

MANAGING SECURITY AND PRIVACY IN A CROSS-AGENCY COLLABORATIVE ENVIRONMENT

Identity and access management systems create a secure foundation for integrated government.



A NUMBER OF FACTORS cause information and application silos in government: politically shifting priorities that fund and deploy projects based on short-term vision as opposed to long-term architecture, lack of interoperable technologies, turf protection and political boundaries, as well as security issues. All of these contribute to the disjointed processes and services that are the hallmark of 20th-century government. In the 21st century, however, this form of governing is quickly becoming unacceptable to the citizens that government ultimately serves. Government must overcome its traditional silos to offer integrated services and holistic processes that deliver more value to its citizens and businesses. This requires interoperability among IT systems and a readiness to collaborate, share data and integrate with other agencies, and in some cases, among state and federal agencies. This is demonstrated by the increasingly important coordination among emergency responders. Doing so, however, brings about its own set of security challenges.

Although governments are expected to operate across silos, they're also

expected to protect citizen and other sensitive data. As both the provider and consumer of numerous kinds of sensitive data — Social Security numbers, tax information, health records and other personally identifiable information — government agencies are expected to meet strict regulations for limiting access to this information. Because access requirements differ among agencies, and even among staff within agencies, governance and privacy rules have complicated the process of breaking down information silos. Agencies are challenged by operational rules and legal mandates that limit internal staff's access to data. For instance, Health Insurance

the barriers to better care and efficient operations are falling in places like Louisiana, where a rural health initiative links local hospitals with the Louisiana State University Health Sciences Center in Shreveport. Now doctors at major medical institutions can view patient records from other — typically remote and rural — medical institutions in order to treat patients via telemedicine without the need for long-distance travel.

By leveraging a comprehensive identity and access management strategy, agencies can work across silos and establish relationships with trusted partners to better meet their goals. A good identity and access man-

Government privacy rules complicate the process of bridging silos. A federated approach to identity management makes appropriate information sharing possible.

Portability and Accountability Act (HIPAA) guidelines and legal protections for juvenile justice data set strict rules for information access. And the issues become even more complex for data sharing among different agencies. Security and compliance requirements — along with the fear of cost, embarrassment and public ire associated with a data breach — have kept agencies from collaborating and sharing data and systems in a way that best supports their missions. However, the public demands that government overcome these challenges for the sake of better service to constituents.

Electronic health records are a prime example of intrinsic inefficiency caused by privacy and regulatory concerns. It is clear that governments, insurance providers, and ultimately citizens, can save time and money if health records could be shared electronically with appropriate parties. As identity and access management solutions become more sophisticated,

agement solution improves security and reduces administrative burdens and costs within the organization. It also lays the foundation for secure interoperability with other agencies and trusted private-sector partners. And it allows citizens to securely access their personal information and use it to conduct transactions with government.

Establishing Rules

A mature identity and access management solution is role-based and works by defining each role based on the business rules that govern what information the user can access. When user accounts are defined by roles established by the organization, automating the management of users' identity and access privileges becomes highly leveragable. Automation of identity and access processes reduces the burden on IT and administrative staff and improves accuracy because staff is not trying to keep up with the ever-changing roles of employees or



tion secure by minimizing the need for writing down passwords.

Self-service registration and automated password reset also reduce costs associated with administrative effort and further boost convenience for users.

Flexibility Is a Must

Identity and access management systems should protect existing systems — including custom-built applications — and scale to work with systems and users that join in a federated fashion later. Standards, such as SAML (Security Assertion Markup Language), let the solutions work across platforms, organizations, applications and security systems. For an identity and access management solution to be flexible enough to grow

other users. It also allows identity and access management solutions to be applied to external users, including those in other agencies, business partners and even the general public.

For internal staff, identity and access should be defined centrally so roles and rules apply to most if not ultimately all systems in the organization. And the management system should be capable of managing user privileges throughout an employee's tenure with the agency. For instance, if an employee changes positions during his or her tenure with an agency, the employee's privileges are automatically removed and added based on job function. And if that employee quits or is terminated, all privileges can be revoked in one fell swoop.

Under a federated identity model, external users' privileges would change based on their job status within the partnering organization. And citizens are subject to their own rules as well. For instance, a revenue agency that allows users to directly access their tax accounts may require a password reset after a given

To support information sharing, an identity and access management solution should work with all existing systems, including custom applications, and scale to include other systems as users within federated organizations are added.

length of time or may even allow professional tax preparers direct access if approved by the citizen

Good for the User, Good for the Organization

An identity and access management system should make it easy for users to act securely. A single sign-on, which establishes identity with one login and allows access to all systems relevant to the user, reduces risk associated with writing down passwords for numerous applications. It also reduces help-desk demand for resetting forgotten passwords, which are typically forgotten as they become more numerous.

Single sign-on for public-facing systems provides more convenience for constituents, and like internal users, helps them keep their informa-

with the organization, it must be standards-based. Standards increase cost efficiency because organizations only need to invest once in the solution, and it will work with other standards-compliant systems going forward.

In addition, standards ease the integration and governance process involved with creating and federating identities with partnering organizations. Each organization only needs to establish its own roles and rules, and agree on what privileges those roles will be eligible for across organizational boundaries. If federation standards are in place, authentication automatically takes place at the user's home site without burdening the user with security at trusted application partners. This is key to truly integrating arm's-length systems and providing better government services. For

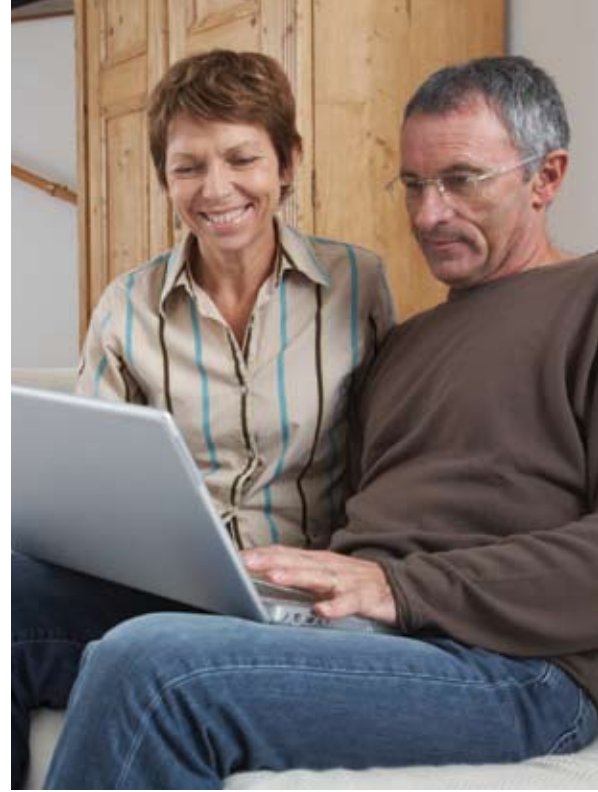
instance, a county mental health caseworker whose job function allows him to view clients' criminal histories might access that application or data from his own case record application using federation behind the scenes with the appropriate criminal justice system. And because the caseworker's role is established within his organization and in agreements made with the criminal justice agencies, the appropriate results are returned to the caseworker's case record application.

Besides being standards-based, identity and access management solutions should be modular, so the organization can use only the elements it needs and add to them later as its priorities or strategies

ing pieces that meet longer-term goals. For example, an agency may only be primarily concerned with managing identity and controlling access for internal users to start, but should be able to add an externally facing Web component later if the organization decides to allow citizens or partner organizations to access its systems.

Prove Yourself

In order to enforce compliance policies, an agency must be able to track and monitor who is accessing what information. An identity and access management solution should provide agencies with the ability to prove their IT security efforts, analyze the effectiveness of current policies and



With a modular identity and access management solution, agencies can start by addressing immediate internal security concerns and expand the solution to provide limited system access to government partners and support secure citizen transactions.

change. Additionally a modular solution lets organizations add components as their budget allows, beginning with pieces that answer urgent security needs and later add-

track who is accessing its applications and data. A solution should provide auditing and analysis tools, and in addition, alert managers when behaviors might be suspect.

In today's world, interoperability and integration of government services is a must — and these capabilities depend on the ability to securely manage access to critical information systems. The right identity and access management strategy gives governments the security they need to transform government into the integrated provider of services that citizens need and demand.



For more information call: 1-800-225-5224 or 1-800-CALL-CAI
www.ca.com/stateandlocal