Passkey (Passkey Authentication)

by Senior Editor
Margaret Rouse

Updated on
23 June 2023

What Is a Passkey?

A passkey is an authentication mechanism that uses a possession factor instead of a knowledge factor as the primary authentication credential.

Passkeys are based on FIDO2 (Fast Identity Online 2), an authentication scheme that uses cryptographic keys instead of strong passwords. The keys are created by a FIDO2-compatible device (such as a smartphone, tablet, or desktop computer) and are unique to each passkey-enabled website or app.

Some passkeys are protected by two-factor authentication (2FA) and require a PIN or biometric authentication factor for subsequent sign-ins. In such cases, the end user may not even realize their device is using a passkey as its first authentication factor.

Tier-1 tech vendors like Apple, Microsoft, and Google are promoting passkeys as an easy and effective way to prevent phishing and other types of credential theft.

If widely adopted for multi-factor authentication (MFA), passkeys are also expected to also eliminate the need for password managers.

How Do Passkeys Work?

Most Popular Terms

CYBERSECURITY
Offline Signing Orchestrator (OSO)

What is an Offline Signing Orchestrator (OSO)? Offline Signing Orchestrator, also known as OSO, is an IBM cybersecurity software product...

Full Explanation

MARGARET ROUSE • Senior Editor

A passkey uses public-key cryptography to create a secure and private connection between an end user's computing device and a compatible website or app.

Public-key cryptography uses a public key to encrypt data and a private key to decrypt data. The public key is shared, and the private key is not.

When an end user initially signs into a website or app that supports passkey authentication, their device generates a unique public and private key pair and sends the public key to the website or app's server. The private key remains on the user's device.

The next time the user signs in, the website or app sends a challenge to the user's device. A challenge is a random string of data that is encrypted with the user's public key.

The user's device uses its private key to decrypt the challenge and then sends the decrypted string back to the website or app. If the decrypted challenge matches the original challenge sent by the website or app, the user is automatically logged in.

On the backend, FIDO2 passkeys use the Web Authentication (WebAuthn) standard, a set of application programming interfaces (APIs) that supports passwordless authentication.

Advantages of Passkeys

Passkeys are more convenient than passwords because users do not have to create them, remember them, or update them.

They are also more secure than passwords because the private keys are stored locally in an isolated part of the originating device's operating system that can only be accessed by the device's processor.

If a compatible website or app server is compromised, only the passkey's public keys will be exposed.

Given that a classical computer is not able to use a public key to reverse-engineer a private key within a reasonable amount of time, user authentication will remain secure even if the server that stores the public key experiences a major data breach.

Passkeys are often promoted as the best way to discourage spear phishing and whaling attacks because, unlike passwords, they can't be shared with third parties. Some implementations of passkeys do provide end users with the option of syncing private keys on all their devices, however.

If someone wants to sign in on a new device for the first time or temporarily use someone else's device to sign into their Google account, for example, they can select the option to "use a passkey from another device" and follow the prompts to either approve a one-time login or store the private key locally on the new device.

Disadvantages of Passkeys

Passkeys are still a relatively new technology, and not all websites and apps support them or implement them the same way.

The biggest issue is that if an end user's device is lost or stolen, anyone who can unlock the device can use the passkeys that don't require an additional authentication factor.

In such a scenario, the end user would need to know which keys to revoke manually, or they would need to re-register and create new passkeys for all the compatible websites and apps they use.

Related Questions

How can passwords be stored securely in a database?

Related Terms

Endpoint Authentication

Zero Trust

Password Authentication Protocol
Out-of-Band Authentication
Authentication Server
Machine Authentication

Related Reading

Simply Secure: Changing Password Requirements Easier on Users
Biometrics: Moving Forward with Password-Free Security
Choosing a Password Manager for Business: 8 Features to Look For
How Passive Biometrics Can Help in IT Data Security
Can Public Key Infrastructure Provide More Security Online?

Search a tech term...

A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z

About Techopedia's Editorial Process

Techopedia's editorial policy is centered on delivering thoroughly researched, accurate, and unbiased content. We uphold strict sourcing standards, and each page undergoes diligent review by our team of top technology experts and seasoned editors. This process ensures the integrity, relevance, and value of our content for our readers.

TAGS

CYBERSECURITY ENCRYPTION IDENTITY & ACCESS GOVERNANCE

Margaret Rouse

Senior Editor

Margaret jest nagradzaną technical writerką, nauczycielką i wykładowczynią. Jest znana z tego, że potrafi w prostych słowach przybliżyć złożone pojęcia techniczne słuchaczom ze świata biznesu. Od dwudziestu lat jej definicje pojęć z dziedziny IT są publikowane przez Que w encyklopedii terminów technologicznych, a także cytowane w artykułach ukazujących się w New York Times, w magazynie Time, USA Today, ZDNet, a także w magazynach PC i Discovery. Margaret dołączyła do zespołu Techopedii w roku 2011. Margaret lubi pomagać znaleźć wspólny język specjalistom ze świata biznesu i IT. W swojej pracy, jak sama mówi, buduje mosty między tymi dwiema domenami, w ten…

All Articles by Margaret Rouse →

Related News

INVESTING

Growth vs. Value Stocks: Which Is Best for Investors in 2024?

ROB GRIFFIN . 9 hours

EMERGING TECHNOLOGY

Why Remote Work Apps Could Go the Way of Fax Machine

FRANKLIN OKEKE . 9 hours

INTERVIEW

Being Global with Regional Tech Regulations — It's Difficult

FRANKLIN OKEKE . 11 hours . Technology Journalist

BLOCKCHAIN

The Big Interview: Ernst & Young: The Future of Supply Chain is...

NICOLE WILLING . 11 hours . Technology Journalist

EMERGING TECHNOLOGY

Quantum Computing Investment Boom: Funding Driving...

MARIA WEBB . 14 hours . Technology Journalist

CYBER THREATS

Gaps in the Cloud Are Letting Hackers Fly Under the Radar

RAY FERNANDEZ . 14 hours . Senior Technology Journalist

Popular Categories

Show All →

Antivirus	Artificial Intelligence	Audio	CRM	Cryptocurrency	Gambling	Gaming	HR
Investing	Laptops	Network	Password Managers	Project Management	Spy	VoIP	VPN

Get Techopedia's Daily Newsletter in your inbox every Weekday.

Add your email

Subscribe

Trending News Latest Guides Reviews Term of the Day

By signing up, you agree to our Terms of Use and acknowledge the data practices in our Privacy Policy. You may unsubscribe at any time.

Resources

Dictionary

Job Board

Q&A

Raid Calculator

Topics

Tutorials

Popular Categories

Artificial Intelligence

Cryptocurrency

Cybersecurity

Data Management

Networking

Personal Tech

Featured Content

Accounting Software

Antivirus Software

CRM Software

Project Management Tools

Spy Apps

VPN Services

About Techopedia

About Us

Advertising Info

Contact

Contributors

Editorial Policy

Privacy Policy

Techopedia Terms

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z