transmit security

Buyer's Guide:

How to Select a Passwordless Customer Authentication Service

Your guide to identifying, evaluating and selecting the right passwordless solution for your customers.

Password-based authentication is inherently vulnerable to attacks that target the weakest link in the security chain — the user. It's inevitable that customers are going to make mistakes when it comes to their passwords. Most reuse passwords multiple times or fail to make them strong enough. **The average consumer reuses the same password up to 14 times**.[1] In a phishing attempt, they might even hand over their passwords unknowingly.

On top of the security risks, passwords damage the user experience, which negatively impacts business. Customers can't check out if they've forgotten their password and don't want to hassle with recovery. A complicated sign in process with SMS one-time passcodes (OTPs) scares off potential customers who may never return. In fact, **55% of customers have stopped using a website due to the complicated login process**.[2]

To optimize security and the customer experience, a passwordless customer authentication service is essential. By verifying customer identities with confidence, you'll reduce the risk of fraud and resolve the problem of passwords for both customers and organizations.

In many cases, security and the customer experience are at odds with each other. We've created this guide for you to decipher if the passwordless authentication service option you are considering includes the core requirements needed to meet both your security and customer experience needs.

1 https://securityboulevard.com/2020/04/8-scary-statistics-about-the-password-reuse-problem/

2 https://www.transmitsecurity.com/content-hub/the-impact-of-passwords-on-your-business

Defining passwordless

The term ‘passwordless’ is thrown around a lot these days, but what does it actually mean? When we say passwordless, we don’t mean that passwords are used less. We’re talking about the **complete and final elimination of passwords** in the entire customer authentication journey.

Why your business needs a passwordless customer authentication service

- Eliminate all forms of password-related risk and fraud
- Provide greater assurance customers are truly who they say they are
- Minimize customer attrition and build loyalty by offering customers a quick and easy way to access their accounts across all apps, channels, devices and browsers
- Reduce the operating costs associated with support calls, password resets and overly complex identity stacks

How your customers benefit from a passwordless experience

- Guarantee ironclad security across all accounts with no weak or reused passwords in sight
- Deliver a frictionless, pain-free passwordless experience across all channels, devices and apps — every time!
- Simplify logins with a familiar and trusted method across all apps and channels
- Easily recover accounts without the frustration of forgotten passwords

Core requirements of a passwordless customer authentication service

1. Passwordless: no passwords — anywhere
2. One identity, across all devices
3. Cross-channel on any devices, apps and domains
4. Authenticate customers instantly with one-step multi-factor authentication
5. Flexible to be used app-less, or as an app
6. Easy to integrate with existing identity systems
7. Deploy quickly — weeks to months, not months to years

1.

Passwordless: no passwords — anywhere

In order to improve the customer experience and reduce risks, **a customer authentication service should be 100% free of passwords**. That means no passwords in the entire authentication journey, including the enrollment and account recovery process. Many customer authentication services provide passwordless experiences, however they still store passwords in the underlying architecture. If there are passwords anywhere, the risk and frustration of passwords will persist, with password-based attack vectors still open for exploitation.

Why it's essential:

Passwords are the leading driver for all security breaches and invite the risk of account takeovers and fraud. With the growing sophistication of cyberattacks, passwords are the easiest target to exploit. A single customer breach can damage trust and ruin your brand reputation. By removing passwords and all shared secrets, your business can mitigate all risks and costs involved.

Key questions to ask:

1. Does the solution store any passwords in the infrastructure?
2. Do my customers need to create a password when they create an account?
3. What is the fallback authentication method for customers?
4. What does the account recovery process look like for a customer?

2.

One identity, across all devices

Your customer should only have to register once, and only once, and then be able to transfer trust to other devices they own. This process creates a single identity for the customer no matter which device they are using. The majority of passwordless services available today force the customer to register each device independently under a new and separate account, often using password-based credentials. They do this for each and every application too, resulting in more identities than you actually need (or want).

Why it's essential:

Considering that the average household has 25 connected devices,[1] the need to seamlessly authenticate from every device is imperative. Too often the customer experience is fragmented and frustrating. In some cases a customer will have many identities with the same business: one for a mobile app, one for the store and a third for support. When authentication is based on identity and not by device, all complexity, including re-registering, is removed. With the right passwordless solution, you can create a smooth journey across all channels.

Key questions to ask:

1. How do you ensure every customer has only one user identity?
2. Does your customer have to re-register their account on every new device?
3. How do you create a passwordless experience across various devices, apps and domains?
4. Does your authentication scenario rely on the device alone?

1 https://www.telecompetitor.com/report-connected-devices-have-more-than-doubled-since-2019/

3.

Cross-channel on any devices, apps and domains

Customers should be able to move seamlessly between apps, channels and devices with little to no friction. Whether it's on the web, mobile apps, incognito browsers or offline channels like call centers or kiosks, **customers must be quickly recognized each and every time with the same identity for a consistent cross-channel experience.** Meeting this requirement has been historically intractable, with digital and non-digital interactions requiring different authentication methods, and underpinned by different technology stacks. Your passwordless methodology needs to be universally leveraged from any channel, promoting consistency of security and user experience.

Why it's essential:

When customers are unable to easily login to an account using the device or browser available, they flee. The idea of a dreaded password reset is enough to make them never return, resulting in high levels of customer attrition. By enabling a cross-channel authentication service, customers can benefit from an improved ease of use paired with a higher level of security.

The same is true for offline experiences. Matching the offline authentication experience, like calling into a call center, to the online experience is essential for a smooth and familiar experience.

Key questions to ask:

1. Do you provide a unified passwordless experience across all digital and offline channels?
2. Do users have to re-register on new devices and channels?
3. Do customers have to re-authenticate when they switch between browsers or devices?
4. Are you able to provide a passwordless experience throughout changes to the domain state, such as incognito mode or cleared cookies?

4.

Authenticate customers instantly with one-step multi-factor authentication

By replacing antiquated methods with a passwordless service, organizations can rid their entire customer authentication journey of complex, costly and friction-filled methods like passwords backed by SMS OTPs executed in onerous step-up journeys. **Authenticating customers via passwordless authentication, on the other hand, enables MFA in a single click**; the device is the "what you have" factor and the biometrics are the "who you are" factor.

Why it's essential:

Legacy two-factor authentication (2FA) methods are still based on something you have, which ultimately reduces down to shared secrets. These shared secrets are easily intercepted, stolen or compromised just like passwords. OTPs and knowledge-based authentication (KBA) also present another point of failure. If the customer doesn't receive the OTP or fails to correctly answer their own questions, they can't login and you've lost their business.

By implementing a passwordless service you're able to offer stronger security as well as a seamless customer experience free of SMS OTPs, KBAs and other annoying, friction-filled hurdles.

Key questions to ask:

1. Does your passwordless solution exhibit "pure passwordless" attributes, enabling inherent MFA in one click?
2. How many steps does it take for customers to set up and verify their identities with multiple factors?
3. Is it possible for the MFA method to be intercepted?
4. How much friction does the MFA step present?

5.

Flexible to be used app-less, or as an app

The service of choice should allow organizations the flexibility to **decide** whether or not to be used with or without an app. If the app route is taken, the service needs to enable easy integration with the organization's existing mobile app. If the app-less route is taken, protocols such as WebAuthN and FIDO become crucial components in your technology stack, as passwordless can now be activated using common browsers already installed in a user's operating system.

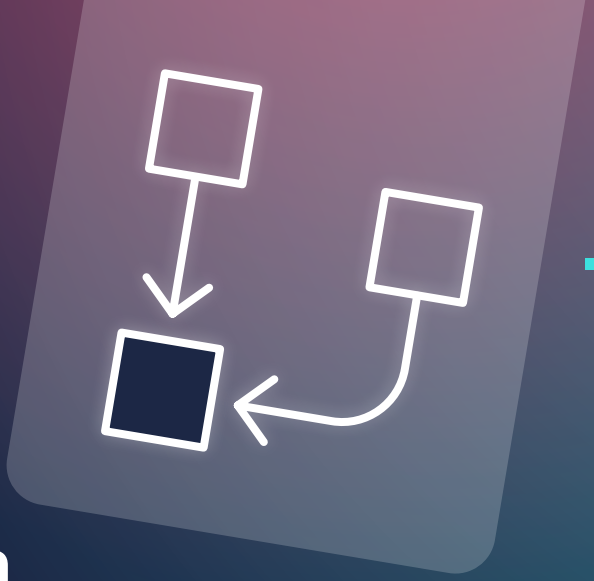
Why it's essential:

The flexibility to be used as an app or app-less is imperative to ensure that the passwordless service is aligned with the company's mobile strategy. Organizations should have the option to offer the experience that customers want and the level of security they need. It could be that you don't want your customers to have to download another app or that you want the passwordless service to be integrated into your existing customer app.

Key questions to ask:

1. How does your customer authentication service help improve my mobile adoption strategy?
2. Does your customer authentication service offer the flexibility to be used app-less or as an app?
3. Is it easy to integrate with my existing app?
4. Does your authentication service require customers to download software to their device?

6.



Easy to integrate with existing identity systems

Organizations usually have incumbent CIAM systems already in place, so adding a passwordless login experience for customers must be able to work with existing technologies. **Flexibility, agility and the capacity to easily integrate a passwordless service is crucial to sustaining existing authentication systems, lowering deployment risk and ensuring continuity of service**. Augmenting with passwordless should not be complex, costly nor require undue effort.

Why it's essential:

As technology, security and customer expectations evolve, your organizations need solutions that can readily adapt to their ever-changing security and customer experience strategies. It is critical for any business to ensure identity systems are integrated to simplify management and to also have a holistic view of their entire identity stack.

Key questions to ask:

1. Does your service integrate with my existing identity provider?
2. How flexible is your service to integrate?
3. Am I able to customize the service in alignment with my own branding?
4. How can I incorporate the service with low risk to existing operations?

7.

Deploy quickly — weeks to months, not months to years

Typical customer identity management transformation programs require armies of developers and can take years to implement. This is often caused by the existence of many different application technologies, divergent security needs and a mix of legacy and home-grown systems bolted together. In order to avoid building everything from scratch, passwordless can be utilized to create consistency of integration, customer identity handling and a means of integration. With passwordless being an augmentation and not a rewrite, **your service should have the ability to be deployed quickly** — measured in weeks to months, not years.

Why it's essential:

Time is of the essence here. The sooner your business can implement a service, the sooner you can reap the benefits, realize the competitive advantages and reach your KPIs. The opposite is also true. A passwordless solution that is difficult to implement can drain resources, taking more of your budget, time and developers.

Key questions to ask:

1. How long does it take to deploy your customer authentication service?
2. How many resources will it require to deploy the service?
3. How much maintenance and management will the service require over time?
4. Does it simplify and speed integration by leveraging open standards?

BindID

The future of customer authentication

BindID is the only passwordless authentication service that allows customers to effortlessly access all channels with no passwords — anywhere.

An industry first, BindID creates a single customer identity and binds the identity across channels and devices, enabling customers to gain one-click passwordless access without the risk of account takeover fraud.

BindID provides a totally passwordless experience that carries the customer across all channels, while protecting user privacy. As the first app-less customer authentication service, BindID creates a frictionless identity experience without the need for complex changes at the web and application levels.

One of the most compelling aspects of BindID is the fact that it takes only days to integrate into all your existing channels. With ultra-fast implementation thanks to open standards, production can begin within weeks and with as little as one developer.

By using a combination of open standards and device biometrics, passwords are not created, used or stored anywhere — not in the front or back end experience and not even in the registration or device recovery process. This allows for easy, secure and portable customer authentication. It's native passwordless in action!

transmit security

Ready to implement the future of authentication?

Learn more about BindID today!