VERIDIUM
TRUSTED DIGITAL IDENTITY

THE DIFFERENCES BETWEEN PASSWORDFREE AND PASSWORDLESS AUTHENTICATION

ELIMINATE PASSWORDS, DON'T REPLAY THEM

There seems to be consensus in the identity and access management space that passwords aren't an ideal way to protect data and that no one likes using them. And there's agreement that an authentication method that doesn't involve passwords is needed.

What to call that authentication method is where dissension occurs. Some use the term passwordfree authentication. Meanwhile, Gartner talks about going passwordless and Microsoft is rolling out passwordless authentication to its employees. The phrases seem interchangeable since they both imply not using passwords. But the technical differences between the two are what sets them apart, according to Veridium Chief Product Officer John Spencer.

Passwordfree authentication improves the user experience but doesn't remove the password from the authentication process, allowing the security issues associated with passwords to remain. With passwordless authentication, passwords are never used at any stage in the authentication process. People are never asked to create a password or use one to log in, eliminating the possibility that a password can be used for malicious activity.

In this guide, Spencer provides an in-depth technical breakdown between passwordfree and passwordless authentication and what they mean from an information security perspective.

If a password is still involved in the authentication process, attackers can use it for malicious purposes

WHAT IS PASSWORDFREE AUTHENTICATION

Passwordfree authentication lets people authenticate without using a password. However, the password is not removed from the authentication process. In some capacity, it is still used to gain access.

Often times, what is billed as passwordfree authentication is really password replay. How people access their smartphones and mobile apps is the best example of this. No one enters a PIN anymore. Instead, they use their biometrics to unlock a phone by either touching a fingerprint sensor or using facial recognition technology.

But the PIN is still heavily involved in the authentication process, although a person doesn't have to enter it. Using a fingerprint or facial recognition validates a person's identity and gives a smartphone permission to replay the PIN and unlock the phone.

"The PIN still exists on the phone. Password replay is not passwordless authentication," Spencer said.

Want proof? Restart your smartphone. To unlock it after a reboot, you have to enter your PIN. You can't use a biometric. In other words, the PIN is still part of the authentication process.

PASSWORDFREE AUTHENTICATION

- **Doesn't really eliminate passwords.**
- **Stores passwords on a device, in a browser or in a password management service or tool like OneLogin or Apple Keychain.**
- **Replays the password instead of removing it from the authentication process.**
- **Offers a convenient way to authenticate, but doesn't eliminate the security risks linked to passwords.**
- **Allows password authentication via a Web browser.**

PASSWORDFREE AUTHENTICATION: ADDING CONVENIENCE BUT NOT SECURITY

This same concept applies to authenticating with mobile apps. Take American Express' mobile app. Yes, you can access your account by touching your phone's fingerprint sensor instead of entering a password. But that's password replay. Your fingerprint confirms your identity and replays your password, letting you into your account. If you're using an iPhone, the password for your American Express account is saved on Apple's Keychain along with the other passwords you use.

"From a user's perspective, this method is passwordfree since you don't have to type in a password. But on the back end, there's still the ability to type in a password," Spencer said.

Need evidence? Think of how you access your American Express account from a laptop. You open your browser, go to American Express' site and press the log-in button, which challenges you to enter your user name and password. There's no option to use something other than a password to log in. Unlike authenticating on the mobile app, using a biometric isn't an option. Logging in using a browser still requires a password.

And if a password is still involved in the authentication process, attackers can still use it for malicious purposes.

"If I'm being malicious, I can go to your American Express account or bank account on a laptop browser and use your credentials to enter your account since they can still be used to authenticate," he added.

Password managers that provide passwordfree authentication by storing all of a person's passwords in one location make logging in easier at the expense of security. If an attacker figures out a person's password for that service or tool, then they have all the passwords that a person uses.

"If that password is compromised, I have to reset all the passwords that were in that file. That one key opens up all the doors to my digital identity," Spencer said.

Password replay is not passwordless authentication

PASSWORDLESS AUTHENTICATION

- **Completely removes the password from the authentication process. People are never asked to create a password or enter one to log in.**
- **Uses something besides a password, such as a biometric, to validate a person's identity and passes along a certificate to permit authentication.**
- **Eliminates the option to enter a password, including when people use their laptop's browser.**
- **Increases security by eliminating the risks associated with passwords and improves the user experience.**

WHAT IS PASSWORDLESS AUTHENTICATION

Passwordless authentication completely removes the password from the authentication process. A person is never prompted to create a password when they setup an account or enter a password to access that account. When they open an application or try to access a cloud service, the log-in screen lacks a password field.

"Genuine passwordless authentication doesn't replay passwords in any way, shape or form. When you go to a website and you're challenged to log in, there's no ability for you to put a password in," Spencer said.

By getting rid of passwords, the security risks associated with them are eliminated. Phishing attacks lose their potency if there aren't any credentials to con out of employees. And if there aren't passwords to steal, threat actors can't use them to infiltrate companies. Not using passwords also means a reduction in the costs associated with password resets. Those expenses can tally $70 per employee, according to Okta.

To take full advantage of the security benefits passwordless authentication offers, organizations need to eliminate all opportunities to use password authentication. This includes using a password to log in with a browser, for example.

"Just enabling passwordless authentication isn't enough. Organizations need to close the other doors that were previously exposed by asking a person for their user name and password. You want to make it impossible to use a password in any situation," he said.

HOW PASSWORDLESS AUTHENTICATION WORKS

So if passwords are completely removed from the authentication process, how do you log in? One way to carry out passwordless authentication involves using a smartphone and a person's biometrics. Here's how passwordless authentication into a Windows desktop would work using that technology. In this example, the ability to log in using a password is turned off. Only authentication using a certificate is allowed.

1. When prompted to authenticate into their Windows desktop, users pull out their smartphone, open up their authentication app and scan a QR code that's on the screen. There are no user name or password fields.
2. They're then prompted to authenticate. They would use the device's native biometrics so a person would either touch the fingerprint sensor or use facial recognition.
3. The submitted biometric is validated against the enrollment template.
4. If the biometrics match, a certificate is passed to the Windows system, allowing users to authenticate into the Windows desktop.

To piece the biometric together, threat actors would need to hack a person's phone, hack the server containing the biometric, locate the biometric and unencrypt it.

"There's no way for you to authenticate into your Windows desktop with a password. You have to use your biometric," Spencer said.

From a user experience perspective, people are accustomed to using their biometrics and smartphones for authentication in their personal lives (and Veridium has found that they're keen on using it at the office as well).

If stored using a distributed data model, biometrics are more secure than passwords, which can be shared easily and are frequently exposed in data breaches. In a distributed data model, a portion of the encrypted biometric resides on a person's smartphone and another portion is stored on a company's server.

To piece the biometric together, threat actors would need hack a person's phone, hack the server containing the biometric, locate the biometric and unencrypt the biometric. If those steps were executed successfully, they would then have to spoof the biometric and deceive a smartphone's biometric sensor. But tricking a biometric sensor isn't as easy as news reports make it seem. Many authentication apps (and some smartphones) use liveness detection and behavioral biometrics to ensure that a person, not a finger mold or a 3D mask, is authenticating.

"It's easy. It's convenient. You can't forget your biometric. We know how to use the technology. We trust it and biometrics are difficult to spoof," Spencer said.

HOW TO DISTINGUISH BETWEEN PASSWORDFREE AUTHENTICATION AND PASSWORDLESS AUTHENTICATION

PASSWORDFREE AUTHENTICATION

Doesn't really eliminate passwords	Stores passwords on a device, in a browser or in a password management service or tool like OneLogin or Apple Keychain	Replays the password instead of removing it from the authentication process	Offers a convenient way to authenticate, but doesn't eliminate the security risks linked to passwords	Allows password authentication via a Web browser

PASSWORDLESS AUTHENTICATION

Completely removes the password from the authentication process. People are never asked to create a password or enter one to log in	Uses something besides a password, such as a biometric, to validate a person's identity and passes along a certificate to permit authentication	Eliminates the option to enter a password, including when people use their laptop's browser	Increases security by eliminating the risks associated with passwords and improves the user experience

HOW PASSWORDLESS AUTHENTICATION BENEFITS COMPANIES

By removing passwords from the authentication process, organizations can:

INCREASE SECURITY: Phishing, password reuse and other security risks linked to passwords are eliminated when passwords are removed from the authentication process.

OFFER A BETTER USER EXPERIENCE: Employees don't have to commit multiple passwords to memory or come up with new, complex passwords to comply with policies that require password changes at frequent intervals.

BOOST PRODUCTIVITY: People don't waste time trying to remember their password and then contacting IT to reset it when they're locked out of their email account after multiple failed log-in attempts. Meanwhile, IT departments can handle more important tasks.

LOWER COSTS: The expenses tied to password resets are reduced when passwords are eliminated.