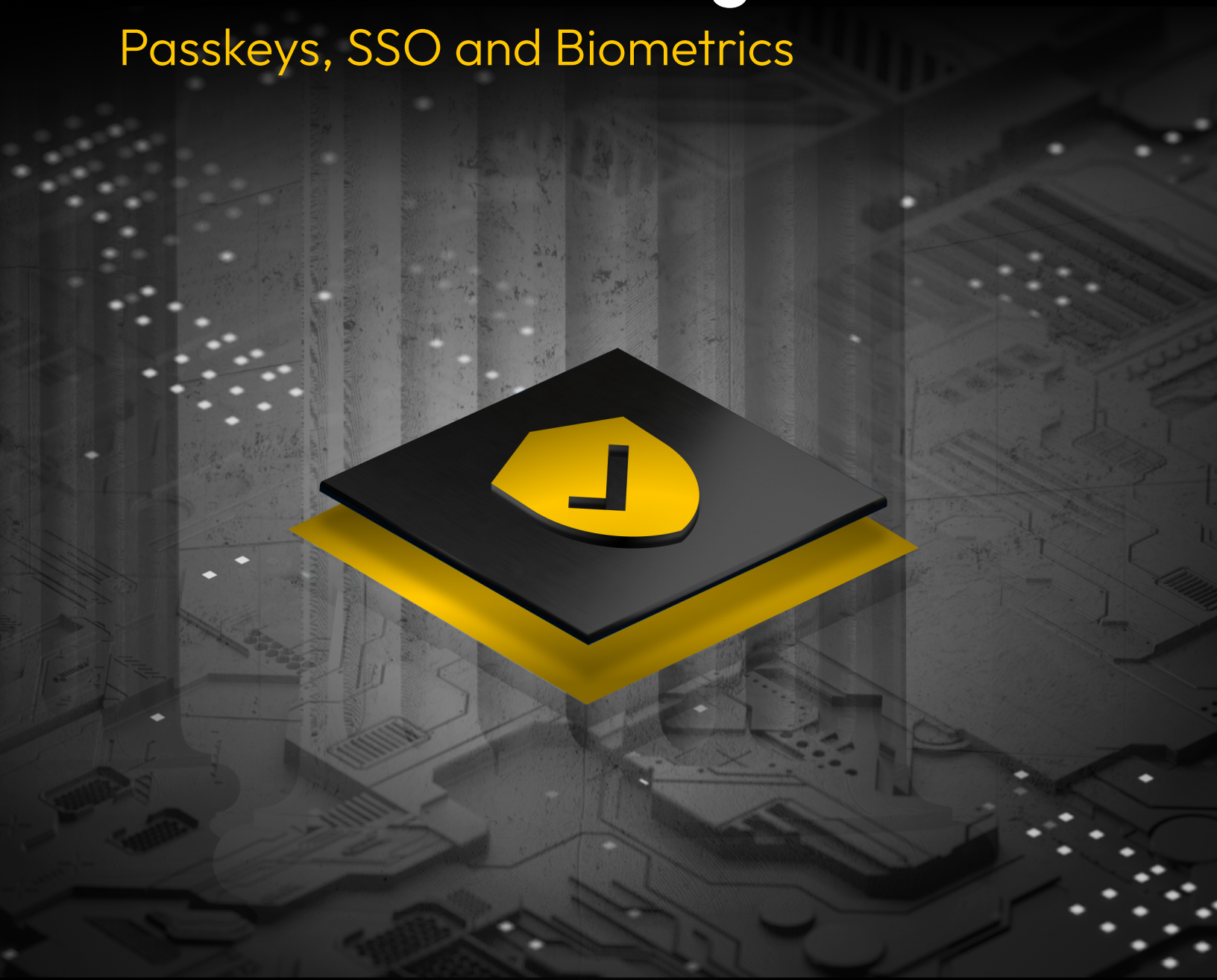
KEEPER®

Passwordless Authentication in Public Sector Organizations

Passkeys, SSO and Biometrics



What is Passwordless Authentication?

By eliminating the need for users to remember and input passwords, passwordless authentication aims to enhance both security and the user experience - reducing vulnerabilities associated with weak or reused passwords, and streamlining the login process.

Passwordless authentication is a security method that allows a user to gain access to a system without entering a traditional password. Instead, it relies on alternative means of verification such as biometric data (like fingerprints or facial recognition), hardware tokens or one-time codes sent to a trusted device.

Because of these benefits, passwordless authentication initiatives have become a top priority for government organizations of all sizes. However, many teams are wary of moving away from legacy systems due to perceived cost and user adoption barriers.

By integrating Keeper Security Government Cloud with single sign-on and biometric solutions, organizations can easily and cost-effectively achieve a fully passwordless experience for their employees.

- Keeper provides a secure digital vault that stores, manages and autofills passwords and passkeys.
- Keeper integrates with SSO providers, enabling users to access their vault records via SSO, instead of having to enter a master password.
- Keeper integrates with passwordless providers, enabling users to access their vaults without the use of a master password.

Your employees authenticate into their Single Sign-On (SSO) via biometrics (such as face scan or fingerprint). SSO allows them to access the major systems that they need. For any applications and websites that are not covered by SSO, KSGC will store, manage and autofill passkeys for authentication. This process is seamless and secure and does not require users to enter passwords.

By integrating with Keeper Security Government Cloud (KSGC) with Single Sign-On (SSO) and biometric solutions, public sector organizations can easily and cost-effectively achieve a fully passwordless experience for their employees.

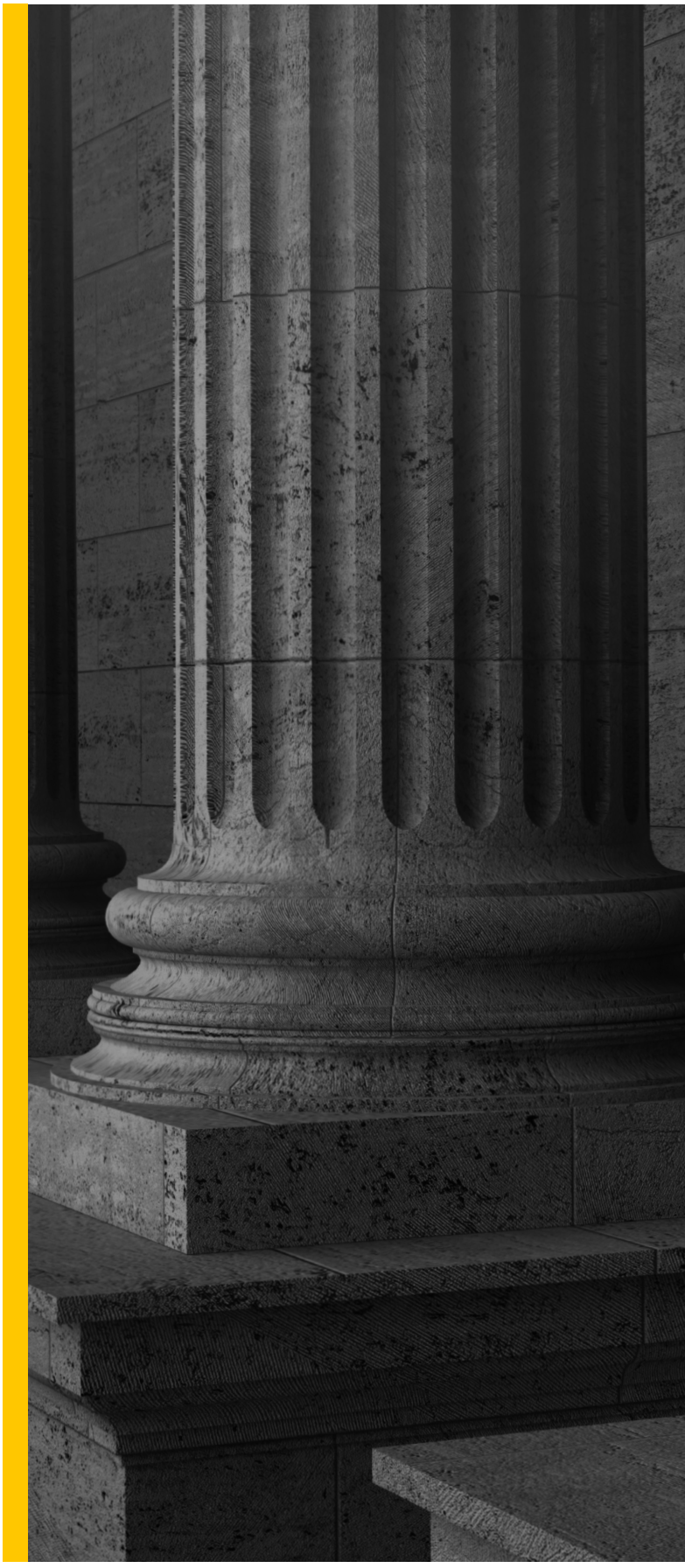
Understanding the Threat

A recent report highlights significant vulnerabilities in the password security measures of the U.S. Department of the Interior (DOI). The primary objective of the inspection was to determine the effectiveness of the Department's password management and enforcement controls in preventing unauthorized access by malicious actors.

The findings revealed that the Department's password complexity requirements and management practices were insufficient in preventing potential unauthorized access. Specifically, **21% of active user passwords, including those of senior U.S. government employees and accounts with elevated privileges, were cracked.** The Department did not consistently implement Multi-Factor Authentication (MFA), leaving 89% of its high value assets vulnerable. Furthermore, password complexity requirements within the organization were outdated, allowing users to choose easily cracked passwords. For instance, 4.75% of all active user account passwords were based on the word "password." The report also found that the Department did not promptly disable inactive accounts or enforce password age limits, leaving over 6,000 accounts vulnerable to attacks.

Password security is a significant challenge for public sector organizations due to the potential risks associated with unauthorized access. Proper identification and authentication of users are fundamental security controls for granting access to organizational systems. Passwords and credentials, being a primary target for malicious actors, play a crucial role in this process. If a cybercriminal or malicious insider compromises an account with elevated privileges, the potential harm is magnified as the attacker can upload malware, steal sensitive data, alter system configurations and change logs to hide their actions.

This report highlights vulnerabilities at a well-funded and highly technical federal agency, but these same challenges are mirrored, if not multiplied, at smaller and less-funded government organizations.



Source: P@s$w0rds at the U.S. Department of the Interior: Easily Cracked Passwords, Lack of Multifactor Authentication, and Other Failures Put Critical DOI Systems at Risk

Password Risks Greater at Small Government Agencies and Organizations

Managing employee access and enforcing password security best practices in state, local and higher education agencies presents unique challenges, especially when compared to well-funded federal agencies. These challenges are accentuated by limited budgets, diverse user populations and the need to balance security with usability.

One of the primary challenges is the sheer diversity of users in such institutions. For instance, a university might have a mix of students, faculty, administrative staff and temporary or contract workers, each requiring different levels of access to various systems. Managing and regularly updating these access privileges can be a daunting task, especially when IT resources are limited. Without a robust **Privileged Access Management** (PAM) system in place, there's a risk of granting excessive permissions, which can lead to security breaches.

Enforcing password security best practices is another significant challenge. While strong, unique passwords are essential for security, they can be hard for users to remember, leading to unsafe practices like writing passwords down or using the same password across multiple systems. Furthermore, regular password changes– while often recommended for security reasons– can lead to increased helpdesk tickets for password resets and strain already limited IT resources.

Providing a secure environment without adding friction to users' daily workflows is a delicate balance to strike. Implementing MFA, for example, greatly enhances security. However, if not seamlessly integrated, it can be seen as an inconvenience that leads to resistance from users. Similarly, while restricting access to certain websites or applications might protect against potential threats, it can also hinder productivity if employees can't access the tools they need for their work.

An Ideal Solution - From Passwords to Passwordless

Passwords are often the only security measure protecting government agencies and assets, especially on the state and municipal level. Most states dedicate less than 3% of their IT budgets to cybersecurity, as opposed to more than 10% in the private sector. Nearly half of all U.S. states lack a dedicated cybersecurity budget line item.

Many organizations are looking to get rid of passwords all together, replacing them with passwordless authentication. Passwordless authentication is a method of verifying your identity without a password. The end goals for a secure login are to determine that you are who you say you are, and that you are permitted to access the resource you are attempting to access. Passwordless authentication can achieve these goals by identifying a user with multiple factors, such as biometrics and device ownership, without having to fumble with passwords.

A typical password-based MFA or Two-Factor Authentication (2FA) login experience requires a user to enter a password followed by a second authentication factor, commonly in the form of a one-time code sent through SMS or an authenticator application. In this scenario, the password is the first factor and the one-time code is the second factor.

Passwordless authentication is a multifactor authentication system that doesn't require users to enter a password. Instead, a passwordless implementation uses other authentication factors. These can include your mobile device, an authenticator application on the device, and a process where an authenticating system establishes a cryptographic pair with the authenticator application on a user device to verify identity.

The Benefits of Passwordless Authentication

Provides unphishable security by eliminating passwords

Prevents breaches from weak and reused passwords

Replaces knowledge factors with more secure biometric and possession factors

Reduce password-related IT support costs

Provides frictionless login experience

Increases productivity

What Is a Passkey?

Passkeys are another type of passwordless authentication that is growing in popularity and adoption. In its simplest form, a passkey is a cryptographic key that lets you log in to accounts and apps without having to enter a password. Think of it as a digital version of a keycard that's stored on your phone, tablet or computer. A passkey leverages biometrics on your device, such as your fingerprint or facial recognition. Passkeys make it possible for you to log in to supported apps and accounts the same way you unlock your phone or tablet with your fingerprint or face.

Passkeys are made up of a public key and a private key, both of which are required for you to log in to an account. The public key is stored with the company you have the account with and the private key is stored locally on your device. Together, these keys authenticate who you are.

When you go to log in to an account that has passkeys enabled, the account server sends a "challenge" to the authenticator, which can be a phone, tablet, computer, web browser or password manager. The authenticator then uses the private key it has stored to solve the challenge and sends a response back. This is also known as "signing" the data, which confirms your ownership of the private key, verifies your identity and enables you to log in to your account without having to enter a password. The private key is never revealed in the login process.

Passkeys only work on websites and applications that support them. They have to be enabled in the account's security settings in order for the user to be able to log in with them. Google, Apple, Microsoft, Amazon, Best Buy, GoDaddy, PayPal, Kayak and eBay are among the major companies that support passkeys right now.

Google recently announced that not only does it support passkeys for all personal accounts across its billions of users, but it is going a step further and will make passkeys the default login setting for users.

Creating a Fully Passwordless Experience with Passkeys, SSO and Biometrics

When you use a password manager while creating a passkey, the password manager handles the passkey creation request so it can be saved to your vault. Once a passkey is stored in your password vault, you can access and use it across multiple devices, browsers and Operating Systems (OS), meaning you're not limited to logging in to an account with a passkey from a single device. An added benefit to using a password manager to store your passkeys is that you can also share it with other users, just like any other record in your vault.

While passkeys may eventually replace passwords, they won't replace password managers. Instead, password managers will become even more important. This is because passkeys are tied to an authenticator. Users have a choice as to whether to use a device – usually a smartphone, but a tablet, laptop or desktop could work – or a password manager that supports passkeys.

At first, using a smartphone as an authenticator may seem like the logical option, as most people have their phones with them all the time. However, since most people use multiple devices, this quickly becomes inconvenient. If a user wants to access an account or app on a different device, like their laptop or tablet, they would have to generate a QR code on that device, scan it with their authenticator, then use their biometrics to finally sign in.

Keeper Security Government Cloud

Keeper Security Government Cloud is a FedRAMP Authorized password manager and privileged access manager. KSGC equips organizational IT administrators with visibility and control over password and passkey security practices across the entire organization, on all devices, and enables IT admins to enhance authentication security.

Integrating passwordless authentication into KSGC provides the ultimate frictionless login experience for users.

Keeper SSO Connect

KSGC offers seamless integration with popular single sign-on solutions, such as Okta, AWS, OneLogin, Ping Identity, F5 BIG-IP APM, Google Workspace, JumpCloud and Microsoft ADFS / Azure AD to provide businesses the utmost in authentication flexibility. Keeper SSO Connect is a patented technology which allows you to quickly and securely integrate zero-knowledge password management and encryption with your existing SSO solution using standard SAML 2.0 (Security Assertion Markup Language) authentication.

Keeper SSO Connect provides secure authentication and end-to-end encryption across all of your websites, systems and applications without the need to remember a master password. Keeper is compatible with Conditional Access Policies (CAP) enforced by the identity provider, including any existing MFA solution.

If your identity provider supports passwordless login, users can choose between any available passwordless options including:

Biometric authentication

FIDO2 security keys

Passkeys

One-time passwords (OTP)

Magic links

Rules engines based on state of systems

Integrating Keeper With Passwordless Systems

Keeper connects SSO, IdP and passwordless solutions with passkey management to provide a seamless and secure login experience.

Keeper SSO Connect is a patented solution that enables users to integrate Keeper's password and passkey management capabilities with any SSO vendor using standard SAML 2.0 authentication.

Keeper SSO Connect also integrates with all popular passwordless platforms that support SAML 2.0 including Trusona, Veridium, HYPR, Secret Double Octopus, Traitware, Beyond Identity and PureID.

By combining passkey management with SSO, biometrics or both, organizations can achieve full coverage, security and control across every application and website without end users ever needing to enter a password.