Changefly: A Distributed Anonymous Authentication System

Lukas J. Dickie
changefly.com

Published: April 23, 2024
updated August 2, 2024

Abstract. In an age where privacy and security concerns are at the forefront of digital interactions, the concept of anonymous authentication emerges as a promising solution. This white paper delves into the intricacies of Changefly's distributed anonymous authentication system, highlighting its significance in safeguarding user privacy while ensuring secure access to online services. Through a comparative analysis with traditional login identifiers such as usernames, email addresses, and phone numbers, this paper elucidates the advantages of anonymous authentication in promoting user autonomy, mitigating identity theft risks, and fostering trust in online ecosystems.

1. Introduction

Authentication serves as the gateway to digital services, verifying the identity of users before granting access. Traditional authentication mechanisms rely on personally identifiable information (PII) such as usernames, email addresses, and phone numbers to validate user identities. While effective, these methods pose inherent risks to user privacy, as PII is susceptible to breaches and misuse:

> ***UnitedHealth says hackers stole health data on 'substantial proportion of people in America'***
> *https://techcrunch.com/2024/04/22/unitedhealth-change-healthcare-hackers-substantial-proportion-americans/*
>
> ***Okta admits hackers accessed data on all customers during recent breach***
> *https://techcrunch.com/2023/11/29/okta-admits-hackers-accessed-data-on-all-customers-during-recent-breach/*
>
> ***Okta warns of unprecedented surge in credential stuffing attacks***
> *https://thehackernews.com/2024/04/okta-warns-of-unprecedented-surge-in.html*

Anonymous authentication presents an alternative approach by decoupling user identities from sensitive personal information. By employing cryptographic techniques and token-based systems, anonymous authentication enables users to access services without divulging identifiable data. This white paper elucidates the principles of anonymous authentication and explores its superiority over traditional login identifiers.

2. Understanding Bad Actors

Bad actors increasingly use dark web platforms and artificial intelligence to profit from account takeovers (ATO) through various means:

> **Financial Theft:** They can directly steal money from bank accounts or make unauthorized purchases using the compromised accounts. This could involve transferring funds to their own accounts, using saved payment methods to make purchases, or exploiting financial services tied to the compromised account.
>
> **Identity Theft:** ATO can provide access to personal information beyond just financial data. This can include social security numbers, addresses, and other sensitive data

that can be used for identity theft. They may sell this information on the dark web to other criminals or use it themselves for various fraudulent activities, such as applying for loans or credit cards in the victim's name.

Data Mining and Profiling: By accessing a user's account, bad actors can gather valuable data about the individual's preferences, behaviors, and personal details. This information can be used for targeted advertising, phishing attacks, or even blackmail.

Credential Stuffing: Bad actors often use ATO as a means to collect valid login credentials that can be used across multiple platforms. These credentials are then sold in bulk on the dark web or used for further attacks, such as credential stuffing attacks where the same login information is tried on multiple websites to gain unauthorized access.

Ransom and Extortion: They may threaten to release sensitive information or lock the victim out of their account (and valuable data) unless a ransom is paid. This could involve threatening to expose compromising photos or personal data obtained from the compromised account, or locking the victim out of their own account (data) and demanding payment for its release.

Fraudulent Activities: Bad actors can use compromised accounts to perpetrate various types of fraud, such as spreading scams, distributing malware or spam, or conducting phishing and vishing attacks on the victim's contacts.

Overall, an individual's life and an organization's reputation can be upended in an instant. Account takeovers are lucrative for bad actors because they provide access to a wealth of valuable information and resources that can be exploited for financial gain or other malicious purposes.

3. Understanding Privacy

Data privacy is crucial for several reasons, spanning individual safety, organizational integrity, and societal well-being. Here are some key points highlighting the importance of data privacy:

Protection of Personal Information: Data privacy safeguards individuals' sensitive information, such as personal identifiers, financial data, health records, and online activities, from unauthorized access or misuse. This protection is essential for

preserving individuals' autonomy and preventing identity theft, fraud, and other forms of harm.

Trust and Reputation: Maintaining strong data privacy practices fosters trust between individuals, organizations, and institutions. When people believe their data is handled responsibly and securely, they're more likely to engage with businesses, share information, and participate in digital activities. Conversely, data breaches or privacy violations can severely damage an organization's reputation and erode trust among its stakeholders.

Compliance with Regulations: Governments worldwide have enacted laws and regulations to ensure the protection of individuals' data rights. Compliance with these regulations, such as the European Union's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), is not only a legal requirement but also demonstrates an organization's commitment to respecting individuals' privacy rights.

Data Security and Risk Management: Data privacy goes hand in hand with data security. By implementing robust privacy measures, organizations can mitigate the risk of data breaches, cyber attacks, and other security incidents. This includes encryption, access controls, regular audits, and employee training to uphold privacy standards and safeguard sensitive information.

Ethical Considerations: Respecting individuals' privacy is an ethical imperative in the digital age. It involves recognizing and upholding people's rights to control their personal information and make informed choices about its use. Ethical data practices promote fairness, transparency, and accountability in how data is collected, processed, and shared.

Promotion of Innovation and Research: Effective data privacy frameworks can encourage innovation and research by providing clear guidelines for responsible data use. By protecting individuals' privacy, organizations can gather data for legitimate purposes such as product development, scientific research, and public health initiatives without compromising confidentiality or violating ethical norms.

As you can see, data privacy is indispensable for safeguarding individual rights, fostering trust, complying with regulations, managing risks, upholding ethical standards, and fostering innovation. Prioritizing data privacy is not only a legal requirement but also a moral and practical imperative in our increasingly interconnected and data-driven world.

4. Weaknesses in Personally Identifiable Authentication

Let's examine a basic account database:

Account ID	Email	Password	Phone
1	john@gmail.com	Bowling4!	206-842-7492
2	fsmith@yahoo.com	ocean$12	409-762-9082
3	mjones@gmail.com	G8j2C3n1&	212-456-7283
4	jane@aol.com	Judge99%	518-364-8765

We've left out other fields, such as first and last name, but here you can see common fields for identifying and authenticating users. Note that if this database were to be compromised in a data breach, the data would be used by bad actors and data brokers.

In the above account database example, a typical use case would be the user provides an email address to identify their account and a password to authenticate their account. The email address and phone number might also be used for two-factor authentication, or to recover the account in the event the user loses or forgets their password.

By using a known email address, phone number or username for account login, both organizations and users are assisting bad actors in the account takeover process. The information is easily found in public records, websites, social media, and data leaks bought and sold on the dark web. Bad actors don't always need a password — they can use the user's email address, phone number, or other techniques such as social engineering for illicit gains.

5. Weaknesses in Multi-Factor Authentication (MFA)

MFA bombing: In an MFA bombing attack, bad actors send a barrage of MFA prompts to a victim's device to fatigue or annoy the user into authenticating the login-in attempt. If someone receives hundreds of messages in a row, they may authenticate simply to stop the barrage of notifications, hence why it's sometimes called 'MFA fatigue attacking.' MFA bombing is an effective counterattack.

> ***Recent 'MFA Bombing' Attacks Targeting Apple Users***
> *https://krebsonsecurity.com/2024/03/recent-mfa-bombing-attacks-targeting-apple-users/*

Adversary-in-the-middle (AITM): AITM attacks essentially trick a user into thinking they're logging into a legitimate network, application, or website, when in fact they're putting their details into a fraudulent lookalike. This means attackers can intercept passwords and manipulate MFA prompts and other types of security.

> ***Takeovers of MFA-protected accounts increase, as Microsoft 365 phishing campaign shows***
> *https://www.csoonline.com/article/649242/takeovers-of-mfa-protected-accounts-increase-as-microsoft-365-phishing-campaign-shows.html*

Social engineering: Attackers can use social engineering to trick IT support into bypassing MFA altogether by pretending they've forgotten their password.

> ***The chaotic and cinematic MGM casino hack, explained***
> https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware

SIM swamps: A SIM swap attack is where attackers trick service providers into switching services to a SIM card or eSIM they (the attacker) control, effectively hijacking the victim's mobile service and phone number. This allows attackers to receive the MFA prompts and grant themselves access.

6. Weaknesses in Passkeys

William Brown best sums up the design failure and Big Tech interests of passkeys:

> ***Passkeys: A Shattered Dream***
> *https://fy.blackhats.net.au/blog/2024-04-26-passkeys-a-shattered-dream/*

7. Understanding Anonymous Authentication

Anonymous authentication involves the validation of user identities without the need for revealing personally identifiable information (PII). This is achieved through the following key components:

> **Cryptographic Protocols:** Anonymous authentication protocols leverage cryptographic techniques such as zero-knowledge proofs and digital signatures to

verify user identities securely. These protocols ensure that authentication providers can validate users' credentials without storing or transmitting sensitive information.

Token-based Systems: Instead of using PII, anonymous authentication relies on tokens or unique identifiers generated during the authentication process. These tokens serve as temporary credentials, allowing users to access services without disclosing personal data. Tokens can be securely generated and managed to prevent identity theft and unauthorized access.

Decentralized Identity Systems: Some implementations of anonymous authentication employ decentralized identity systems, where users maintain control over their digital identities through blockchain or distributed ledger technology. Decentralized systems eliminate the need for central authorities to store and manage user data, enhancing privacy and security.

8. Advantages of Anonymous Authentication

Enhanced Privacy: Unlike traditional login identifiers, anonymous authentication minimizes the exposure of users' personal information. By dissociating user identities from PII, anonymous authentication mitigates privacy risks associated with data breaches and unauthorized access.

Reduced Identity Theft Risks: Traditional authentication methods often rely on static identifiers such as email addresses or phone numbers, making them vulnerable to identity theft and account takeover. Anonymous authentication, on the other hand, utilizes dynamic tokens that are harder to exploit, thereby reducing the risk of identity fraud.

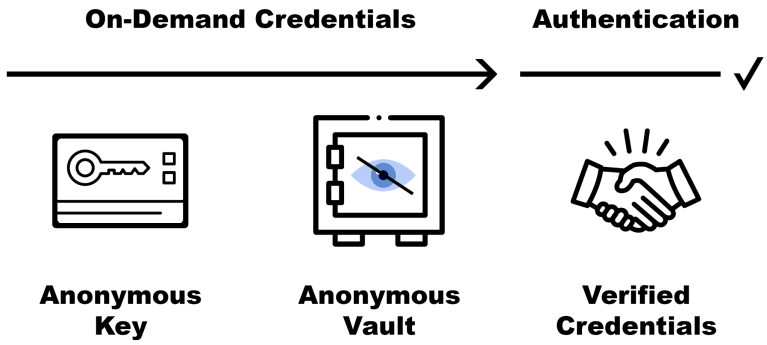
User Autonomy: Anonymous authentication empowers users to control their digital identities without relying on centralized authorities. By preserving user anonymity, anonymous authentication fosters a sense of autonomy and trust in online interactions.

Scalability and Interoperability: Anonymous authentication frameworks are inherently scalable and interoperable, as they can accommodate diverse use cases and platforms without compromising security or privacy. This scalability facilitates seamless integration with existing systems and promotes innovation in authentication mechanisms.

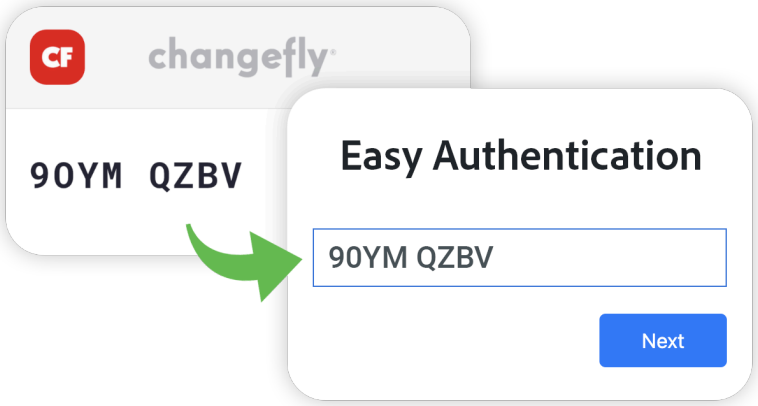
9. Changefly's Anonymous Identification and Authentication: Changefly ID

Changefly is re-imagining a world where accounts no longer need traditional email addresses, passwords, phone numbers, payment details, or other personally identifiable information. A world where personal data and identities are safe. A world where individuals are protected from credential stuffing, phishing attacks, imposter scams, payment scams, identity theft, and more.

Anonymous identification refers to the process of identifying or distinguishing individuals or entities without revealing their personal identities or sensitive information. It's often used in contexts where privacy is paramount, such as online accounts.

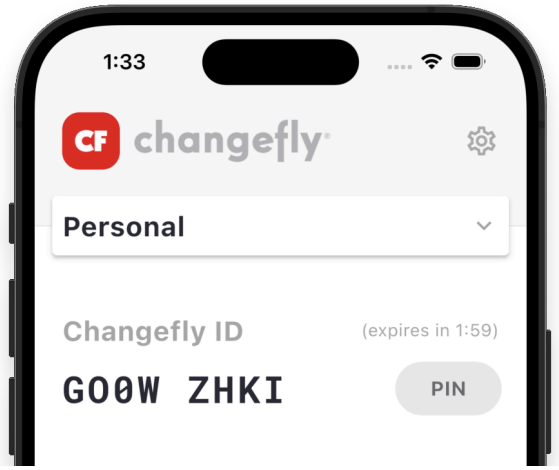


The solution we propose for anonymous identification begins with the Changefly app and Changefly ID — a unique and time-limited cryptographically secure code that is generated on the fly:



10. Anonymous Identification with Changefly ID

Here we see Changefly ID provided in the Changefly app:



Changefly ID is a cryptographically secure, random eight-character alpha-numeric passcode with 2.821 trillion permutations. Each Changefly ID generated by the Changefly app is uniquely tied to the anonymous user and selected anonymous profile (e.g., Personal). Only one unique Changefly ID per anonymous user exists at any given time.

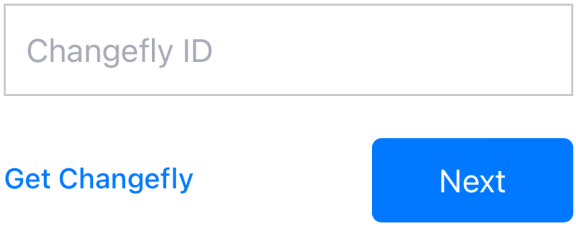
To protect against brute force attacks, an anonymous user's Changefly ID is additionally tied to the IP address where the Changefly ID was generated. Protection against address spoofing and Denial-of-Service (DoS) attacks are mitigated at the network level. In the event of an IP mismatch (e.g., Changefly ID generated on a mobile phone network, but the user is authenticating on another network), a cryptographically secure authentication PIN (Changefly PIN) acts as an additional means of verification. Each Changefly ID has predefined security controls before a new Changefly ID must be generated.

Changefly ID is generated using the following steps:

1. Client app creates a cryptographically secure anonymous user PIN (Changefly PIN, not shown).
2. Client app sends cryptographically secure hash of anonymous user PIN to authentication network.
3. Authentication network receives anonymous user PIN hash from client app.

4. Authentication network creates a unique cryptographically secure anonymous user identifier (Changefly ID).
5. Authentication network saves unique anonymous user identifier metadata.
6. Authentication network sends unique anonymous user identifier to client app.
7. Client app receives unique anonymous user identifier from the authentication network.
8. Client app displays anonymous user identifier (Changefly ID) and may optionally display anonymous user PIN (Changefly PIN).

11. Anonymous Authentication with Changefly ID



Changefly ID authentication is achieved using the following steps:

1. User logs into a third-party entity using Changefly ID. Additionally, third-party may request Changefly PIN (optional) or use the user IP address (preferred).
2. Third-party entity processes Changefly ID and either Changefly PIN or user IP address, and then sends third-party data to the authentication network.
3. Authentication network receives and processes third-party data including Changefly ID and either Changefly PIN or user IP address.
4. Authentication network processes anonymous authentication request and returns approval (**with unique Changefly ID** and other metadata) or denial to third-party entity. In the event of user IP address mismatch, third-party may optionally request the user's Changefly PIN.
5. Third-party entity verifies anonymous authentication approval or denial received from the authentication network.

Success!

See how easy that was?

Sign out

Now let's look again at the earlier example of a basic account database, only this time with Changefly anonymous authentication integrated:

Account ID	Changefly ID	Email	Password	Phone
1	---	john@gmail.com	Bowling4!	206-842-7492
2	**d3f0580efe…**	---	---	---
3	**e9c7b97af1…**	mjones@gmail.com	---	---
4	---	jane@aol.com	Judge99%	518-364-8765

In this latest example, we see the introduction of a **Changefly ID** for users who are authenticating with Changefly ID. The Changefly ID is anonymous and uniquely generated on successful authentication between the user and third-party.

No login ID to leak, password to remember, or passkey to store. Additionally, anonymous Changefly ID hinders tracking beyond the user / third-party connection. Optionally, email and phone number are also no longer necessary, as the Changefly network and app facilitate trusted end-to-end encrypted communications.

12. Changefly ID Use Cases

Next-Gen Account Authentication: Changefly ID can be used as an alternative or direct replacement for traditional login identifiers and authentication. Anonymous authentication minimizes the exposure of users' personal information and strengthens account security through a passwordless user experience with real-time multi-factor authentication. By dissociating user identities from personally identifiable information (PII), anonymous authentication mitigates privacy risks associated with data breaches and unauthorized access.

Next-Gen Multi-Factor Authentication (MFA): Changefly ID can be used as a strong, fast, and low-cost alternative over traditional multi-factor authentication methods (MFA; two-factor authentication, or 2FA) which often rely on security codes sent to a user's email address or phone number (both can be intercepted by third parties), and time-based one-time password apps (TOTP, or OTP) which offer a less-than-desirable user experience. Now users generate a secure Changefly ID for MFA in a single step.

Next-Gen Human Verification: Changefly ID initialization is designed to distinguish between humans and bots, using advanced bot detection technologies and a score-based detection system.

Next-Gen Identity Verification: Changefly ID can be used as a quick and low-cost alternative over traditional identity verification methods which often require users to repeatedly upload their identity documents, such as a government-issued driver's license or government passport. With Changefly, users verify their identity once. Subsequent requests for identity verification or re-verification are provided using their secure Changefly ID in a single step.

Next-Gen Fraud Prevention: Changefly ID can easily be used as a powerful deterrent against fraudulent activities such as bots, ad fraud, unauthorized payments, and identity theft.

13. Conclusion

We have proposed a distributed anonymous authentication system that offers a paradigm shift in user identity verification, prioritizing privacy, security, and user autonomy. By decoupling user identities from personally identifiable information, anonymous authentication mitigates privacy risks, reduces identity theft vulnerabilities, and fosters trust in online ecosystems. Furthermore, by removing the need to remember login ID's and passwords (or storing passkeys), and hardening multi-factor authentication, anonymous authentication provides a seamless experience for the end user and fosters strong security. As digital interactions continue to evolve, embracing anonymous authentication presents an opportunity to redefine authentication paradigms and create more secure and privacy-respecting online environments.