Whitepaper

Delivering public benefits and services at scale with Okta’s integration with Login.gov

Intro

Expectations to deliver top customer experiences (CX) are beginning to trickle from the commercial digital world into the public sector. Like Zero Trust, the journey to great CX involves a range in maturity levels, a rise in new teams and task forces, a balance between service-specific and cross-agency improvement efforts, and multiple federal initiatives underway.

One such initiative is Login.gov. Okta provides a secure pathway between Login.gov and digital service delivery. That pathway accelerates agencies' adoption of shared digital infrastructure, enables developers to build and connect apps more simply, and provides choice and convenience in how the American public interacts with the government.

The path to deter fraud

HISPs are identified due to the scale and impact of their public-facing services.
[Source] performance.gov/cx/assets/files/HISP-listing-2021.pdf

120

new CX hires will support cross-agency life experience projects, customer research, and service improvement activities at agencies considered HISPs.

- Current CX Strategists
- USAJobs CX openings

While a stark contrast exists between the digital services provided by the two enterprises, a misleading popular image holds that government services should operate at the scale of private-sector services. Such assumptions disregard the layers of challenges the government faces: the public's infrequent interactions with the government, the requirement to deliver vital services equitably to diverse populations, competition to attract top talent, and complex bureaucratic structures that can slow down the development and deployment of digital services, to name a few.

Recently, we've seen explosive growth in fraud targeting public benefits, identifying High Impact Service Providers (HISPs), and hiring full-time staff with CX and digital product delivery experience.[1] These trends shed light on ways the government can meet people where they are and build CX similar to the private sector.

Most recently, the government piloted and expanded digital services to provide timely access to benefits throughout the pandemic. While the U.S. federal government funded states to cover those deliverables, they had trouble curbing fraud. Outdated technology, under-resourcing, and an unprecedented volume of claims contributed to the fraud and breakdown of Unemployment Insurance (UI) systems.

[1] https://www.whitehouse.gov/omb/briefing-room/2023/03/09/fact-sheet-president-bidens-budget-improves-customer-experience-and-service-delivery-for-the-american-people/

The path to deter fraud

To understand fraud motives, means, and measures, agencies are encouraged to roll out modern Identity verification tools through new funding (Figure 1). According to the Digital Benefits Network of the Beeck Center for Social Impact and Innovation at Georgetown University, recent actions around Identity in federal-state relief programs will likely impact other benefit programs and areas of service delivery as technology systems are overhauled and new solutions are deployed.[2]

Using the Identity of another person and using fake Identity information are two fraud schemes that had a role in upwards of $60 billion in unemployment insurance fraud during an 18-month period starting April 2020. **[Source]** https://www.gao.gov/assets/gao-23-105523.pdf

Figure 1: Historic Pandemic Anti-Fraud Proposal[3]:

$600M

Investment in fraud prevention and Identity theft

$300M+

to prevent Identity theft in public benefits

$1.6B

in American Rescue Plan funds to be available to states to modernize, improve access and prevent fraud and Identity theft by June 2023

$380M

in anti-fraud grants and Identity theft prevention

[2] https://www.digitalbenefitshub.org/guide-to-us-federal-government-digital-identity?mc_cid=496965db66&mc_eid=0868fc8ed5

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-president-bidens-sweeping-pandemic-anti-fraud-proposal-going-after-systemic-fraud-taking-on-identity-theft-helping-victims/

Right-sizing modern Identity

Login.gov is the government's vision of a public Identity solution for Identity verification. It also offers a single sign-on (SSO) option to reduce the number of accounts needed to access government services. However, the additional layers of a centralized Identity model — multiple authoritative sources of Identity attributes, step-up security requirements, and planning for sudden spikes in usage[4] — require the government-shared service to pair with in-person Identity verification and cloud-native Identity platforms.

Login.gov
launched in 2017 and is a component of the U.S. General Services Administration's (GSA) Technology Transformation Services (TTS).

There's also the recognition that each department and agency is at a different maturity level when it comes to modernization efforts to improve service delivery to beneficiaries. New frameworks have emerged, including human-centered design (HCD),[5] to understand experiences from the customer's point of view, but deploying user-driven technology is easier said than done.

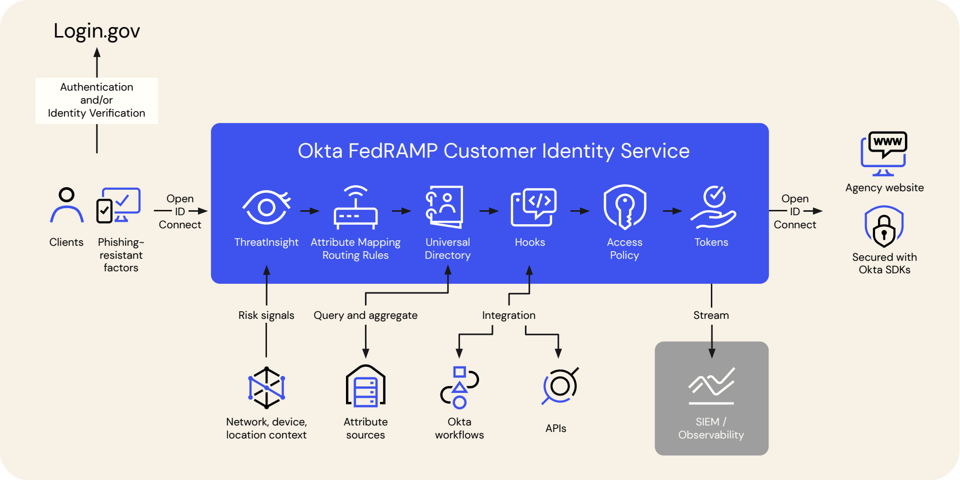
To meet the requirements of a scalable solution tailored to agencies' needs and types of technology, Okta employs the OpenID Connect (OIDC) protocol to authenticate and provision Login.gov users to Universal Directory and to integrate with applications. Using Okta Workflows, agencies can supplement users' profiles with additional attributes from authoritative sources. This consolidated user profile becomes the basis for centrally managing policy and risk level differences between agencies' applications (Figure 2). Okta secures the process using risk signals from ThreatInsight.

[4] https://fcw.com/digital-government/2023/03/planned-login-dot-gov-deployment-irs-postponed/384476/

[5] https://www.performance.gov/cx/hcd/

Right-sizing modern Identity

Figure 2: Okta's integration with Login.gov



Another important factor influencing when and how agencies decide to modernize their Identity and access management systems is understanding the radical changes to the guidelines and technology to provide privacy-protective digital Identity solutions (Figure 3).

Figure 3: Emerging authentication models, techniques, and requirements

New digital Identity initiatives	Description
The National Institute of Standards and Technology (NIST) draft of its digital Identity guidelines, 800-63[6]	This draft seeks to advance equity, emphasize optionality and choice for consumers, deter fraud and advanced threats, and address implementation lessons learned.
Mobile Driver’s Licenses (mDLs)	With mDLs, states can give every resident a tool that enables a state to “vouch” for them when they are trying to prove who they are online – by validating the information from their driver license.[7]
FIDO Passkey	Passkeys are passwordless, more secure sign-ins to websites and apps across a user’s devices, even new ones, and without having to re-enroll every device on every account. Unlike passwords, passkeys are always strong and phishing-resistant.[8]
National Cybersecurity Strategy	Strategic Objective 4.5 in the strategy makes clear, strong digital Identity solutions are vital not just for the workforce. There is a need for stronger customer or public-facing digital Identity protections as well[9].

Okta and Login.gov

If Login.gov is your preferred Identity Provider (IdP), Okta provides a streamlined, simple, and automated onboarding process for developers and a social sign-on option for government customers.

With Okta as a broker, users can add asynchronous workflows, access control policies, and additional authentication factors. The public can then authenticate with their Login.gov credentials and receive System for Cross-domain Identity Management (SCIM) or Just-In-Time (JIT) provisioning, linking the users' Login.gov account to the applications.

Get started on how to create and set up Okta with Login.gov

Figure 4: Use cases to consider Okta's integration with Login.gov

Login.gov	Scenario	With Okta	Solution Tip
Requires two-factor authentication (2FA), using a password and an additional identifier, such as a code sent via email, text message, or third-party authenticator app[9]	Missions that require a series of additional safeguards (e.g. adaptive multifactor authentication (MFA))	Provides Authentication Assurance Level 2 (AAL2) via Personal Identity Verification (PIV)/Common Access Card (CAC) smart cards, FIDO2.0/WebAuthn, and Okta FastPass: Phishing-resistant authentication for all managed devices	Integrate external risk signals from across all your security vendors to gain better visibility into potential threats. Step-up authentication or block requests only when needed to remove friction for your end users.
Enables a large population of the American public to use existing credentials to access services	Missions with a high demand/large volume of login attempts within a short timeframe	Hyperscale for Identity while throttling bad actors	Have your development team hold performance tests for x authenticated requests per minute
Provides document-based Identity proofing for higher confidence in the public's identification	Benefits enrollment services that distribute government assistance to the public	Reduced risk of fraud using Okta ThreatInsights, bot mitigation, phishing resistance, and policy requiring IAL2 Identity proofing from Login.gov	Streamline to an observability platform to provide a unified view of activity on benefits sites
Core set of user attributes,[10] including: • IAL • AAL • Names • UUID • Email • SSN (if IAL2) • DOB (if IAL2) • Phone (if IAL2)	Access decisions, personalization, and intelligence requirements for a unified record of user data scattered across multiple agencies	Extend user profile by aggregating attributes from multiple authoritative sources to unify customer account visibility	Allow government customers to govern their managed attributes in Okta while keeping attributes sourced from authoritative sources at read-only

Check out Okta Authenticator Assurance Levels, enabling administrators to create differentiated access policies for every combination of contextual access

Looking forward

Okta benefits:

- Consistent security layer throughout large, diverse organizations
- Frictionless, streamlined consumer experience
- Scalability and agility to accommodate traffic spikes
- Improved data security using a Zero Trust framework
- Seamless integration of new features and services
- Faster time to value
- Freed up developer resources to focus on non-Identity related issues

The formation of the digital Identity landscape in the U.S. has been fraught with challenges. In the early days of the internet, there was little need for digital identities beyond usernames and passwords. Fast forward to the present day, when the government and private sectors are still struggling to remain resilient to fraud and foster equity, privacy, and consumers' choice of digital Identity solutions.

Okta's vendor-neutral Identity solution can help the government avoid a patchwork of programs with varying technologies, systems, and security. Okta seamlessly integrates with on-premises and cloud resources, allowing agencies to adopt existing, federally-built technology such as Login.gov and future digital Identity technology, minimizing modernization costs and facilitating interoperability.

To learn more about Okta's integration with Login,gov, visit okta.com/logindotgov or contact us at federal@okta.com.

[6] https://csrc.nist.gov/publications/detail/sp/800-63/4/draft

[7] https://static1.squarespace.com/static/5a7b7a8490bade8a77c07789/t/63937744d04cfd3dfa8d9838/1670608710401/Better_Identity_Coalition+-+State+Blueprint+-+Dec2022.pdf

[8] https://fidoalliance.org/passkeys/

[9] https://www.okta.com/blog/2023/03/okta-applauds-new-us-national-cybersecurity-strategy/

[10] https://www.login.gov/help/get-started/authentication-options/