Revolutionizing Authentication: Google Passkeys Technology

Manasvi Malhar Sudershan

Student, Department of Information Technology, BV Raju Institute of Technology, Hyderabad

Abstract

In the ever-evolving landscape of digital security, the traditional methods of authentication are facing increasing challenges in safeguarding sensitive information and user privacy. Google Passkeys technology emerges as a pioneering solution poised to redefine the way users access their accounts and protect their digital identities.

This abstract delves into the innovation of Google Passkeys technology, exploring its fundamental principles and potential impact. Passkeys represent a paradigm shift in authentication by eliminating the need for passwords, which have long been susceptible to breaches and often result in user frustration. Instead, Passkeys harness cutting-edge cryptographic techniques to create a seamless and secure authentication process.

At its core, Google Passkeys rely on a unique combination of hardware-based security keys and advanced cryptographic algorithms. Users are equipped with physical security keys, such as USB tokens or smartphones with built-in security features, which act as the "key" to their digital identities. These keys, paired with secure communication protocols, provide a multifaceted approach to authentication that significantly enhances security.

Keywords: Google Passkeys 1, Authentication 2, Cryptographic Techniques 3

1. Introduction

In the digital age, the security of personal and sensitive information is of paramount concern. Traditional methods of authentication, such as usernames and passwords, have proven to be susceptible to a wide range of threats, from data breaches to phishing attacks. In response to these challenges, Google Passkeys technology has emerged as a groundbreaking solution designed to transform the way users access their accounts and protect their digital identities. Google Passkeys technology represents a significant departure from the conventional approach to authentication. It is built on the foundation of the FIDO2 (Fast Identity Online 2) standard, a set of open authentication protocols that seek to revolutionize the authentication landscape.

At its core, Google Passkeys leverage the power of hardware-based security keys and advanced cryptographic techniques to provide a multifaceted and highly secure authentication process. The primary goal of Google Passkeys is to eliminate the reliance on passwords, which have long been a weak link in the chain of digital security. Instead, Passkeys introduce a novel paradigm where users are equipped with physical hardware security keys, such as USB tokens or smartphones with secure elements. These keys act as the "key" to their digital identities, offering a level of protection that is far superior to traditional passwords. It provides a comprehensive overview of Google Passkeys technology, exploring its fundamental principles, key features, and potential implications. It delves into the inner workings of Passkeys, shedding light on how they operate in real-world scenarios and highlighting their capacity to thwart common cyber threats, particularly phishing attacks. As we delve deeper into Google Passkeys technology, we will explore the intricacies of its registration and authentication processes, emphasizing its robust security measures and user-friendly nature. Additionally, we will discuss the technology's alignment with the industry's shift towards zero-trust security models and its potential to disrupt the authentication status quo. While Google Passkeys offer a promising solution to the pressing issues of authentication security, this introduction will also acknowledge the challenges and considerations that come with their adoption. This includes issues of usability, accessibility, and the need for backup authentication methods to ensure a seamless user experience.

2. Existing Systems

Before the emergence of Google Passkeys technology and FIDO2-based authentication, several traditional authentication methods and systems were widely used for securing online accounts and services. These legacy authentication systems included:

- **Username and Password**: This is the most common and traditional form of authentication. Users create unique usernames and passwords to access their accounts. However, passwords are prone to being forgotten, stolen, or easily guessed, making them a weak link in security.
- **One-Time Passwords (OTP):** OTPs provide an additional layer of security by generating a temporary code that users must enter alongside their password. OTPs are typically sent to users' mobile devices or generated by dedicated hardware tokens.
- **SMS-Based Authentication:** Users receive a one-time code via text message, which they enter during the login process. While it adds an extra layer of security compared to passwords alone, SMS-based authentication is vulnerable to SIM swapping attacks and phishing.
- **Email-Based Authentication:** Some systems send a link or a code to the user's email address, which they need to click or enter for verification. While it's convenient, it relies heavily on the security of the email account.
- **Knowledge-Based Authentication (KBA):** KBA involves answering security questions or providing personal information, like a mother's maiden name or the name of a pet. However, this method can be insecure if attackers have access to or can guess the answers.
- **Biometric Authentication:** Biometric methods, such as fingerprint recognition, facial recognition, and iris scanning, have become more common on mobile devices. However, their effectiveness can vary, and they raise concerns about privacy and the security of biometric data.
- **Smart Cards and Tokens:** Smart cards and hardware tokens generate one-time codes or digital signatures for authentication. They are often used in corporate settings, but their cost and complexity limit their widespread adoption.
- **Social Login (OAuth):** Users can log in to various websites and apps using their existing social media accounts (e.g., Facebook or Google). While convenient, this method raises privacy concerns and relies on the security of the social media account.
- **Multi-Factor Authentication (MFA):** MFA combines two or more authentication factors, such as something you know (password), something you have (smartphone or token), or something you are (biometrics). MFA enhances security but can still be susceptible to certain attacks.

- **Certificate-Based Authentication:** Digital certificates issued by a trusted authority are used for authentication. This is common in secure enterprise environments but may not be user-friendly for consumers.

2.1 Disadvantages of Existing System

The existing traditional authentication systems, while widely used, have several disadvantages and vulnerabilities that make them less secure and user-friendly.

Here are some of the key disadvantages:

- **Password Vulnerabilities:** Passwords are often the weakest link in security due to issues such as weak or easily guessable passwords, password reuse across multiple accounts, and susceptibility to brute-force attacks.
- **Phishing and Social Engineering:** Users can be tricked into revealing their passwords or sensitive information through phishing emails, fake login pages, or social engineering attacks.
- **Credential Theft and Data Breaches:** Usernames and passwords can be stolen through data breaches, putting sensitive data at risk. Many users reuse passwords across multiple accounts, compounding the problem.
- **User Convenience vs. Security:** Balancing security and convenience is a challenge. Increasing security often means adding more steps to the authentication process, which can frustrate users.

2.2 Advantages of Proposed System

Google Passkeys technology, based on FIDO2 (Fast Identity Online 2) authentication standards, offers numerous advantages over traditional authentication methods. These advantages contribute to improved security, user experience, and protection against common cyber threats.

Here are some of the key advantages of Google Passkeys technology:

- **Phishing Resistance:** Google Passkeys provide strong protection against phishing attacks. Even if a user interacts with a malicious website or falls victim to a phishing email, the attacker cannot access the account without the physical hardware security key.
- **Enhanced Security:** Passkeys rely on hardware-based security keys and public-key cryptography, making them highly secure. The private keys stored on the hardware keys are extremely difficult to compromise, significantly reducing the risk of unauthorized access.
- **Elimination of Passwords:** Google Passkeys eliminate the need for traditional passwords. Passwords are a common weak point in security due to issues like password reuse and weak password choices. Removing passwords reduces these vulnerabilities.
- **User-Friendly:** The authentication process with Google Passkeys is user-friendly and convenient. Users simply need to insert their hardware security key and follow a few steps, making it easy to use, even for non-technical individuals.
- **Cross-Platform Compatibility:** Passkeys technology is compatible with various platforms and services that support FIDO2 authentication. Users can use the same hardware security key across multiple websites and applications.

3. Methods

The methodology of Google Passkeys is based on the following principles:

- **Security:** Google Passkeys must be highly secure and resistant to phishing and other attacks.

- **Usability:** Google Passkeys must be easy to use and convenient for users.
- **Scalability:** Google Passkeys must be scalable to support a large number of users and websites.

To achieve these principles, Google Passkeys uses a combination of public key cryptography and biometric authentication.

Public key cryptography is a type of encryption that uses two different keys: a public key and a private key. The public key can be shared with anyone, but the private key must be kept secret. Data encrypted with the public key can only be decrypted with the private key.

Biometric authentication is a type of authentication that uses the user's unique biological characteristics, such as their fingerprint or face scan.

Methodology

Google Passkeys works by generating a public key and a private key for each user. The public key is stored on the user's device, while the private key is stored securely on Google's servers. When a user wants to sign in to a website or app that supports Google Passkeys, they are prompted to use their biometric authentication to verify their identity. Once the user has been verified, their device generates a cryptographic signature using the private key associated with their passkey. This signature is then sent to the website or app that the user is trying to sign in to.

The website or app will then verify the signature using the public key associated with the user's passkey. If the signature is valid, then the website or app will know that the user is the legitimate owner of the passkey and will allow them to sign in. Google Passkeys is still under development, but it has the potential to revolutionize the way we sign in to websites and apps. It is more secure than passwords, easier to use, and more scalable.

The internal methodology of Google Passkeys is

- Google Passkeys uses the FIDO2 protocol, which is an open standard for password less authentication.
- Google Passkeys are stored on the user's device and are never shared with the website or app that the user is signing in to.
- Google Passkeys are encrypted using AES-256 in Galois/Counter Mode (GCM).
- Google Passkeys are signed using RSA.
- Google Passkeys can be used to sign in to websites and apps on any device that supports FIDO2 authentication, regardless of the operating system.

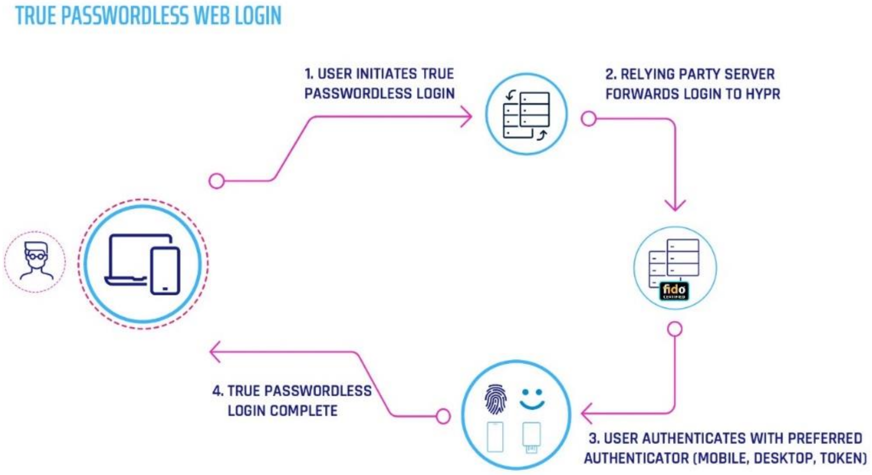

TRUE PASSWORDLESS WEB LOGIN
1. USER INITIATES TRUE PASSWORDLESS LOGIN
2. RELYING PARTY SERVER FORWARDS LOGIN TO HYPR
fido
3. USER AUTHENTICATES WITH PREFERRED AUTHENTICATOR (MOBILE, DESKTOP, TOKEN)
4. TRUE PASSWORDLESS LOGIN COMPLETE

Fig. 1 Working of Google Passkeys

FIDO2 Protocol

The FIDO2 protocol is an open standard for password less authentication. It is designed to be more secure and convenient than passwords, and it can be used to authenticate to websites, apps, and devices. It works by using public key cryptography and biometric authentication. Public key cryptography is a type of encryption that uses two different keys: a public key and a private key. The public key can be shared with anyone, but the private key must be kept secret. Data encrypted with the public key can only be decrypted with the private key.

AES-256 in Galois/Counter Mode (GCM)

AES-256 in Galois/Counter Mode (GCM) is a cryptographic algorithm that is used to encrypt and decrypt data. It is a very secure algorithm, and it is used by a variety of organizations, including Google, to protect sensitive data.

AES-256 is a symmetric encryption algorithm, which means that the same key is used to encrypt and decrypt the data. The key length is 256 bits, which provides a very high level of security. Galois/Counter Mode (GCM) is a mode of operation for block ciphers, such as AES. GCM provides both confidentiality and integrity protection for the data.

To encrypt data using AES-256 in GCM, the following steps are taken:

- A random initialization vector (IV) is generated.
- The data is encrypted using AES-256 with the IV.
- The IV and the encrypted data are concatenated and authenticated using a cryptographic hash function.
- The authenticated data is then sent to the recipient.

To decrypt data using AES-256 in GCM, the following steps are taken:

- The IV is extracted from the authenticated data.
- The encrypted data is decrypted using AES-256 with the IV.
- The decrypted data is authenticated using the cryptographic hash function and the IV.
- If the authentication is successful, then the decrypted data is returned to the user.

RSA

Google Passkeys are signed using RSA to ensure that they are authentic and have not been tampered with. When a user signs in to a website or app using a Google Passkey, the website or app will verify the signature using the public key associated with the user's passkey. If the signature is valid, then the website or app will know that the user is the legitimate owner of the passkey and will allow them to sign in.

RSA is an asymmetric encryption algorithm, which means that it uses two different keys: a public key and a private key. The public key can be shared with anyone, but the private key must be kept secret. Data encrypted with the public key can only be decrypted with the private key.

RSA is used to sign and verify digital signatures. To sign a digital signature, the following steps are taken:

- A hash of the data to be signed is generated.
- The hash is encrypted with the private key using RSA.
- The encrypted hash is the digital signature.

To verify a digital signature, the following steps are taken:

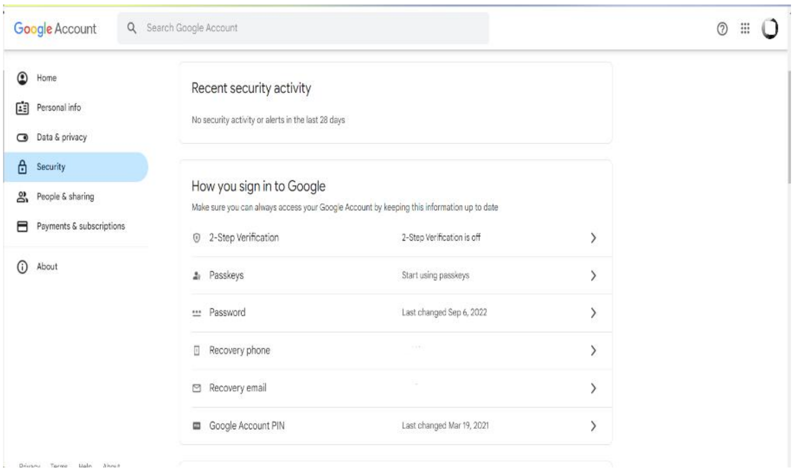
- The digital signature is decrypted with the public key using RSA.
- A hash of the data to be verified is generated.

- If the two hashes are the same, then the digital signature is valid.

4. Figures

Passkey Creation

Fig.1 Google dashboard



Google Account

Search Google Account

Home

Personal info

Data & privacy

Security

People & sharing

Payments & subscriptions

About

Recent security activity

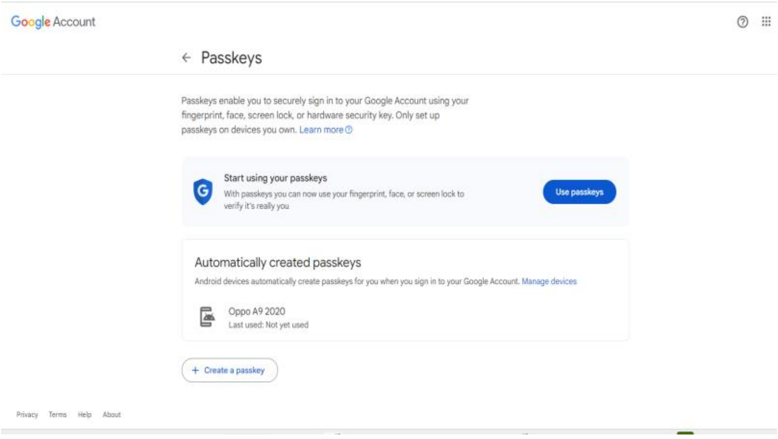
No security activity or alerts in the last 28 days

How you sign in to Google

Make sure you can always access your Google Account by keeping this information up to date

2-Step Verification	2-Step Verification is off
Passkeys	Start using passkeys
Password	Last changed Sep 6, 2022
Recovery phone	
Recovery email	
Google Account PIN	Last changed Mar 19, 2021

Fig. 2 Using of Passkeys



Google Account

← Passkeys

Passkeys enable you to securely sign in to your Google Account using your fingerprint, face, screen lock, or hardware security key. Only set up passkeys on devices you own. Learn more

Start using your passkeys

With passkeys you can now use your fingerprint, face, or screen lock to verify it's really you

Use passkeys

Automatically created passkeys

Android devices automatically create passkeys for you when you sign in to your Google Account. Manage devices

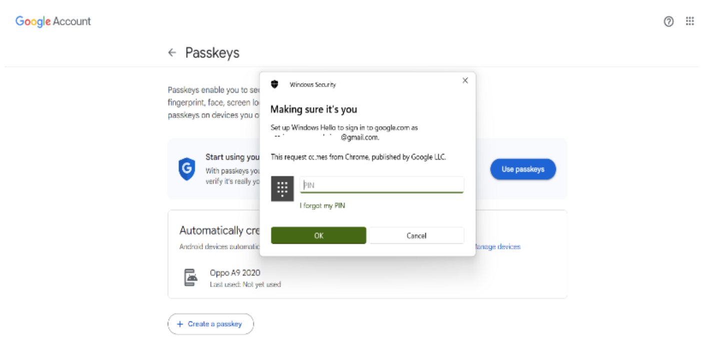
Oppo A9 2020

Last used: Not yet used

+ Create a passkey

Privacy Terms Help About

Fig. 3 Authorization of user



Google Account

← Passkeys

Windows Security

Making sure it's you

Set up Windows Hello to sign in to google.com as @gmail.com.

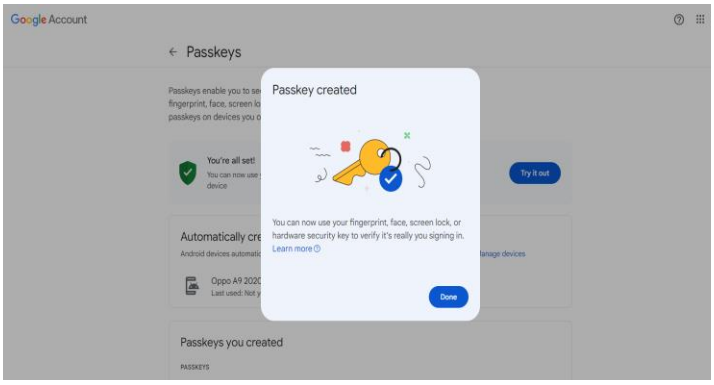
This request comes from Chrome, published by Google LLC.

PIN

I forgot my PIN

OK Cancel

Fig. 4 Passkey created



Google Account

← Passkeys

Passkeys enable you to se
fingerprint, face, screen lo
passkeys on devices you o

You're all set!
You can now use
device

Try it out

Automatically cre
Android devices automatic

Oppo A9 2020
Last used: Not y

lanage devices

Passkeys you created

PASSKEYS

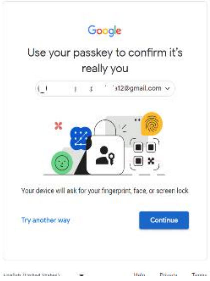
Passkey created

You can now use your fingerprint, face, screen lock, or hardware security key to verify it's really you signing in.
Learn more

Done

Login using Google Passkeys

Fig. 5 Authorization using Passkey



Google

Use your passkey to confirm it's really you

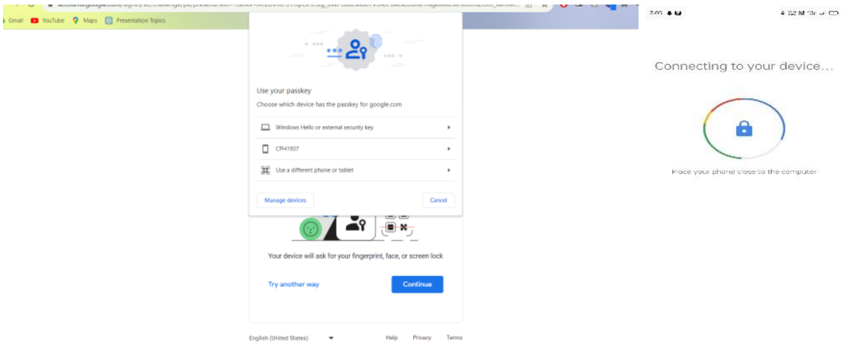
[illegible]12@gmail.com

Your device will ask for your fingerprint, face, or screen lock

Try another way

Continue

Fig. 6 Device Selection & Device Authorisation



Gmail YouTube Maps Presentation Topics

Use your passkey
Choose which device has the passkey for google.com

Windows Hello or external security key
CPH1937
Use a different phone or tablet

Manage devices
Cancel

Your device will ask for your fingerprint, face, or screen lock

Try another way
Continue

English (United States) Help Privacy Terms

Connecting to your device...

Place your phone close to the computer

5. Conclusion

In conclusion, Google Passkeys technology represents a significant milestone in the evolution of online security and authentication. By eliminating the reliance on traditional passwords and introducing hardware-based security keys coupled with advanced cryptographic techniques, it addresses many of the vulnerabilities and usability challenges associated with legacy authentication methods. Passkeys technology not only enhances security by offering robust protection against phishing attacks but also prioritizes user-friendliness, making it accessible to individuals of all technical backgrounds. Its compatibility with a wide range of platforms and services, along with its alignment with the principles of zero-trust security, positions it as a pivotal solution for the modern digital landscape.

6. References

1. https://www.hypr.com/security-encyclopedia/fido2-web-authentication
2. https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption
3. https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
4. https://www.geeksforgeeks.org/rsa-algorithm-cryptography/
5. https://www.strongdm.com/blog/fido2
6. https://sites.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf
7. https://developers.google.com/identity/passkeys
8. https://timesofindia.indiatimes.com/gadgets-news/how-to-get-started-with-google-passkeys-a-step-by-step-guide/articleshow/99991827.cms