

# Passkey Integration and Authentication - Vision/MRD Document

## Version Control Log

Date	Version	Author	Notes
Oct 30, 2024	Draft 1	@Kevin Fessler	Working draft for first collaboration workshop

## Table of Contents

- 1. Purpose
- 2. Involved Team Members
- 3. Market Context and Problem Definition
  - 3.1 Market Context
  - 3.2 Problem Definition
  - 3.3 Competitive Analysis
  - 3.4 Why should Match Group implement Passkey Functionality?
  - 3.5 Bumble Current State
- 5. Solution Vision
  - 5.1 Objectives
  - 5.2 Key Features
  - 5.3 Personas
  - 5.4 Use Cases
  - 5.5 User Journeys
  - 5.6 Technical Requirements
  - 5.7 Assumptions, Questions, and Risks
- 6. Design Ideation
  - 6.1 Analysis
  - 6.2 Scope
  - 6.3 Timeline & Milestones

# 1. Purpose

The purpose of this document is to provide vision and context to enhance user security and authentication efficiency by integrating passkeys into our portfolio of mobile app brands. Passkeys will provide a passwordless, device-specific, and phishing-resistant method for users to authenticate themselves using biometric verification (such as fingerprint or facial recognition).

## 2. Involved Team Members

Who is participating in workshop preparation meetings to refine this document?

@Kevin Fessler

@Beomjun Shin

@Scott Alverson

@Tricia Parker

@Pete Hamblett

## 3. Market Context and Problem Definition

### 3.1 Market Context

The market for secure and convenient authentication solutions is rapidly evolving as users become more aware of the risks associated with traditional password-based systems. High-profile data breaches and the growing sophistication of phishing attacks have heightened the need for more advanced security measures. Passkeys, which replace passwords with device-based, cryptographic authentication methods, have emerged as a promising solution.

Companies like Google and Microsoft have already started adopting passkey technology, integrating it into their ecosystems to provide users with a seamless and secure login experience. Apple's introduction of passkey support in iOS 17 further signals a major shift toward this new authentication standard, positioning passkeys as the future of online security.

Businesses across various industries are beginning to see the strategic value in adopting passkey authentication. By leveraging this technology, companies can offer their users an efficient, frictionless login process while significantly reducing security vulnerabilities. The early success of passkey implementations in platforms like Google Chrome and Microsoft Authenticator demonstrates the technology's potential to enhance user satisfaction and trust. As more organizations recognize the benefits of transitioning to passwordless authentication, the market landscape is expected to shift toward widespread adoption, with companies that implement passkeys early gaining a competitive advantage in security and user experience.

## 3.2 Problem Definition

Traditional password-based authentication methods expose users to significant security risks, such as phishing attacks, credential theft, and password reuse. Our current authentication system requires complex password management, leading to a subpar user experience and potential security vulnerabilities. With the introduction of passkeys supported by iOS 17, we have an opportunity to simplify user login and strengthen account security by implementing a modern, device-based authentication method.

### 3.2.1 Problems we want to solve:

#### **Improve Security:**

Eliminate risks associated with password-based authentication, making accounts more secure.

#### **Enhance User Experience:**

Simplify the login process by using biometric authentication and reducing friction.

#### **Increase DAU (Daily Active Users):**

Make the authentication process seamless to encourage more frequent app usage.

## 3.3 Competitive Analysis

As of October 2024, the adoption of passkey authentication among major dating apps outside the Match Group is as follows:

- **Bumble:** Currently, Bumble has not yet implemented passkey authentication. Users continue to authenticate using traditional methods, such as email and password combinations or social media account integrations.
- **Grindr:** Grindr has not publicly disclosed the implementation of passkey authentication. Users typically log in using email and password credentials or through linked social media accounts.
- **Coffee Meets Bagel:** There is no available information suggesting that Coffee Meets Bagel has adopted passkey authentication. The platform continues to use conventional authentication methods, such as email and password logins.

In summary, while passkeys offer enhanced security and a streamlined user experience, major dating apps outside the Match Group have yet to adopt this authentication method. They continue to rely on traditional login mechanisms, including email and password combinations and social media account integrations.

## 3.4 Why should Match Group implement Passkey Functionality?

Based on the above market analysis, integrating Passkeys into our brand portfolio would place our apps at the forefront of our Trust & Safety objectives.

## **Customer Benefits**

Integrating passkey-based authentication offers significant advantages for both the customer experience and the business. For customers, the experience is vastly improved through a simplified and secure login process, eliminating the need to remember complex passwords. Users benefit from reduced anxiety about security threats, as passkeys are resistant to phishing and credential theft. Additionally, the use of biometrics makes authentication quick and effortless, providing a smooth and user-friendly interaction that enhances satisfaction and builds trust in our apps.

### **Trust & Safety:**

Enforcing robust passkey rules and biometric authentication methods increases user confidence in the app's security measures. This, in turn, promotes a sense of trust and safety, reducing the likelihood of fraudulent activities or unauthorized account access. A secure platform attracts more genuine users, fostering a safer and more reliable dating environment.

### **Enhanced User Experience & Stickiness:**

The seamless login experience provided by passkeys and biometric authentication significantly enhances user satisfaction. By removing the friction associated with remembering and typing passwords, users are more likely to engage with the app frequently. This ease of access increases app stickiness, making it more attractive for users to return and interact regularly.

## **Match Group Benefits**

For the business, implementing passkeys boosts overall security, significantly lowering the risk of data breaches associated with traditional password-based systems. This improvement reduces support costs related to account recovery and fraud management, allowing the organization to allocate resources more efficiently. Furthermore, the streamlined authentication experience drives user engagement and retention, increasing daily active users (DAU) and promoting long-term customer loyalty, which can ultimately enhance revenue and brand reputation.


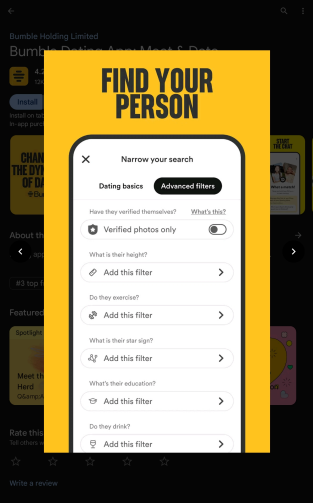
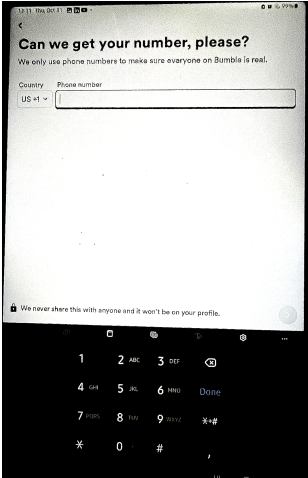
### **Operational Efficiency:**

Automating security features, passkey setup, and user authentication processes reduces the need for manual interventions or user support for account recovery and security issues. By streamlining these processes, the dating app can allocate resources more efficiently, focusing on developing new features and enhancing the overall user experience.

### **Increased Revenue:**

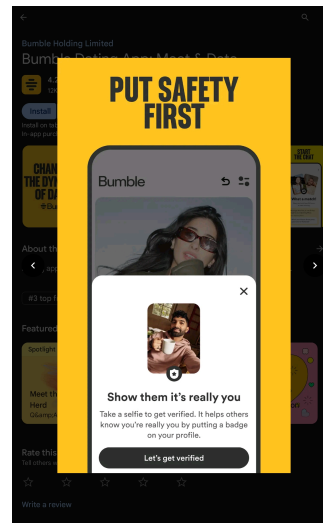
A more secure and user-friendly experience can lead to higher user retention and engagement, ultimately increasing revenue through subscription renewals, in-app purchases, and premium features. Additionally, by building trust and ensuring safety, the app can attract more high-value users willing to pay for enhanced services, contributing to long-term revenue growth.

3.5 Bumble Current State

<div><p><b>Passkey Overview / Dashboard</b></p><p>App allows biometric login</p></div>	<div></div>
<div><p><b>Passkey Dashboard</b></p><p>App allows configuration of filters and profile details</p></div>	<div></div>
<div><p><b>Phone Number Input</b></p><p>The app uses phone and SMS to verify identity</p></div>	<div></div>

### Phone Number Input

App encourages users (not required) to verify their profile with additional checks



## 5. Solution Vision

### 5.1 Objectives

Our goals and objectives center on enhancing both security and user experience by implementing passkey-based authentication. We aim to eliminate the risks associated with traditional passwords, such as phishing and credential theft, by using device-specific, passwordless technology. At the same time, we seek to streamline the login process, making it effortless for users through biometric verification. By simplifying authentication, we expect to increase daily active users (DAU) and drive engagement higher, as users will appreciate the seamless and secure experience provided by our brands.

### 5.2 Key Features

The integration of passkey-based authentication into our mobile app introduces a new level of security and convenience for our users. By replacing traditional passwords with passkeys, we address common vulnerabilities such as phishing, credential theft, and password fatigue. Passkeys utilize device-specific cryptographic keys and biometric verification, making them both highly secure and user-friendly. This innovative approach ensures that users can quickly and seamlessly log in to their accounts, while also significantly reducing the risk of unauthorized access.

The features focus on creating an effortless user experience without compromising security. Users can easily set up a passkey during the account sign-up or login process, with the app guiding them through biometric verification to save their unique passkey securely on the device. Logging in becomes frictionless, as the app automatically detects stored passkeys and prompts users for biometric authentication, eliminating the need for remembering or managing complex passwords. By leveraging Apple's latest passkey support in iOS 17, we aim to simplify authentication and drive higher engagement by offering a smooth and secure login experience.

### 5.2.1 Passkey Creation and Setup

- Users will be prompted to create a passkey during the account sign-up or login process.
- The system will use device biometrics (e.g., Face ID, Touch ID) to verify identity and save the passkey on the device.
- The passkey will be stored securely in the user's device keychain.

### 5.2.2 Effortless Login

- Users will be able to log in effortlessly using biometrics.
- The app will automatically detect a stored passkey and prompt the user to authenticate with their fingerprint or facial recognition.

### 5.2.3 Device-Specific Authentication

- Passkeys will be device-specific and will not be transferable across devices unless manually set up by the user on additional devices.
- Passkeys will be resistant to phishing and other credential-based attacks.

## 5.3 Personas

### Emily, 28 – The Young Professional

- **Background:** Emily is a marketing manager living in a busy urban area. She works long hours and prefers using dating apps to meet potential partners who share her lifestyle and values.
- **Goals:** Find meaningful connections with people who have similar ambitions and interests. She values privacy and wants to ensure her personal data is secure.
- **Behavior:** Checks the app daily, values convenience, and prefers quick and seamless login processes. Often switches between devices, such as her phone and tablet, throughout the day.

### Jake, 33 – The Outdoor Enthusiast

- **Background:** Jake works as a software engineer and spends his weekends hiking, rock climbing, and traveling. He uses dating apps to meet people who enjoy outdoor adventures as much as he does.
- **Goals:** Connect with adventurous and like-minded people who are active and love the outdoors. He appreciates user-friendly features that make managing his profile and messages efficient.
- **Behavior:** Uses the app a few times a week, usually when planning his weekends or during evenings. Values security but may be less tech-savvy when it comes to understanding new authentication methods.

## Mark, 40 – The Single Parent

- **Background:** Mark is a single dad who works as a sales manager. Balancing work and parenting leaves him with little time to date, so he uses dating apps to meet new people when he has a free evening or weekend.
- **Goals:** Find someone who understands the challenges of being a parent and is looking for a serious relationship. Prioritizes safety and security for himself and his children's privacy.
- **Behavior:** Uses the app a few times a week, mostly in the evenings after his kids are asleep. Appreciates efficient, secure login methods and wants the reassurance that his information is protected.

## 5.4 Use Cases

### 5.4.1 Emily, The Young Professional

- **Use Case 1: Quick and Secure Login**
  - **Scenario:** Emily wants to quickly log in to the dating app during a short break at work.
  - **Steps:**
    1. Emily opens the app and is immediately prompted to authenticate using Face ID.
    2. She completes the biometric verification and is logged in within seconds, ready to check her messages.
  - **Outcome:** Emily appreciates the speed and security of the login process, making her more likely to use the app frequently.
- **Use Case 2: Switching Between Devices**
  - **Scenario:** Emily needs to log in to the dating app on her tablet for a larger view while relaxing at home.
  - **Steps:**
    1. Emily sets up a passkey on her tablet using Face ID.
    2. The app securely syncs her passkey, ensuring she can use biometric login on both her phone and tablet.
  - **Outcome:** Emily experiences a seamless transition between devices, enhancing her user experience.

### 5.4.2. Jake, The Outdoor Enthusiast

- **Use Case 1: Effortless Biometric Authentication**
  - **Scenario:** Jake wants to log in to the app to check for new matches before heading out for a weekend hike.
  - **Steps:**
    1. Jake opens the app and is prompted to authenticate using fingerprint recognition.
    2. He quickly verifies his identity and checks his matches.
  - **Outcome:** Jake enjoys the ease of login and feels secure knowing his account is protected.
- **Use Case 2: Understanding Passkey Setup**
  - **Scenario:** Jake is not familiar with passkey technology and needs guidance when setting it up.



- **Steps:**
  1. The app provides a simple tutorial explaining what a passkey is and how to set it up.
  2. Jake follows the instructions, sets up his passkey, and feels more confident using the app.
- **Outcome:** Jake successfully sets up the passkey and feels reassured about the security of his account.

### 5.4.3. Mark, The Single Parent

- **Use Case 1: Secure Login After a Long Day**
  - **Scenario:** Mark wants to unwind and check his matches after putting his kids to bed.
  - **Steps:**
    1. Mark opens the app and is prompted to log in using Face ID.
    2. He verifies his identity and accesses the app securely without having to remember a password.
  - **Outcome:** Mark appreciates the convenience and security, especially when he's tired and wants a hassle-free experience.
- **Use Case 2: Account Recovery and Security**
  - **Scenario:** Mark loses his phone and is concerned about the security of his dating app account.
  - **Steps:**
    1. Mark uses his new device to access the app and follows the account recovery steps.
    2. He re-establishes his passkey using Face ID on the new device, ensuring his account remains secure.
  - **Outcome:** Mark is reassured that his account is protected even when switching devices.

## 5.5 User Journeys

### 5.5.1 User Journey: Setting Up a Passkey

Step 1: User opens the app and starts the sign-up or login process.

Step 2: The app prompts the user to create a passkey for secure and seamless login.

Step 3: The user is asked to verify their identity using the device's biometric feature (e.g., Face ID or Touch ID).

Step 4: Upon successful biometric verification, a passkey is generated and securely stored on the device.

Step 5: The app confirms the passkey creation and provides information on how it will be used for future logins.

### 5.5.2 User Journey: Logging In with a Passkey

Step 1: User opens the app and taps the "Log In" button.

Step 2: The app detects the stored passkey and prompts the user to authenticate using biometrics.

Step 3: The user verifies their identity with Face ID or Touch ID.

Step 4: The app logs the user in automatically and directs them to the home screen.

## 5.6 Technical Requirements

- **Server-Side**

- Implement support for passkey authentication protocols (e.g., WebAuthn).
- Update backend systems to recognize and manage device-specific passkey credentials.
- Ensure secure communication and key exchange mechanisms between the app and the server.

- **Client-Side (Mobile App)**

- Integrate iOS 17 passkey APIs for secure key storage and biometric authentication.
- Build UI components for passkey setup, biometric prompts, and user guidance.
- Ensure compatibility with existing security and account management features.

- **Passkey Certificates & Security**

- **Types of Certificates Used:** To ensure secure communication between the mobile app and servers, several types of digital certificates and encryption methods will be used:
  1. **SSL/TLS Certificates:** These certificates will secure data transmission between the mobile app and servers, encrypting all data exchanged to prevent interception by unauthorized parties. By using SSL/TLS, the app can establish a secure, encrypted channel for sensitive information, such as user authentication and passkey verification data.
  2. **Device Authentication Certificates:** Certificates tied to the user's device will validate the device's identity when interacting with the server. These certificates ensure that only authorized devices can communicate with the server, adding an extra layer of security.
  3. **Passkey-Specific Certificates:** Certificates unique to each passkey may be used to sign and validate authentication requests, ensuring that the passkey generated on the user's device is legitimate and untampered.
- **Relationship Between Passkey and Server's Public Key Infrastructure (PKI)**

The passkey stored on the user's device consists of a unique, cryptographically generated key pair: a **private key** stored securely on the device and a **public key** registered with the server.

  1. **Private Key:** The private key never leaves the user's device and is used for signing authentication requests. It is stored in a secure enclave or keychain protected by the device's operating system. The device uses biometric verification (e.g., fingerprint or facial recognition) to unlock access to the private key, ensuring only the legitimate user can initiate authentication.
  2. **Public Key:** The corresponding public key is sent to the server during passkey setup. It is integrated into the server's public key infrastructure (PKI) and used to verify the signatures generated by the private key. The server uses the public key to authenticate requests and confirm that they originated from the correct device and user.

This relationship ensures that even if data transmitted between the app and server is intercepted, the private key cannot be compromised, as it remains securely stored on the user's device. The use of PKI also allows the server to confidently verify the identity of the user without the need for transmitting or storing passwords, thereby enhancing overall security and reducing vulnerabilities.

- **Analytics & Success Metrics**

- Track the adoption rate of passkeys vs. traditional login methods.
- Monitor biometric authentication success/failure rates.
- Measure the impact on DAU (Daily Active Users) and app engagement.

## 5.7 Assumptions, Questions, and Risks

### Assumptions

1. Users will be familiar with biometric authentication features on their devices (e.g., Face ID, Touch ID) and will be comfortable using them for passkey-based login.
2. Passkey technology will continue to be supported and developed by major platform providers like Apple and Google, ensuring compatibility with future software updates.
3. The majority of our user base has access to devices that support biometric authentication and passkeys, minimizing the need for extensive backward compatibility with older devices.

### Questions

1. How should we handle users who do not have passkey-compatible devices or choose not to use biometric authentication? Are there alternative secure login methods we should implement?
2. Will implementing passkeys impact our app's performance or require significant changes to our existing infrastructure?
3. How do we educate users about the benefits and functionality of passkeys to ensure widespread adoption and minimize confusion during the transition?

### Risks

1. **Adoption Risk:** Users may be hesitant to switch to passkey authentication due to a lack of understanding or comfort with the new technology, potentially leading to lower adoption rates.
2. **Compatibility Risk:** Older devices or specific operating systems that do not support passkey technology may pose challenges, affecting a segment of our user base.
3. **Security Risk:** If a user's device is lost or compromised, there is a risk that unauthorized individuals could access the user's account, even with biometric authentication. Contingency measures must be implemented to address such scenarios.

## 6. Design Ideation

### 6.1 Analysis

#### 6.1.1 Proposed Solution:

The proposed solution involves integrating passkey-based authentication into the dating app to replace traditional password methods. This approach leverages device-specific cryptographic keys and biometric verification, such as Face ID and Touch ID, to provide a seamless, secure login experience. The user journey will be enhanced by eliminating the need for passwords, streamlining account access, and providing peace of mind with modern security measures. The integration will also include a guided onboarding process for passkey setup and account recovery mechanisms for users who lose their devices.

---

#### Open Questions and Options Based on Model and Flow

##### 1. How Do We Handle Account Recovery?

- **Option 1:** Implement a secure recovery method that uses a trusted email or SMS-based link.
- **Option 2:** Allow users to register a backup device for passkey access and recovery.
- **Consideration:** The chosen option must balance security with ease of use, ensuring that users can recover access without compromising account protection.

##### 2. What is the Best Way to Educate Users About Passkeys?

- **Option 1:** Provide an in-app tutorial during the setup process, including animations or videos explaining passkey benefits.
- **Option 2:** Offer a dedicated help section with FAQs and troubleshooting guides.
- **Consideration:** Effective education is critical to drive adoption, especially for users unfamiliar with passkey technology.

##### 3. How Do We Manage Multi-Device Support?

- **Option 1:** Enable users to manually set up passkeys on additional devices with biometric authentication.
  - **Option 2:** Delay full multi-device syncing and focus on single-device passkey functionality for the initial release.
  - **Consideration:** The initial focus should be on delivering a robust single-device experience, with multi-device support considered for future updates.
-

## Impact of This Solution on User Journeys

1. **Enhanced Security and Convenience:** Users like Emily will experience a quicker and more secure login, reducing friction and making the app more appealing to use frequently. This will likely increase user engagement and daily active users (DAU).
2. **Effortless Login for Busy Users:** For personas like Mark, who value convenience, biometric authentication simplifies account access, providing a hassle-free experience, even at the end of a long day. This positive impact can boost overall user satisfaction and retention.
3. **Confidence in Account Protection:** Users like Jake who are concerned about security and use the app in various environments, will benefit from knowing that their accounts are protected against phishing and other attacks. This assurance can build trust in the app and encourage more consistent usage, even from different locations or on-the-go.

## 6.2 Scope

### 6.2.1 What is Included?

1. **Passkey Integration for Authentication:** The implementation of passkeys for secure, device-specific login using biometric verification methods, such as Face ID and Touch ID.
2. **User Onboarding and Setup:** A guided setup process for creating and saving passkeys, including educational content to help users understand the benefits and functionality.
3. **Biometric Login:** Users will be able to log in effortlessly using biometrics, providing a seamless and passwordless experience.
4. **Account Recovery with Passkeys:** A secure account recovery process for users who lose their devices, including steps to re-establish their passkey on a new device.
5. **Security Notifications:** Alerts and notifications for users in case of unusual login attempts or account activity, ensuring heightened awareness and control over account security.
6. **Multi-Device Support:** Limited support for setting up passkeys on multiple devices, ensuring ease of use for users who frequently switch between devices.

### 6.2.2 What is Explicitly Out of Scope?

1. **Integration with Non-Biometric Devices:** Supporting passkey setup and login on devices that do not have biometric authentication capabilities is not included in this release.
2. **Cross-Platform Passkey Synchronization:** Automatic syncing of passkeys across different operating systems (e.g., syncing between iOS and Android devices) will not be supported.
3. **Support for Legacy Passwords:** Maintaining or enhancing legacy password-based authentication methods is out of scope, except for basic account recovery needs.

4. **Advanced Multi-Factor Authentication (MFA):** Implementation of additional MFA methods, such as SMS or email-based authentication, is not part of this project.

### 6.2.3 Other Related Passkey Enhancements (Future Scope)

1. **Cross-Platform Passkey Synchronization:** Developing features to enable seamless passkey syncing across both iOS and Android ecosystems.
2. **Integration with Wearable Devices:** Expanding passkey support to smartwatches and other wearable devices for more authentication options.
3. **Customizable Security Settings:** Allowing users to adjust their security preferences, such as setting up multiple passkeys for different devices.

### 6.2.4 Other Related but Out-of-Scope Enhancements

1. **Integration with Third-Party Password Managers:** Compatibility or integration with external password management tools is not included.
2. **Offline Passkey Authentication:** Support for using passkeys in offline mode, without internet access, is out of scope.
3. **Enhanced Biometric Options:** Development of new biometric authentication methods, beyond Face ID and Touch ID, such as voice recognition or retinal scanning, will be considered in future releases.

## 6.3 Timeline & Milestones

- **Phase 1:** Research & Development (2 weeks)
- **Phase 2:** Supporting Backend Implementation (3 weeks)
- **Phase 3:** Client-Side Development & Adoption of Backend Changes (4 weeks)
- **Phase 4:** Testing & QA (2 weeks)
- **Phase 5:** A/B Testing and Analysis in Production (2 weeks)
- **Phase 6:** Launch & User Education (1 week)