Whitepaper

Building flexible and secure government services: An Identity-first guide

Table of contents

Introduction

U.S. state and local governments face mounting pressure to deliver secure digital services that match commercial experiences. How many have launched practical online portals that still provide fragmented Identity systems and legacy infrastructure, creating security gaps, frustrating residents, and straining IT resources? This ebook examines how a modern Identity foundation enables agencies to accelerate digital transformation while strengthening security and improving the resident experience.

The current landscape of state and local government digital services

Modern Identity security is the foundation for solving these challenges.

Residents increasingly expect government services to be as simple and accessible as their everyday digital experiences. Forward-thinking agencies are responding with ambitious digital transformation initiatives. Wisconsin's MyWisconsin ID, for example, received an A- rating for its innovative approach to whole-state services, enabling residents to access services offered by nearly a dozen agencies through a Single Sign-On system. At the local level, the City of Los Angeles is recognized for its citizen-centric digital transformation, improving access to city services and resources with the rollout of the Angeleno Account. Through cloud-native systems and Identity-first security, these pioneering agencies deliver faster, more personalized services that residents can access anywhere, on any device.

However, this transformation remains fragmented across the public sector. Agency silos force residents to navigate multiple login systems, repeatedly provide the same sensitive information, and manage separate accounts and credentials for different services. Legacy systems that are incapable of supporting secure, rapid information-sharing within and across agencies impose additional burdens on applicants. Additionally, complex verification processes further discourage the adoption of online services. Addressing these technological and procedural barriers will be critical to enhancing user experience, improving operational efficiency, and driving broader adoption of digital services.

Challenges agencies face

As U.S. state and local agencies prioritize the digital transformation of resident services, three fundamental challenges stand in their way:

The budget & legacy dilemma

Despite escalating cybersecurity threats and growing resident demand for better digital services, agencies face mounting budget pressures. CISOs express concerns about the sustainability of their budgets. They are often also forced to prioritize core functions like the mounting costs to maintain legacy systems over much-needed upgrades and innovation. Some agencies spend up to 80% of their IT budgets to maintain outdated systems that can't meet today's digital demands.

The great government skills gap

The workforce challenge hits state and local agencies harder than any other sector. As experienced staff approach retirement, agencies are confronting a two-sided dilemma.

- Maintaining legacy systems with diminishing expertise
- Attracting tech-savvy talent who view outdated systems and authentication processes as a red flag

Growing security and fraud risks

Legacy systems, especially those with outdated Identity controls, leave agencies increasingly vulnerable. Weak password systems and social engineering attacks have created security gaps that invite breaches and fraud. Recent Identity theft incidents in major government programs like Pandemic Unemployment Assistance (PUA) and Paycheck Protection Programs (PPP) highlight the urgent need for stronger Identity and access controls.

The agency imperatives

These priorities require a modern Identity platform that secures and connects services while adapting to evolving security requirements and resident expectations.

To drive digital transformation while ensuring security and efficiency, agencies must focus on three core priorities:

1. Modernize IT systems for security and scale

Transforming legacy infrastructure into flexible, secure platforms that support innovation and growth requires agencies to focus on:

- Deploying cloud-native solutions that enhance security and enable exceptional service delivery
- Integrating Identity management across applications to simplify access decisions and strengthen security
- Implementing automation that reduces manual overhead and accelerates deployment

2. Deliver seamless digital experiences for resident services

Consistent, secure interactions across all service channels and touchpoints means agencies can:

- Unify resident access through centralized Identity management
- Enable secure, frictionless authentication across digital services
- Provide consistent experiences across web, mobile, and in-person channels

3. Ensure privacy and reduce cyber risk

An accessible means of protecting resident data and maintaining compliance includes:

- Centralizing Identity governance that strengthens security controls
- Deploying adaptive multifactor authentication based on risk level
- Automating compliance monitoring and reporting

Importance of Identity and Access Management (IAM)

Enhanced security and trust
Modern IAM protects sensitive data through robust Identity verification and fraud prevention.

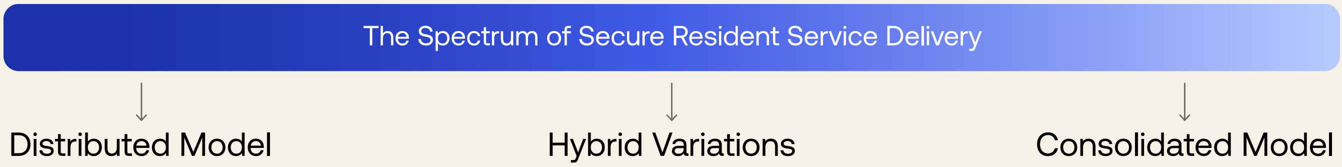
Operational efficiency
Centralized Identity eliminates silos and automates access management across systems.

Improved citizen experience
Single Sign-On delivers the seamless access citizens expect from modern government services.

Simplified compliance
Built-in controls and automated enforcement streamline regulatory compliance.

The spectrum of secure resident service delivery

Today's agencies need flexible, secure ways to deliver seamless digital experiences. A modern Identity foundation enables this transformation while maintaining security and efficiency. Across a spectrum of implementation models, two distinct approaches exist at opposite ends—fully distributed and fully consolidated—while hybrid variations offer flexible options in between.


The Spectrum of Secure Resident Service Delivery

Distributed Model

Hybrid Variations

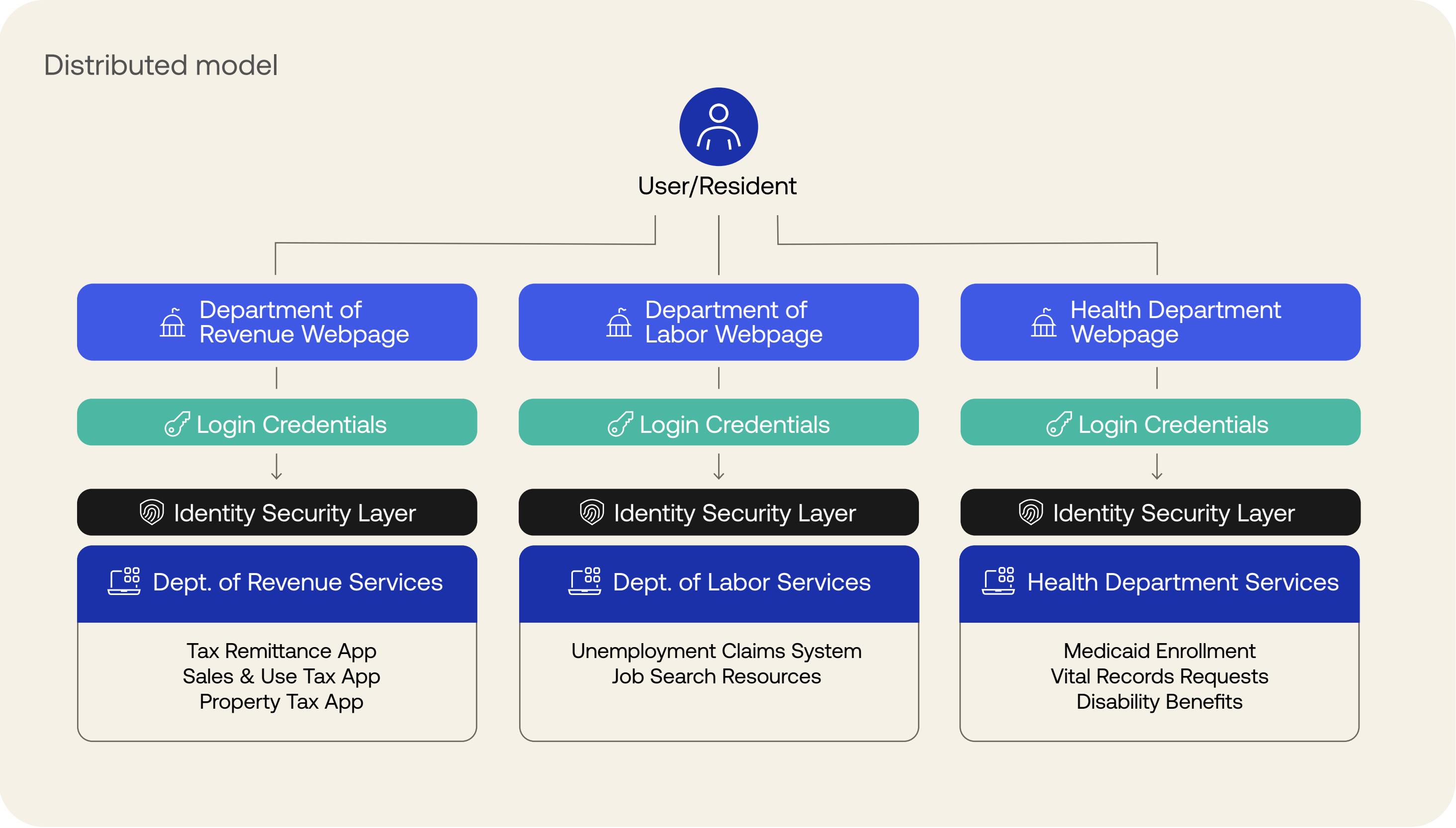
Consolidated Model

Distributed model

This approach places full responsibility for Identity security and service delivery on individual agencies. For example, a U.S. State Department of Revenue might launch an online tax platform that allows residents to file taxes, check refund statuses, and process payments—reducing the need for in-person visits while streamlining operations.

In this model, the agency has complete control over the Identity security and service delivery. However, resident identities remain siloed, with no shared authentication across other agencies. While this maximizes agency autonomy, it can create a fragmented user experience for residents accessing multiple government services.

The State's IT department provides overarching guidelines for Identity infrastructure, security, and governance, while the agency manages its portal and authentication framework.



Distributed model

Key benefits

- **Balanced governance:** Agencies maintain autonomy over their Identity solutions and services. Meanwhile, IT department guidelines ensure consistent policy enforcement, baseline security standards, and oversight.
- **Targeted risk management:** Agencies implement Identity controls suited to their threats and compliance needs, reducing risks by adhering to state-mandated security guidelines.
- **Innovation support:** Agencies modernize independently—adopting new technologies and improving digital services rapidly—enhancing resident experience without central delays.

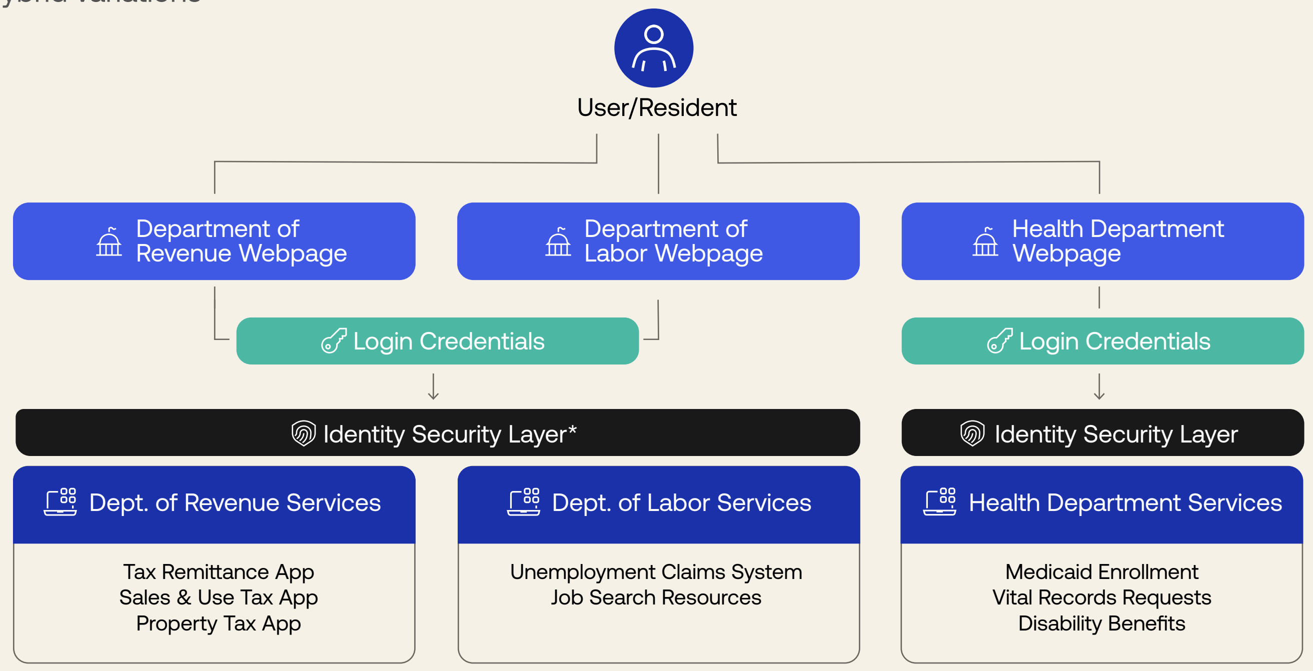
Important considerations:

- **Operational oversight:** Define clear roles and responsibilities between central IT and agency teams for Identity management and security operations.
- **Technology standards:** Establish baseline security and integration requirements that agencies must meet while maintaining flexibility for specialized needs.
- **Enterprise architecture:** Ensure the Identity platform aligns with your broader state IT modernization strategy and security framework.

Hybrid variations

Hybrid models exist along a spectrum between fully centralized and fully distributed approaches, allowing agencies to balance autonomy with a unified Identity framework. **In this model, agencies maintain their own service portals while leveraging a shared authentication layer to provide residents with secure and consistent access to government services.** Some variations allow agencies to operate separate Identity providers (IdPs) that federate with a central authentication service, while others integrate more tightly under a centrally managed platform. This approach ensures flexibility in implementation while maintaining strong security and interoperability across the ecosystem.

Hybrid variations



*These agencies may have similar security requirements, funding vehicle overlap, shared data/resources

Hybrid variations

Key benefits

- **Accelerated modernization:** Agencies can continue delivering and improving digital services through their existing portals while gradually implementing centralized Identity controls. This incremental approach allows them to leverage new IAM capabilities without disrupting established processes.
- **Risk reduction:** A shared Identity layer strengthens security and compliance across services while preserving the agency's autonomy. Uniform authentication standards help reduce vulnerabilities without forcing a one-size-fits-all solution.
- **Cost optimization:** Agencies avoid the expense of replacing functional service portals and applications while eliminating redundant Identity infrastructure.
- **Change management:** The measured approach helps overcome resistance to centralization and preserve autonomy over service delivery.

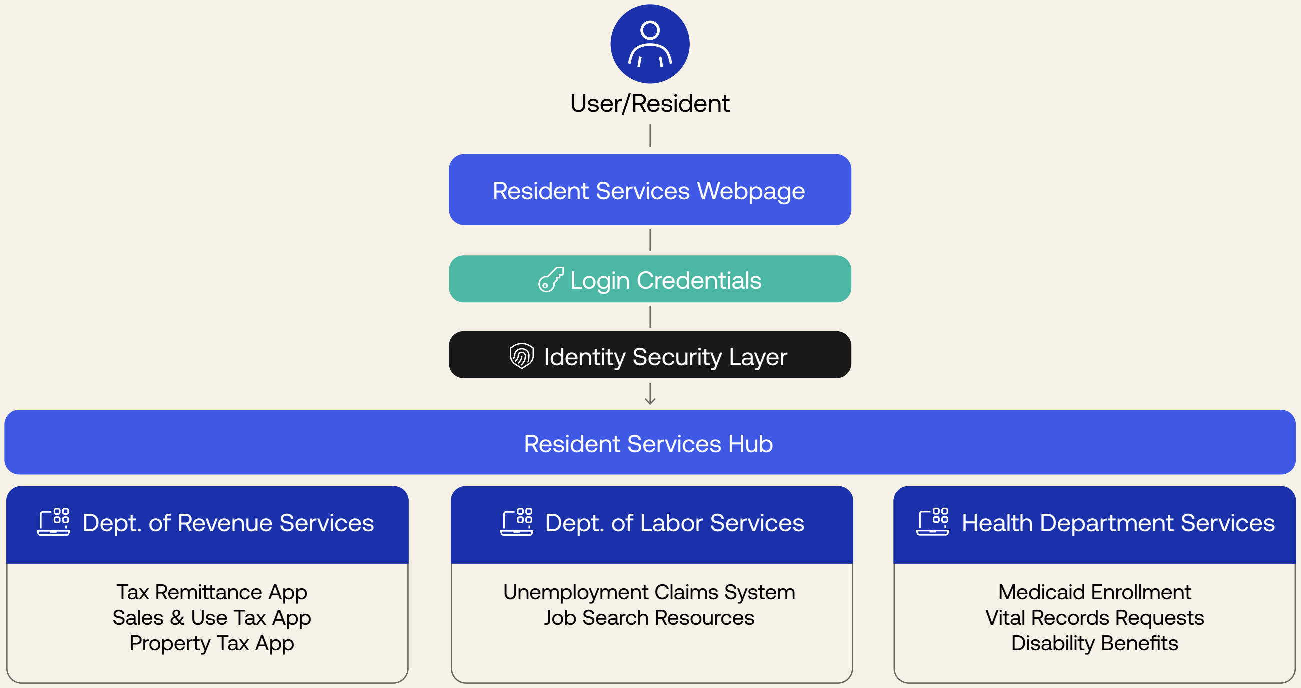
Important considerations:

- **Integration requirements:** Success depends on selecting an Identity platform with robust federation and interoperability capabilities, including support for modern and legacy systems.
- **Governance framework:** Organizations must establish clear policies for IAM, security controls, and cross-department data sharing.
- **Service coordination:** Effective communication channels and operational processes between central IT and agency teams are essential for ongoing success.

Consolidated model

A consolidated model approach provides a unified digital front door to all government services within a state or local government. **Under this model, a central IT authority creates a single, secure platform where residents can authenticate once and access services provided across multiple agencies, from vehicle registration renewals to animal services appointments.** This centralized, single-tenant Identity provider ensures consistent security standards and a seamless user experience while individual agencies continue to manage their own service delivery and authorization.

Consolidated Model



Consolidated model

Key benefits

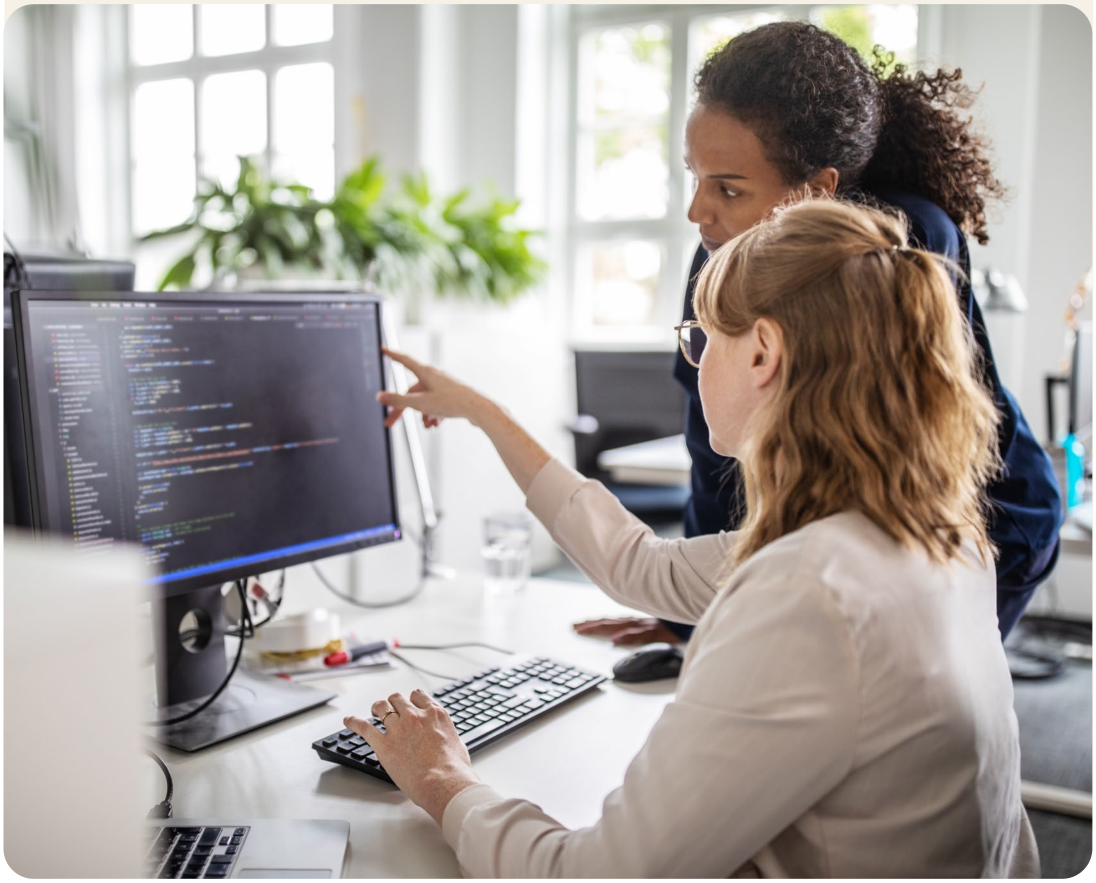
- **Enterprise-wide security controls:** Enforce consistent security policies and access controls across all agencies through centralized Identity management, reducing vulnerabilities from siloed systems.
- **Comprehensive analytics:** Gain complete visibility into service usage patterns and security events across agencies, enabling data-driven decisions about digital services.
- **Streamlined operations:** Reduce duplicate systems and administrative overhead through unified Identity, infrastructure, and automated user on-and off-boarding.
- **Enhance resident trust:** Build confidence in digital government services through consistent branding, reliable security, and a seamless single sign-on experience that simplifies access to a range of services.

Important considerations:

- **Operational resilience:** The central platform is critical—any downtime or issues can impact all services simultaneously. It’s essential to implement high availability and redundancy measures to ensure continuous operation.
- **Security posture:** Centralizing authentication creates a single point of entry, requiring robust defenses and proactive threat management to safeguard against sophisticated cyber attacks.
- **Integration complexity:** Coordinating diverse agency systems and requirements demands significant technical and organizational resources. Effective planning and collaboration are key to overcoming these challenges.

Takeaway:

State and local agencies can adopt an Identity implementation model that best aligns with their needs, digital maturity, and modernization strategy. Whether fully distributed, fully consolidated, or a hybrid approach, each model offers distinct trade-offs in cost, control, and service quality. Selecting the right approach requires evaluating the scope of services, desired outcomes, and available resources to strike the right balance between security, efficiency, and flexibility.



Okta: The modern Identity platform for government services

Identity is critical infrastructure—the vital connection between Americans and the always-on digital government services they need. Therefore, your Identity capabilities must be convenient, secure, and reliable. Even though modern access management feels like a big service challenge, it doesn't have to.

Okta ensures that your Identity management processes seamlessly address digital modernization challenges for agency security teams, employees, partners, and residents. Our central admin console, frictionless user sign-up, and provisioning workflows enable agencies to manage any user, apps, and policies.

As an independent and neutral Identity platform, Okta offers more than

7,000

integrations in the Okta Integration Network so you can securely use your applications of choice.

Including over

35

mission-critical CX tools like ServiceNow, Salesforce, Acquia, Qualtrics, Adobe, Granius, and Zoom.

With a proven foundation that has transformed digital services for hundreds of government organizations, Okta enables agencies to modernize confidently while ensuring security and resident trust. Okta's GovRAMP and FedRAMP Moderate and High Authorizations demonstrate Okta's commitment to meeting rigorous security standards for protecting resident data and digital services. Learn more about our approach at the Okta Trust Center and see it in action at okta.com/solutions/public-sector/state-and-local.