beeckcenter
social impact + innovation

DECEMBER 2023

A Guide to Identity Management

CDO Insights Brief

This document was written collaboratively by Beeck Center Fellow Milda Aksamitauskas and members of the State Chief Data Officers Network.

Many government processes—from issuing fishing licenses to processing applications for medical assistance—were originally designed around paper records and in-person interactions. Over time, many of these processes were transferred to computerized systems but were not substantively redesigned for use in the digital era. This lack of digital integration ignores part of what made the shift to digital possible: the implementation of new identity-management protocols that link a person's digital identity to various personal attributes stored in other databases.

While there are ongoing debates regarding the definition of digital identity, this guide adopts the definition provided by the National Institute of Standards and Technology (NIST) as a reference point ("The unique representation of a subject engaged in an online transaction"). Despite its limitations, NIST's definition serves as a solid starting point when assessing the identity management landscape.

When government processes integrate and are built with identity-management tools and workflows in place, everyone wins. Constituents get faster, more accurate, and more secure services. Governments save time, money, and employee hours. Both groups gain the benefit of true digitization so that digital information is collected, processed, and analyzed with less risk of identity theft.

Achieving meaningful modernization improvements to identity management systems is challenging. Various identity management solutions have been implemented by state agencies and programs without intra- or interstate coordination. This means the transition to online services isn't always smooth and accommodating, burdening some users more than others and thwarting everyone's ability to interact with the government easily or understand what their government is doing with the data it collects. Additionally, technical rules designed to keep digital identity-management systems current and secure create complex end-user requirements, including requiring users to create and remember long, complex passwords in addition to using telephone or SMS verification codes, the latter of which can create issues that affect the privacy, equity, and freedom of constituents.

Contributing Author

MILDA AKSAMITAUSKAS
Fellow,
State CDO Network

Increasingly, state chief data officers (CDOs) are getting involved in the identity management discussions. On the federal level, the U.S. Senate Homeland Security and Governmental Affairs Committee in May passed the Improving Digital Identity Act of 2023, which created an agency task force to support "reliable, interoperable digital identity verification in the public and private sectors." Additionally, several governors, including Wisconsin's Governor Tony Evers and Colorado's Governor Jared Polis, have requested their state IT teams make the user experience on government websites easier. Both governors are championing the concept of "one login," allowing states to develop a set of standards for user-identity management that can be incorporated into the hundreds of software applications used by governments both internally and externally.

While each state agency runs and designs its own websites, using a one login approach means the login credentials would be the same for any application or system using the same identity management tool. While this approach may not work for every government asset, some government services are not bound by administrative state borders. There are cities that reside in more than one state and large hospital systems that may have campuses that are only a few miles away but are in different states. People living in such communities experience firsthand the different standards and approaches when they attempt to access such services across state lines.

At first glance, all of these issues may seem like they are simply technical projects for information technology and security groups to take on and solve. However, identity management is an integral part of data infrastructure, and data leaders are often involved in such projects as well to provide strategic guidance. Finding solutions takes collaboration and work.

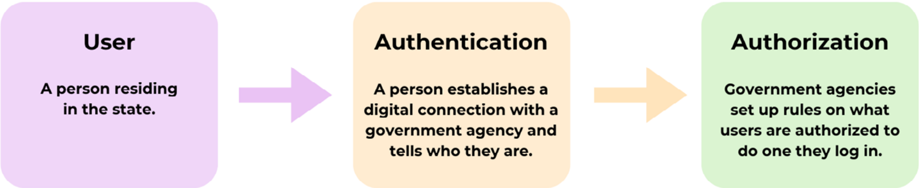
This guide incorporates insights gathered by the Beeck Center's State CDO Network working group and draws from the research of the Digital Benefits Network (DBN) on identity management and public benefits. It provides eight recommendations aimed at advancing identity management throughout various levels of government and territories in the US.

The networks have helped state CDOs shape identity management initiatives and expand the conversations around broader uses of person identifiers for measuring outcomes and providing better services. By better understanding the work and strategies currently being successfully employed, we hope data leaders can highlight the importance and implications of data infrastructure and governance in identity management initiatives in their states, agencies, and contribute to national conversations.

Master the Basics: Digital Identity Management 101

As any state CDO can confirm, mastering technical definitions is key to understanding and joining in on strategic conversations about statewide or cross-state identity-management projects. This section includes a number of terms frequently encountered by CDOs during identity-management discussions. They have been gleaned largely from the DBN's digital identity glossary and NIST's Digital Identity Guidelines.

Government digital interactions



User

A person residing in the state.

Authentication

A person establishes a digital connection with a government agency and tells who they are.

Authorization

Government agencies set up rules on what users are authorized to do one they log in.

- **A user** of a computerized system is the technical term for a person residing in a state or government entity or a business entity representative who interacts with the government through digital communication tools.

- **Authentication** is the verification of the identity of a user, process, or device. Authentication is often a prerequisite to accessing a system and its resources. From a user's perspective, authentication requires a process and protocol of setting up username and password and incorporates any accompanying password reset rules, session out times, and security requirements, among other factors. It provides verification that a returning user is the same person to whom the government site originally granted an account and access.

- **Authorization** addresses the actions a user is allowed to take once they have been approved to access certain information, resources, or functions. Government sites set up rules and protocols about what users are allowed or authorized to do once they login. For example, some users may be able to provide and update their own information while other users—designated as administrators of the site—may process cases or be authorized to unlock or delete accounts.

- **Federated access** allows organizations to link a user's identity across different identity management systems. It allows the transmission of identity data to partners inside and outside the organization. When each program or system has their own separate login, people interacting with government agencies have to keep track of every username and password they create to access government services. Federation solves this problem. It allows states to have more flexibility for varying levels of identity proofing based on the type of service people are applying for and improves security across the board.

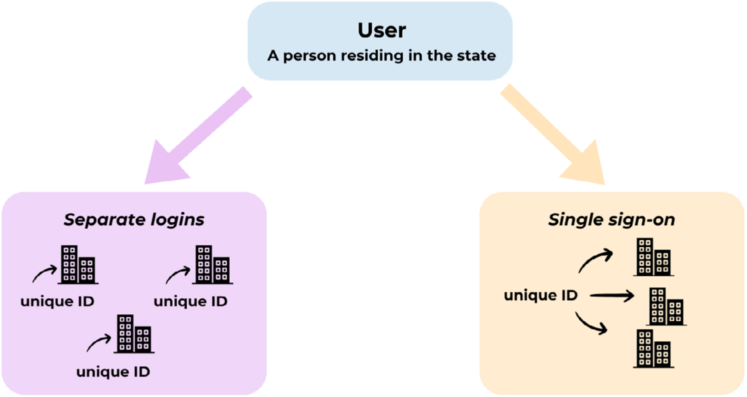
- **Single sign-on** is an authentication framework that allows users to use a single set of credentials such as a username and password to access multiple government sites. This approach allows more consistency and potentially less confusion for users. Many states have already implemented or are working on implementing single sign-on. These include:

  - **Colorado's** Governor Jared Polis in 2019 issued an executive order supporting adoption of the digital personal identification technology. In 2022 he shared a digital government strategy. Colorado's journey started with its MyColorado platform for state digital IDs, vaccination records, and parks and wildlife services digital licenses.

  - **Indiana** has a single sign-on portal, Access Indiana, for residents to access, link, and manage their online accounts related to government services.

  - **Washington** state has a SecureWashington service and offering, which is a single sign-on account for Washington residents to access government services.

  - **Wisconsin** recently launched its MyWisconsin ID initiative. The state is working on creating a single personal account for each state resident that will be used to access all government services.



Proving who you are

- **Identity proofing**, also known as **identity verification**, is a process of providing sufficient information to establish an identity. In other words, it is a validation that a user is who they say they are. It differs from in-person identity proofing in several ways.

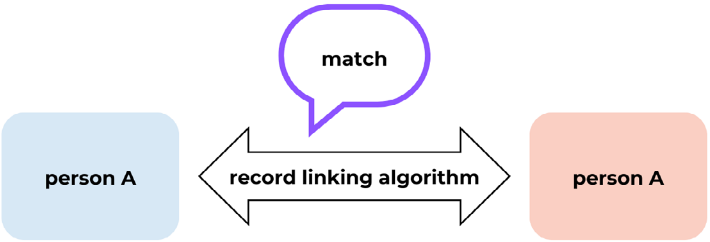
  When people apply for services in person, it doesn't matter if they show their state or federal identification card or passport at the beginning of the appointment or in the middle of the appointment. For online interactions, however, the specific moment when identity proofing happens—if it needs to happen at all—is decided and set during the digital journey process design.

  As government agencies gain more experience and maturity in designing digital services, they are learning to be more thoughtful around the need for identity proofing at all. In situations where identity proofing is necessary, experts are working to balance the need for information with when and what level of identity proofing should be inserted in the digital process. For example, a person applying for a fishing license may not need to prove their identity using biometrically-based verification. A simple upload of their driver's license number or SMS message verification may be enough.

  NIST has detailed explanations and guides for the more technical aspects of identity proofing, such as resolution, validation, verification, and various levels of assurances.

Matching records

- **Record linkage** is the administrative function and process that enables a person's identity to be used for record linking and analysis purposes. During record linkage, a set of person level identifiers from one dataset are matched against another dataset with the same person level identifiers with the goal of finding matching records for the same person in both datasets. This process is not commonly encountered by the end users during most digital interactions within government, however many CDOs are currently involved in creating and using linked datasets to analyze data from multiple sources. The process is not without challenges, though. Mistyped information, common names, twins, and name changes play a role in the performance of a record linking algorithm.



Standard setting organizations

- **International Organization of Standards** (ISO) is an international nongovernmental organization comprising national standards organizations. The group develops and publishes various standards. For example, ISO 8601 is a standard for date and time format. September 27, 2022 at 6 p.m. is represented as 2022-09-27 18:00:00.000 in ISO. By having this data convention across countries and states compatibility is never an issue between those entities that use this standard.

- **NIST** issues various standards and security frameworks including digital identity guidelines for authentication and identity proofing for users interacting with federal technology systems, including the public, employees, and contractors. As part of its work, NIST provides requirements for federal systems, which in turn influence industry solutions. The organization also provides a common way to assess the functionalities of different public and private digital identity solutions.

  State governments are not required to follow NIST guidelines, but the guidelines can offer technical and legal expertise that may not be available elsewhere. Indeed, many private sector companies also rely on the NIST guidelines given the lack of a comparable set of standards focused on private sector applications. As of the publish date of this guide NIST was expected to release its identity-management guidelines soon. NIST provided an industry briefing in July 2023 and a slidedeck presentation from that meeting is available here.

Recommendations

State executives from the State CDO Network's identity management working group recommend government data leaders consider these eight practical steps for understanding and including data considerations in statewide identity-management initiatives.

1. **Bring data leaders into identity-management discussions.**

   Chief information officers and information technology departments typically own the identity-management process, providing software, hardware, and middleware solutions for various state government platforms. Technologists should assure the availability, security, and lifecycle of those platforms and the services they provide to constituents. Since data used for record linking and identity management also have to undergo data standardization, quality checks, and lifecycle management, identity-management initiatives provide a strategic opportunity for collaboration. Partnerships between technologists and data leaders such as CDOs can help build better digital services for state residents.

2. **Prioritize public trust from the beginning.**

   With public trust in government at record lows, prioritizing transparency across government practices would likely improve the public's trust in government institutions. As such, government sites collecting data for authentication and verification should be very clear and transparent about why, how, when, and for what purposes they are collecting each data point. CDOs and other data leaders participating in identity management initiatives can help raise important questions and considerations, protecting people with different needs or circumstances such as children, the unhoused population, individuals with disabilities, and non-English speakers. Their participation can also help maximize the value of data collection and appropriate re-use of data so that government agencies can build integrated systems and track outcomes for individuals, families, and communities.

3. **Prevent bias or misinterpretation by investing in data quality.**

   Data is considered low quality when it has missing and inaccurate data attributes about people, which creates problems matching individual information for identity-management purposes. Investing in data-quality checks helps prevent bias or misrepresentation and ensures data about people is up-to-date and correct. CDOs often have data quality-improvement projects underway, which can involve demographic data used for record linkage.

Consider the case for data quality in state immunization information systems. Vaccine records are part of electronic data exchanges, providing access to consolidated patient immunization information. Patients, public health authorities, and providers depend on high quality, timely, validated data. The American Immunization Registry Association released a detailed guide on immunization record data quality, how to implement best practices, and how to onboard provider organizations, among other processes. The association's suggestions are applicable and useful for many state and local agencies.

4. **Adopt national and international data standards to increase interoperability and reduce time spent on data preparation.**

   Interoperability has always been an issue at state and local levels, and data interoperability is no different. Data elements should be compatible across programs, systems, states, and sectors—in particular the data elements that connect people's records across systems. Adopting data standards allows data analysts to spend less time preparing data for further use and helps agencies coordinate their operations and design more seamless systems.

   Wherever possible, consider ISO and NIST standards for data standards. Other organizations working on specific domain standards include:

   + The American Association of Collegiate Registrars and Admissions Officers (AACRAO) is working on interoperable **learning and employment records** (**LERs**). LERs will allow individuals to share their academic, professional, and employment data with employers and education institutions in a digital format. The AACRAO has established a competence-based education network standard and is working with higher education institutions across the U.S. to make education data interoperable.

   + The U.S. Department of Commerce Foundation is working on a data standard for jobs. **The Job Data Exchange** (JDX) is a set of open-data tools and resources that leverage global data standards. Employers can use the data standard when posting help wanted ads, highlighting skills and competencies they are looking for. Government and education institutions can use the standard, too, to confirm students have the right credentials and skills based on the description of their completed coursework.

5. **Incorporate existing administrative record-linkage practices when building identity-management solutions.**

   Engaging CDOs as strategic partners who can provide clarity and visibility about record-linkage algorithms and discuss the impacts of using certain data elements will improve the outcome of identity management solutions. Identity management solutions and data-exchange systems depend on how robust the record-linkage algorithms are when embedded in the systems. These record linkage rules and algorithms are usually invisible to the end user even though they interact with user-provided information.

   There is also potential for mismatch or bias in administrative records when not all data elements are available or simply do not match because of differing standards or poor data quality. Some examples include:

   + **Arkansas's efforts** to build robust data linkages were highlighted in an Institute of Educational Services report. The Arkansas Research Center (ARC) has developed two identity-management systems: OYSTER (Open-System Entity Resolution) system, which maintains all representations of an entity (i.e., all IDs) and generates agency-specific identifiers; and the TrustEd system, which produces privacy-protected data for research. Even with such robust systems in place, Arkansas's CDO indicated the need for constant evaluation and adjustment of the state's systems. For example, over time Arkansas data experts noticed a difficulty in matching educational records of foreign students who don't have a Social Security Number. The implications of a bias-related lack of educational record matching is that a state may not accurately estimate post-educational outcomes of students who attended its universities.

- **State background check** forms usually ask for race and gender as required data elements. Race and gender—along with name, birth date, and Social Security Number—are included in the state's record matching algorithms designed to see if there is a match between a person and the data repository of people with criminal records. Some required fields in background check services such as race and gender are problematic because they are typically assigned by law enforcement during the event that generates a criminal record, and not by individuals themselves. As a result, background check results may not include accurate information about the person of interest and may even result in individual matches that are incorrect. Yet, background checks are still used in housing, employment, and child care and have huge implications for individuals and families.

6. Facilitate statewide data-sharing and consent-management processes.

Government programs are administered by a myriad of departments and agencies and, inherently, such separations create data silos. Whether for identity management or administrative purpose data sharing, CDOs should play a critical role in finding ways to mitigate data silos and facilitate statewide data sharing agreements and frameworks. Usually only a few data elements need to be shared and this can be accomplished in a secure manner. Examples include:

- **Virginia Data Trust** (known as the "Commonwealth Data Trust") was implemented by the state's Office of Data Governance and Analytics. It provides a legally-compliant information-sharing environment among government agencies, which is governed by a standardized data-sharing agreement process. The site includes a template agreement for trust members and users, non-disclosure agreements, and dataset-readiness review guidelines. Virginia categorizes data into five tiers and applies different security standards based on each.
- **California** uses an Interagency Data Exchange Agreement (IDEA), which is signed by more than 100 state entities. The state created a playbook to help other agencies better understand this umbrella data-sharing agreement and join it. Former California CDO Joy Bonaguro wrote an article about the benefits of creating such mechanisms to share data within government agencies.
- The **Texas** Statewide Data Exchange Compact (TSDEC) is a uniform data-sharing and data-security agreement for participating Texas state agencies to share data.

The State CDO Network's Identity Management working group also emphasizes a nuanced distinction between linking data for identification purposes and sharing details of actual events in an individual's life or changes in their situation. For example, people change their first and last names for various reasons, and that new name data needs to be incorporated into existing records so systems can continue identifying the person and allow them access to their accounts. However, there should be rules and considerations around whether (and how) a life event such as a marriage, divorce, gender change, or adoption may or may not be shared among the programs. It is important to build consent-management processes into data collection and transparently list out what data may be shared and reused later that may have direct implications for individuals. An example of this type of data linkage is:

- **Washington** state has an active project related to electronic consent management for substance-use data. There is a detailed guide explaining legal aspects, exceptions, and common scenarios. The project site also has videos and brochures for health care providers and people who may need to provide consent to share their data.

7. **Find funds to sustain efforts.**

Sophisticated and sensible identity management and data exchanges cost money and require a constant stream of funds for updates and new features. CDOs should ensure partnerships among agencies or **funding sources** by sharing a common infrastructure and covering the initial and ongoing staff and tool costs. As such, data leaders should advocate for executive orders and state laws that include budget appropriations. To increase capacity further, consider federal grants or public-private partnership grants to support your state's strategies on identity management. Examples include:

- The Centers for Disease Control and Prevention (CDC) has issued more than $3 billion in grants for **public health infrastructure**. The data modernization initiative includes work on data standards and data interoperability to improve public health.
- The federal Broadband Equity, Access, and Deployment (BEAD) Program, provides more than $40 billion to expand **high-speed internet access** across the country. The funding includes an asset mapping and management component, which can improve the data infrastructure in each state.

8. **Consider innovative approaches.**

Data and technical leaders in the U.S. should look to other countries for inspiration. European Union (EU) members, for instance, have adopted electronic digital identities at various levels. The electronic identity-management community (eID) has summarized trends in the EU and highlighted each member country's approach to identity management.

EU member countries are different sizes and have different legal structures and approaches. Examples include:

- **Estonia** was the first adopter of national digital identity in 2000 and other EU members have introduced and expanded use of digital identifiers over the past 20 years. Because those who live in the EU can move between countries freely, interoperability and recognition of ID issued by disparate member states is crucial.
- **Uruguay** issued *Uruguay Digital 2025 - Resilient digital society* agenda, building on work started in 2015 when the government issued physical identification cards with chips that can be used to digitally identify Uruguayan people.
- The Institute of Technology & Society of Rio de Janeiro in **Brazil** is also working on creating a single digital identity for South Americans and Africans.
- The Better Identity Coalition, a nonprofit, cross-sector group of companies working on digital identity in the U.S., issued a Blueprint to States report that suggests using Department of Motor Vehicles (DMV) and vital records data, such as drivers licenses and birth certificates, as the basis of identity proofing. The Coalition calls on state governments to issue digital equivalents of the widely-used physical proofs of identity issued by state governments.

Conclusion

While there is much work still to be done in the field of digital identity and identity management, the groundwork has been laid. Governors are interested in identity management work, and there is recognition at the federal level that "state governments are particularly well-suited to play a role in enhancing digital identity solutions used by both the public and private sectors, given the role of state governments as the issuers of driver's licenses and other identity documents commonly used today." Given the activities, interest, and need for functional and efficient identity management in physical and digital spaces, it would be encouraging to see action from the U.S. federal government. Movement toward universal identity management, integrating the best practices from state governments, could lead to promising advancements in identity management adoption in the U.S.

Resource Recommendations

We have assembled a list of resources for anyone working at the intersection of data and identity management. It will be updated as we discover additional resources. Please email us at statecdonetwork@georgetown.edu with any additions or suggestions to this resource or to the following list:

- NIST Digital Identity Guidelines and special publications on digital identity
- Office of National Coordinator Patient Identity and Patient Records Matching
- A white paper from the American Workforce Policy Advisory Board Digital Infrastructure Working Group, September 2020
- A white paper on Interoperable Learning Records Data Transparency Working Group, September 2019
- Digital Identity page of resources on the Digital Benefits Hub
- Digital Benefits Network paper on federal actions on digital identity "Logging In and Providing Proof: A Guide to U.S. Government Actions on Digital Identity"
- Digital Benefits Network dataset and analysis on Digital Authentication and Identity Proofing in Public Benefits Applications
- OECD recommendations for governance of identity management including taking a strategic approach to digital identity and defining roles and responsibilities across the digital identity ecosystem.