Enterprise Strategy Group by TechTarget

SHOWCASE

Devising Your Enterprise Authentication Strategy: Passkey Implementations and Tradeoffs

Date: November 2022 **Author:** Jack Poller, Enterprise Strategy Group Senior Analyst

ABSTRACT: As organizations look to make authentication more efficient and secure, the idea of passwordless authentication has rapidly gained momentum. One approach organizations should consider is the use of passkeys, which modernizes authentication in a way that is beneficial to both security professionals and users. This paper looks at the benefits and challenges of different forms of passkeys and talks about what to look for in a passkey solution.

Introduction: The Changing Face of Authentication

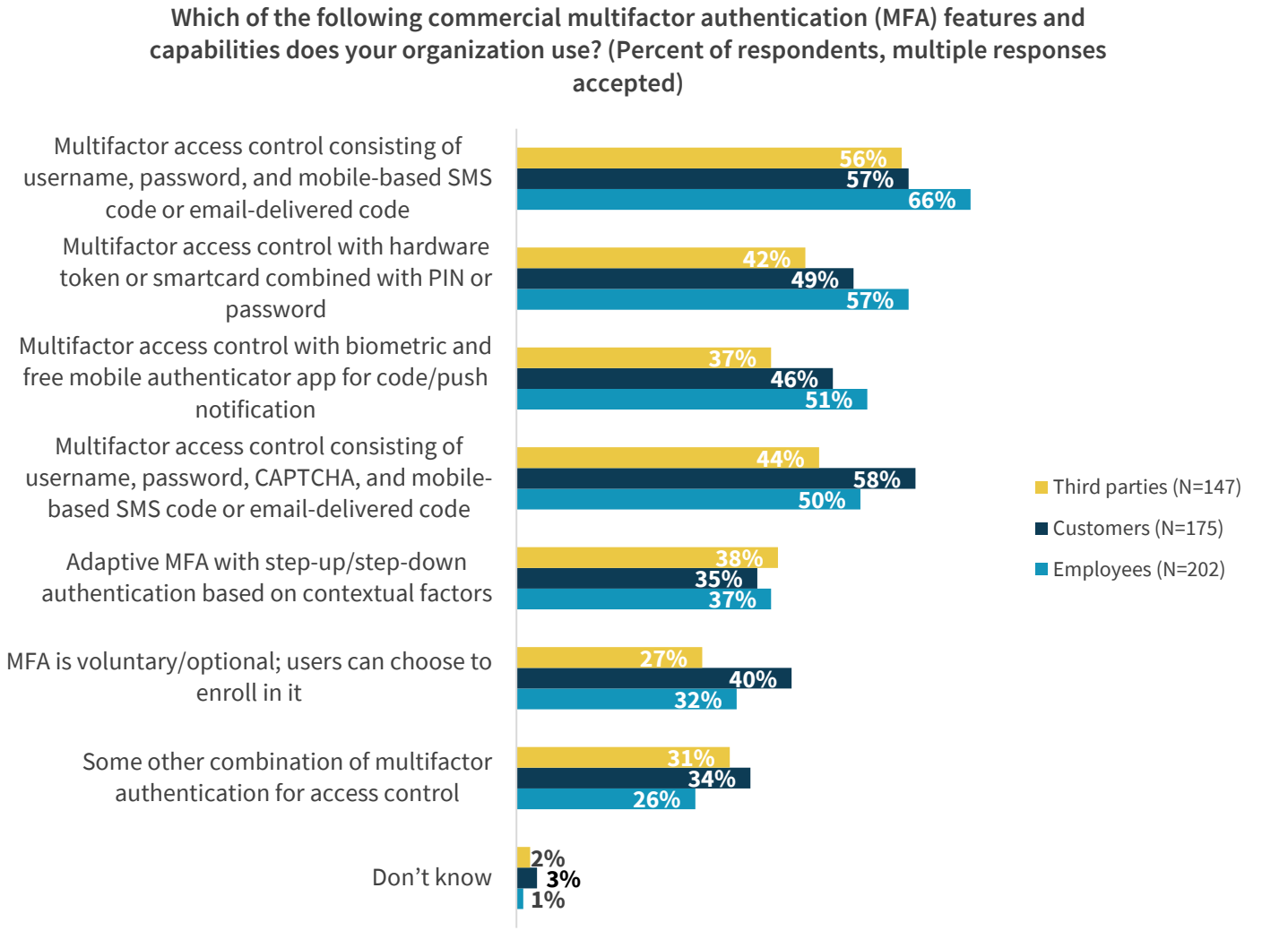
Authentication has become more challenging recently, in direct relationship to the growing complexity of security frameworks, infrastructure challenges, and emerging use cases. It also has become more difficult in the face of an increasingly sophisticated set of threat actors and expanding threat vectors, as potential points of entry increase and hackers' ability to move laterally across networks, once they gain entry via credentials theft and account takeover, becomes more pronounced.

Additionally, organizations—and their users—have had to contend with more rigid guidelines set by the cybersecurity organization on password protocols and hygiene, such as frequent password changes and the need to use complex password syntax to ward off potential credentials theft. In short, passwords no longer are sufficient for ensuring proper and safe authentication.

That's a big reason why multifactor authentication (MFA) has taken off in recent years. Research from TechTarget's Enterprise Strategy Group notes that organizations, their business partners, and their customers all are embracing a range of MFA approaches that combine usernames, passwords, mobile SMS/email codes, and hardware security keys. However, the research also points out that many organizations fail to make MFA participation a firm requirement for their users (see Figure 1).[1]

[1] Source: Enterprise Strategy Group Research Report, *Securing the Identity Perimeter with Defense in Depth*, May 2022. All Enterprise Strategy Group research references and charts are from this research report.

Figure 1. MFA Is Prevalent for All Human Identities



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Clearly, organizations and users are trying to address the authentication challenge by moving away from passwords. In fact, Enterprise Strategy Group research notes that passwordless security techniques are key to organizations' efforts to improve authentication effectiveness and efficiency, as 65% of organizations say passwordless authentication is either their top identity-related activity or one of their top three priorities (see Figure 2). Their reasoning is well founded. According to Enterprise Strategy Group research, password authentication has had a significant positive impact on:

- Increasing IT and security efficiency (63%).
- Improving user experience (57%).
- Reducing risk (56%).

As a result, it's not surprising that passwordless solutions and processes are now becoming—and in many cases, already have become—strategic initiatives.

Figure 2. Passwordless Authentication Is Becoming Strategic

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

There is little doubt that organizations are accelerating their efforts to replace—not just augment—passwords as the principal method of creating secure access. Until fairly recently, there weren't a lot of good options that obviated the need for passwords. And for consumers, the move to passwordless has been slow due to ease and familiarity with passwords and for ease of account recovery. But passwordless technologies have made big advances in usability, easy deployment, and efficiency for both security teams and users in recent years. And one of the most interesting passwordless authentication solutions is passkeys.

The Benefits of Passkeys

While most security decision makers, if not all, understand the limitations and challenges of password-based authentication, moving away from passwords was difficult for a long time because of a perceived lack of suitable alternatives. Non-password-based solutions were often tricky to deploy and less than fully reliable, or they created friction for the users. And many initial MFA implementations still used passwords to some degree, since other passwordless options may not have been available for many organizations. The benefit of passkeys is that it now makes phishing-resistance available to everyone, whether they are enterprises or consumers.

The evolution of passkeys (FIDO-based credentials), however, represents a major leap forward for consumers and organizations looking to sever long-standing ties with passwords. Using widely available and widely accepted public key encryption technology, passkeys can be implemented and deployed in different formats, depending upon the unique needs of organizations and individual users.

Passkeys and Devices

Passkeys are automatically stored for the user in a high-security vault on a trusted device or using a software-based authenticator. While passkeys can be backed up or copied and used on multiple devices, authenticators may be tied to a single device. Copyable passkeys are suitable for consumers desiring ease of use and flexibility.

Single-device passkeys are restricted to storage on a single device and cannot be copied to other devices. This provides high assurance to enterprises that the passkey cannot be compromised or used if the device is lost.

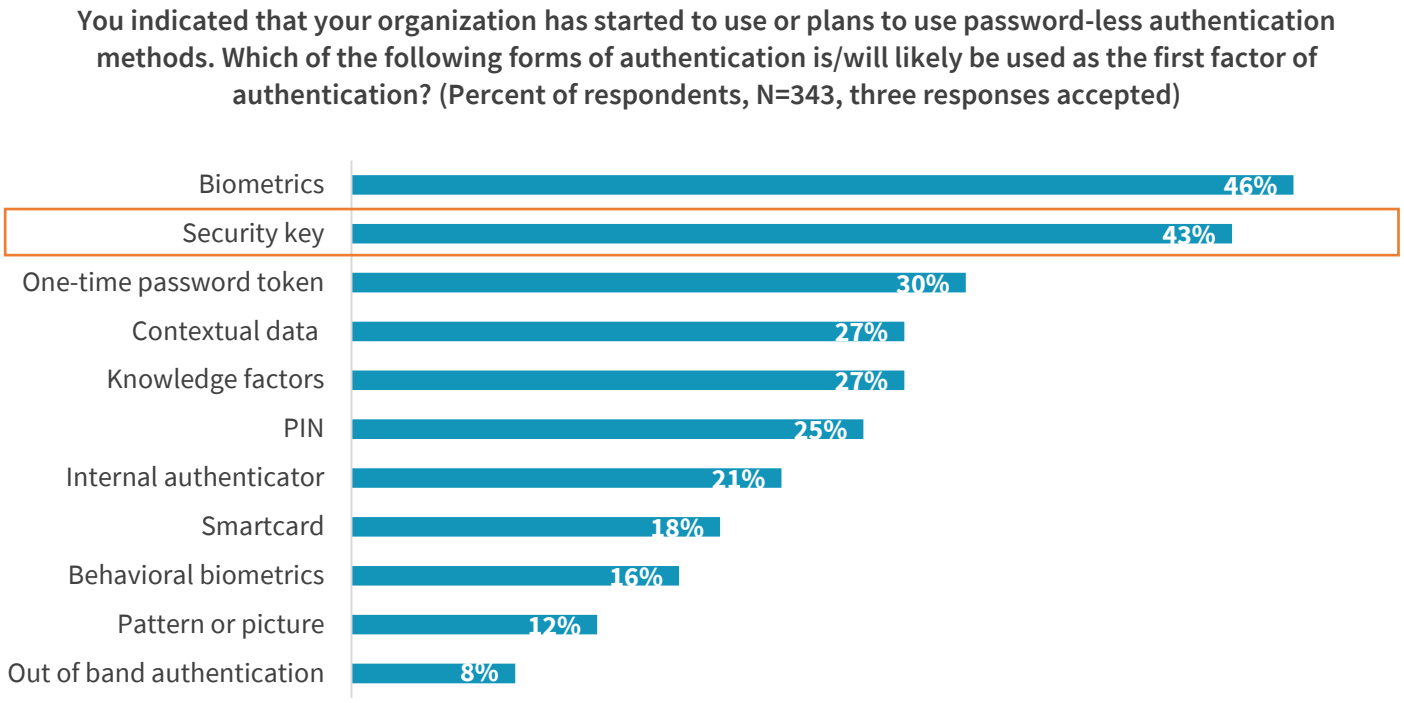
For instance, commercial enterprises and public sector organizations that need robust and reliable authentication can opt for single device passkeys implemented on a hardware-based authenticator such as a security key. These "high-assurance" solutions utilize the widely embraced FIDO2 standard, as well as the WebAuthn authentication specification.

Alternatively, individual consumers can use a syncable, mobile device-based set of credentials where the passkey is not tied to a single, dedicated device. Syncable passkeys utilize the integrated password manager so the passkey's credentials can be copied to and used with other mobile devices that have the same password manager and cloud account. These could be referred to as "low-assurance" passkeys—not because they are unreliable (they are quite reliable), but they don't offer the same high level of protection and trust or adherence to compliance requirements that that organizations and businesses typically demand and currently receive from security keys.

Compared with traditional password-based authentication, passkeys dramatically reduce the potential for identity theft, account takeover, and other methods of credentials theft. They also reduce user friction and frustration, as well as the management burden typically borne by security teams and help desks.

Single device hardware-bound passkeys are stored on security keys, and they are now a highly recognized and increasingly widely used form of passwordless authentication. According to Enterprise Strategy Group research, 43% of organizations that use or plan to use passwordless authentication said they already use or will use security keys as the first factor in their MFA methodology and process (see Figure 3).

Figure 3. Biometrics and Security Keys Are Most Popular Passwordless Authentication Methods



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Bottom line: Passkeys are easier to use, manage, and troubleshoot than traditional passwords, while also reducing user friction. As a result, passkeys reduce risk and promote better cybersecurity hygiene.

What to Look For in a Passkey Solution

First, organizations need to keep in mind what kind of passkey solution is best for their needs. While both syncable and single device passkeys offer many benefits, there is a clear distinction. Organizations looking for a passkey-based authentication solution definitely should evaluate and, ultimately, select a hardware-bound passkey solution because of its high-assurance security. As we've mentioned earlier, copyable passkeys make a lot of sense for consumers who crave ease of use and device flexibility and who are comfortable with a lower-assurance solution. Business users and public sector organizations, however, should also opt for the higher-assurance option.

Security professionals charged with researching and selecting passkey solutions and suppliers should include several must-have capabilities at the top of their evaluation and selection criteria, including:

- Support for key industry standards and protocols, especially FIDO2 and WebAuthn. The technologies behind these standards have been rigorously tested and improved by the many organizations—both technology suppliers and their customers—closest to the passwordless movement.
- Cryptographic attestations that provide confidence that systems are truly secure in a provable fashion.
- Support by a large ecosystem of software developers who are key to seamless integration of passkeys into both existing and new security environments.
- Ability to work with a wide range of services, including Windows and Mac login, as well as popular social media platforms, email applications, and web-based collaboration sites.
- A clear "path to the future," giving organizations the confidence to know they will not run afoul of obsolete technology down the road, especially when new versions of the existing protocols with higher functionality are introduced.

The FIDO Passwordless Standard

More than 250 organizations—coming from both the technology side and private and public sectors—have collaborated for passwordless security standards under the aegis of Fast Identity Online: FIDO. This industry standard has rapidly gained acceptance as a means of providing simple, yet highly reliable, user authentication.

The FIDO standard supports the development and deployment of passwordless solutions that eliminate the need for dedicated authentication applications and take advantage of work already done in such areas as public key encryption and biometrics.

FIDO authentication is designed to support organizations' commitment to privacy, since all biometric and/or personally identifiable information remains on the user's device, rather than being shared over a network or in the cloud.

Using application programming interfaces, FIDO-compliant solutions abstract the protocol implementation, making it ideal for mobile devices. These solutions also can be utilized with different operating systems.

Yubico's Hardware-based Approach to Passkey Authentication

Organizations in both public and private sectors need to modernize and fortify their authentication tools and processes, considering that credentials theft is one of the top ways hackers infiltrate systems and are able to move laterally throughout the network. While lower-assurance, copyable passkeys certainly have their place, organizations should adopt hardware-based passkeys for more reliable and secure authentication and greater visiblity into where the credential is.

Yubico offers hardware-based passkeys or FIDO credentials that reside in YubiKeys that—due to Yubico's co-authoring of authentication standards and early support of the FIDO Industry Alliance—come with FIDO2 and WebAuthn compatibility. Its YubiKey 5 FIPS Series of hardware-based security keys (the actual passkey is integrated within the YubiKey hardware)

delivers AAL3-level assurance, making it highly suitable for use in enterprises, including government and regulated industries such as healthcare, financial services, and education.

In addition to FIDO2 and WebAuthn, Yubico's approach supports a range of authentication protocols, including SmartCard, OTP, and OpenPGP.

Yubico also offers a number of other passkey solutions, including the YubiKey Bio Series—supporting biometric authentication—and the Security Key Series.

Additionally, Yubico provides a number of authentication services that help organizations scale, including YubiEnterprise Subscription for flexible purchasing options and YubiEnterprise Delivery for distributed workforces, customer support, consulting, and onboarding. It also offers developer support for software companies that want to integrate hardware-based passwordless authentication into customers' environments.

Finally, Yubico's early involvement in industry standards groups such as those responsible for developing and promoting FIDO2 and WebAuth gives it important insight into the future of passwordless technology development and deployment.

The Bigger Truth

Replacing passwords as the de facto standard process for user authentication is a given in the minds of just about all organizations and their users. But getting users and security professionals used to new authentication approaches requires making smart decisions on the right solution.

Passkeys offer a wide range of benefits, such as strong phishing defense, the ability to stop account takeovers with the use of public key encryption, and availability in different formats for different environments and use cases.

The development of industry standards such as FIDO2 and WebAuthn has made adopting passkeys easier and generated greater confidence by organizations because of widespread support across platforms and technology providers. Yubico has positioned itself as a leader in the passkey movement as a natural extension of its work on passwordless solutions, and it offers a number of passkey solutions that align with different authentication use cases, protocols, and security frameworks.

Enterprise Strategy Group by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188