity for all identity-related events.

Second, you need labeling. After a user completes an identity-proofing transaction, evaluate after a period of time whether that user shows signs and characteristics of being the right or wrong person. You should be able to tag and detail any suspicious activity (e.g., account takeover). These labels will help drive your fraud strategy.

Finally, include your program integrity and business teams in fraud detection. These teams will help you develop risk mitigation strategies for addressing fraud in the long run.

✓ Tested, Proven

There are several digital identity solutions on the market, many of which claim to provide a seamless verification process that also captures a high rate of fraud.

Rather than integrate a solution based on such claims alone, your agency should prioritize solutions that offer performance-based testing and measurement. Thompson of Socure says agencies should ask about the percentage of constituents a solution can automatically identify as legitimate or fraudulent.

"Companies should be able to measure and benchmark false positives or the number of good people that you're stopping for every bad person you stop," he says.

Metrics on program integrity and total cost of ownership are also crucial. Asking about fraud capture and identification metrics can help your agency assess how accurately a solution identifies fraud.

It's particularly important to know the average number of constituents who have to go through manual review, which would require the involvement of your agency's human resources department. Your organization should also measure for disparate impact and get information from potential providers about how often people of different races, ethnicities, genders, socioeconomic backgrounds or marginalized groups encounter friction when trying to verify their digital identity. ●

Digital Identity Innovation in Action

Some states have taken great strides in developing a digital identity program, showing that governments can address the issue in multiple creative ways.

How One Florida Agency Reduced Friction and Improved Access

The Florida Department of Economic Opportunity (DEO) develops economic development, workforce development, community planning and development, and affordable housing policies and strategies to advance economic opportunities for the state's residents. DEO also distributes assistance to residents affected by unforeseen events, such as natural disasters.

During the pandemic, DEO oversaw Florida's Homeowner Assistance Fund (HAF), which was created to support residents who faced financial hardships due to the public health crisis. HAF financed several programs to provide assistance with home energy services, internet, property and flood insurance, and other related expenses, as well as money to prevent mortgage delinquencies, defaults, foreclosures and displacements. Eligible homeowners could receive up to $50,000 in assistance through HAF programs.

DEO faced the challenge of how to verify the eligibility of homeowners amid rampant government benefits fraud during the pandemic. The agency turned to an identity verification platform to streamline the onboarding process, reduce friction and combat fraud.

The platform used risk-based scoring models that analyzed a variety of identity data and user behavioral patterns to more accurately detect various types of fraud, such as synthetic identities, while also reducing false positives. To streamline the approval process, the platform leveraged ML-driven automation for document and data verification and an identity graph, or a database that links different identifiers derived from a user's various digital interactions.

With these advanced capabilities, HAF was able to process 100% of applicants, auto-approve 95% of them in less than one second and move remaining applications through an automated step-up verification process, where the system identified some applications as fraudulent.

DEO reaped several benefits from using this technology. The agency has securely disbursed more than $400 million in aid to residents. It also didn't have to assign employees to do manual reviews, reduced fraud using dynamic decisioning criteria and increased the accuracy of its identity validation processes.[14]

Advancing Equitable Access to State Services in Ohio

Since 2018, the state of Ohio has focused on building and modernizing its digital identity infrastructure.

The state has a platform called "OH|ID" that allows constituents and businesses to sign into multiple agency systems and access a range of state services from a single place. The platform incorporates single sign-on, two-factor authentication, pattern recognition to detect fraudulent activity, real-time analytics to analyze user behavior and identity proofing to create a centralized identity for users.

OH/ID also encrypts every user's personal information, providing a unique key for each user that gives them — and no one else — the ability to decrypt their information. The platform maintains users' email addresses and phone numbers but doesn't store any more data than is necessary.

"Through OH ID, we provide three and a half million Ohioans and the state's workforce with a secure, private digital identity to support their interactions with the state," says state CIO Katrina Flory. "They're empowered to control the security surrounding their accounts, and changes to their accounts are communicated to them through a verified email address. Over 1,200 agency applications are integrated with our ID solution."

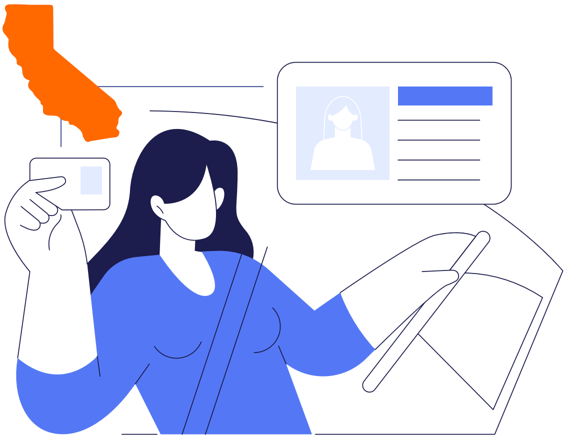
The state is now upgrading its digital identity solution so it can move its citizen accounts to the cloud and benefit from increased scalability and performance, says Remard Colston, platform administrator for InnovateOhio, an agency focused on advancing IT modernization in the state. Equity is an essential priority. The state currently uses Experian to create digital identities but plans to use more inclusive data sources once it upgrades its identity solution.

"We know there are a lot of folks who don't have a long credit history," he says. "Identity data can't be only financial. We're looking at things like driver's license data, tax records, mobile device data, and data from service providers like utility and cable companies."

As part of its RFP process, the state is asking identity providers to share various metrics, including the percentage of users it can identity proof using its current data sources. The state hopes gathering this information from vendors will help ensure that the "most people possible can leverage our services," Colston says.

Ohio looks to use digital identity to educate constituents about the services they may be eligible for. The state plans to implement a TurboTax-like questionnaire, where constituents answer questions about their background and needs so the state can match them with appropriate services.

California DMV Builds Next-Generation Digital Identity Infrastructure



The DMV is generally the first touchpoint most constituents have with government. As such, the California DMV seized the opportunity to remake the state's approach to identity.

Gupta, chief digital transformation officer of the agency, says the department is focused on maturing progressive identity — a life cycle approach to managing identity that facilitates streamlined, frictionless customer onboarding into the DMV's digital identity system, with additional checks as a user requests access to additional services. The department also uses both biometric and biographic data to validate identities based on Real ID standards.

The CA DMV has implemented identity level two assurance strategies based on NIST guidelines[15] for identity verification, or the onboarding phase in the digital identity life cycle. DMV can do this process remotely, so it uses strategies such as photo matching and liveless checking that use biometric data to establish a digital identity and provide access to a range of DMV services, including those that previously required in-person interactions.

DMV is also using mobile technologies to innovate and decentralize parts of its digital identity system. It has introduced mobile licenses and IDs, "where people can hold their identity in their digital wallet," Gupta says.

"It's consent based, meaning you get to decide when you want to use it," he says. "There is no phone home to the DMV or another state entity to get any additional information. It's a digitally signed credential sitting on your digital device. The general idea is that you put in the rigor to create that credential. After which — and this is extremely important to us from a privacy standpoint — you selectively allow for certain things to be shared depending on the use case."

The department is looking to extend these digital credentials to other paper-based credentials, such as disability placards and temporary licenses.

The CA DMV illustrates some of the methods state agencies can use to modernize their digital identity processes. With the need to comply with Real ID requirements by 2025, increased constituent demand for digital services and a heightened focus on equity, state agencies must begin to bridge the gap between physical and digital identities and create a unified identity system. ●

Digital Identity Best Practices:

A Go-Forward Plan for State and Local Governments

As your agency crafts its digital identity approach, the following best practices can provide guidance.

Follow standards

Look to the federal government for direction. The National Cybersecurity Strategy and the NIST digital identity standards are the best places to start.

The National Cybersecurity Strategy calls for greater public-private collaboration on various areas of security, including identity, while NIST is integrating more risk-based alternatives to biometric data collection into its guidelines, says Jeff Shultz, senior manager solution consulting at Socure. Agencies should track how these strategies and guidelines evolve and determine how to integrate any changes to mature their digital identity strategy. "Don't try to recreate the work yourself at the state level. That's going to be impossible," Grant says.

Take a network approach

No single agency can solve digital identity.

You need a network approach to see how fraud evolves across a broader landscape rather than at a single agency level. Fraud is constantly changing, as are the demographics of the constituent base, so you need a multiagency perspective.

State and local governments must first understand the fraud they're trying to stop by assessing their data or security analytics and creating a plan from there.

Use a unified platform

There isn't a perfect end-to-end digital identity solution. But a unified digital identity verification platform that performs authentication at the point of origination and accounts for all different forms of identity can provide a solid foundation for agencies.

The platform should use inclusive data sources to verify identity, including education, subscription-based and telecommunications information, which can boost approval rates for historically marginalized groups. Burris says agencies should look for a solution with approval rates in the 90% range.

"Many solutions have 50-70% approval rates, which means large swaths of the population experience undue friction," he says.

Fraud is constantly changing, as are the demographics of the constituent base, so you need a multiagency perspective.

An identity verification provider should also measure its solution's disparate impact, regularly assess its fraud models and include variables for any adverse effects on protected classes.

✓ Leverage the DMV and vital records

As California's example shows, the DMV relies on in-person proofing that can be successfully translated to an online context to close the digital identity gap. States could also use their vital records bureaus, which provide physical credentials such as birth and marriage certificates that can facilitate digital identity creation.[16]

Grant says modernization is necessary in many of these departments to make this happen. His group, the Better Identity Coalition, has called for more federal funding to support modernization.

"In many cases, DMVs and federal records bureaus use 14-year-old mainframe systems that aren't well suited to handling an additional workload to support things like digital credential validation," he says.

More federal funding opportunities to modernize legacy systems may be emerging. For example, the Infrastructure Investment and Jobs Act (IIJA) provides funding states and localities can use for both traditional physical infrastructure and digital infrastructure. Carefully review funding guidelines and explore multipurpose ways to use federal money for system and records modernization at the DMV and other transportation-related agencies.

✓ Stay diligent

State and local governments should constantly test their digital identity systems as they build them. They need to think like a fraudster and collaborate with providers who update their models frequently to stay ahead of changing fraud patterns. Rodriguez says governments must continue to monitor the ever-changing identity verification landscape, staying current on new technologies and industry best practices to adapt strategies.

Payne-Johnson says the stakes are high with digital identity.

"If you don't get digital identity right, you damage the government's reputation, you damage that trust," she says. "The country needs to a come-to-the-mountaintop moment about being more serious and intentional around privacy, security and identity." ●

Endnotes

1. https://www.fox17online.com/news/problem-solvers/nurse-waiting-on-16-weeks-of-uia-benefits-still-cannot-get-her-id-verified
2. https://www.idtheftcenter.org/post/2022-annual-data-breach-report-reveals-near-record-number-compromises/
3. https://www.gao.gov/assets/gao-17-708sp.pdf
4. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
5. https://pages.nist.gov/800-63-3/
6. https://www.socure.com/blog/unpack-game-changing-federal-guidance-impacting-identity-verification
7. https://www.aspi.org.au/report/future-digital-identity-australia
8. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/digital-credentials.html
9. Connect ID 2021, “Cutting-Edge Developments in IAM,” Ralph A. Rodriguez Presentation
10. Ibid.
11. https://www.biometricupdate.com/202207/facial-recognition-moratoriums-bans-and-un-bans-wash-across-the-united-states
12. https://www.consumerfinance.gov/about-us/newsroom/cfpb-report-finds-26-million-consumers-are-credit-invisible/
13. https://offers.socure.com/rs/570-ENG-578/images/Fact_Sheet_State_Polling_Results.pdf
14. https://www.socure.com/resources/casestudies/socure-idv-platform-part-of-nation-leading-homeowner-assistance-fund-program-in-florida
15. https://www.cyberark.com/resources/blog/nist-800-63-a-enrollment-and-identity-proofing
16. https://static1.squarespace.com/static/5a7b7a8490bade8a77c07789/t/63937744d04cfd3dfa8d9838/1670608710401/Better_Identity_Coalition+-+State+Blueprint+-+Dec2022.pdf

Produced by:

government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation’s only media and research company focused exclusively on state and local government and education. **www.govtech.com**

Sponsored by:

Socure

Socure is the leading provider of digital identity verification and fraud solutions. Its mission is to verify 100% of good identities in real-time and end identity fraud on the internet. Socure’s platform applies artificial intelligence and machine learning techniques with trusted online/offline data intelligence from physical government-issued documents as well as email, phone, address, IP, device, velocity, date of birth, SSN, and the broader internet to verify identities in real time. The company has more than 1,500 customers across the financial services, government, gaming, healthcare, telecom, and e-commerce industries. **socure.com**

SHUTTERSTOCK.COM/ VISUAL GENERATION