okta

Solutions for the Next Gen of Fraud Prevention

How to Leverage Okta's Identity Cloud as the First Line of Defense for Government Services

Connecting the right people to the right benefits: it's the cornerstone of public services. As governments race to move services online, they'll need to integrate Identity-centric security measures. It's a critical step towards protecting the personal data of the American public.

Why start with Identity?

Identity keeps information private. And an effective Identity strategy reduces the lingering threat of fraud, preparing government agencies for potential emergencies. The COVID-19 pandemic highlighted the importance of such strategies, with cyber risk threatening federal-state relief efforts and estimated fraud in the Department of Labor's Unemployment Insurance programs reaching a shocking $191 billion.

Bad actors have access to sensitive information like dates of birth and Social Security Numbers (SSN), which is why government services need additional, unified layers of protection built into their application processes. Securing identities is a pivotal component of this protection.

This datasheet will walk through the three steps that make up the foundation of a secure Identity solution:

1. Verify Identity
2. Set up pre-authorization methods
3. Enforce additional user authentication, when required

okta

Building a secure Identity solution: align trust to context

Step 1: Verify Identity

Identity verification is any method that allows the public to personally verify who they are. This is how US citizens and non-citizens will access information relevant to only them.

Examples of Identity verification:

Secure passwords: To avoid hacking attempts, ensure that users are defining passwords based on best practices for length and complexity.

Account recovery: Offer account recovery solutions for forgotten passwords. In addition, establish alerts, additional Identity verification, and/or account freezes when multiple, incorrect login attempts are made.

Step 2: Set up pre-authorization methods

Robust pre-authorization protocols use advanced technology to protect your sensitive information. By considering context, device, network, and location, you can leverage artificial intelligence and logic-based rules engines for added security.

Examples of pre-authorization:

IP Detection: Use the global IP database to identify user location, then analyze login patterns to flag unusual activity.

Anonymous Proxy Detection: Use Tor (The Onion Router) anonymizer proxies to identify and block anonymized activities or hidden locations.

Dynamic Network Zones: Leverage factors such as geolocation, IP type, or ASN to enforce a higher level of assurance or to deny authentication.

Behavior Detection: Use the detection of user behavior changes (e.g., an unusual geolocation) to drive authentication policies.

Risk Scoring: Get a complete understanding of user login context with the help of real-time intelligence.

okta

Step 3: Enforce additional user authentication, when required

Multifactor authentication (MFA) combines more than one Identity-based security measure (e.g., knowledge, possession, and/or biometric factors) to provide multiple layers of assurance. The more factors you enable, the greater your assurance (Figure 1).

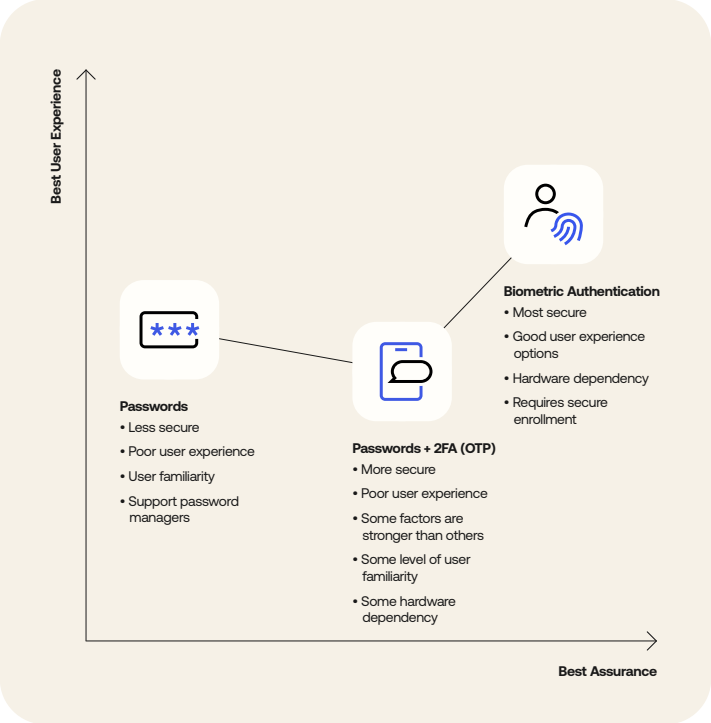


Figure 1: Two key evaluation attributes: Assurance/security which ensures only the authorized user gets access to the account, and User experience which provides a seamless registration, authentication, and recovery journey.

What happens without a secure Identity?

In a word: fraud. By some estimates, the rate of fraud and improper payments of unemployment insurance made from pandemic-related jobless aid programs exceeded 21.52 percent. This staggering number reflects the number of vulnerabilities within the public sector that bad actors can exploit. What's more, it risks the public losing trust in government platforms—an outcome that can be as harmful as data breaches themselves.

Identity attacks: Weak or nonexistent Identity protections leave government services vulnerable to synthetic Identity fraud (e.g., bad actors registering under a stolen SSN) or account takeovers that shut legitimate users out of their benefits.

Password breaches: Password-driven security policies have limited protective efficacy. The leading causes of account takeover include insecure password recovery flows, as well as the common practice of sharing and reusing passwords across different sites.

Fraud: Some legacy fraud protections offer a dangerous false sense of security. Solutions that can't provide Identity Assurance Level 2 (IAL2) Identity proofing capabilities often delay incident detection, leading to blind spots that enable fraud.

okta

Why Okta?

Okta's industry-leading Identity Cloud makes it easy to connect the American public with the services they need—securely and seamlessly. Okta is not only committed to delivering effective services today, but also to keeping up with evolving technological and governmental mandates to ensure a future-proofed Identity solution.

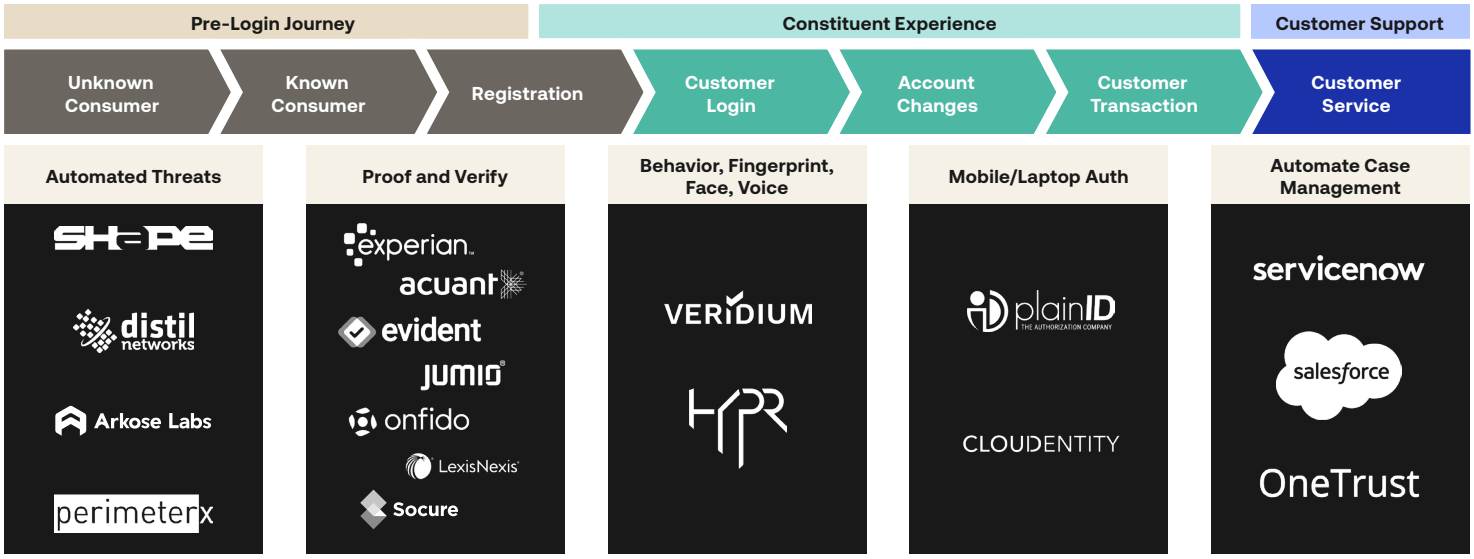
The move to digital services is well underway.

Government agencies are storing a growing number of user identities, deploying new sign-on policies, and automating the lifecycle of users in agency systems. Nationwide digital Identity standards outline the need for strong, flexible tools that ensure all this data is handled securely.

Okta's suite of Identity solutions

Okta's solution network has helped governments improve their security posture through Identity proofing, bot detection and more—in addition to deploying operational tools to improve analytics, reporting and consent management. With a large suite of pre-built integrations, the Auth0 marketplace and Okta's Integration Network (OIN) connect agencies and users to preferred applications.

Ready to learn more about how Okta can help? Visit okta.com/publicsector to get started.



About Okta
Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.