KuppingerCole Report

EXECUTIVE VIEW

By Alejandro Leal
June 22, 2022

Beyond Identity Secure Customers

Password authentication is not only insecure, but it leads to poor consumer experiences and is costly for organizations to maintain. As far as customer authentication is concerned, there are three main problems: friction, security, and legacy MFA solutions. Beyond Identity's Secure Customers provides a passwordless MFA authentication solution that protects customers against account takeover fraud by eliminating passwords, one-time codes, push notifications, and second devices on native and web applications.

By **Alejandro Leal**

Content

1 Introduction

Over the last decade, organizations have found it necessary to store data and information about business partners, suppliers, and customers in their own enterprise identity management systems. Consumer Identity and Access Management (CIAM) solutions are designed to meet evolving technical requirements for businesses and other organizations that deal directly with consumers and citizens. However, CIAM systems generally feature weak password-based authentication, but modern solutions can also support social logins and other stronger authentication methods.

In order to increase security, comply with new regional and industry-specific regulations, and improve customer experiences, organizations are adopting CIAM solutions. CIAM systems must be able to manage many millions of identities, and process potentially billions of logins and other transactions per day. Nonetheless, the problem with existing solutions of customer authentication is that they do not eliminate the root cause of friction and security risk - the password.

The practice of typing passwords to access applications and services has become a regular part of the daily routine of millions of users. Since the early days of the internet, however, the use of passwords has introduced a number of weaknesses and security challenges. In many organizations, users have a tendency to keep their passwords simple, easy to remember, and reuse them across applications, which puts the user and the overall organization's security at risk.

As a result, many businesses and organizations are increasingly looking for better solutions for authenticating those users. Although the introduction of multi-factor authentication (MFA) has often been regarded as a remedy to security issues, the adoption rate of MFA solutions on the customer side has been surprisingly slow. On top of that, legacy MFA that uses passwords as a first factor are vulnerable to social engineering, SIM swaps, and man-in-the-middle attacks. Since attackers are continuously finding new ways to bypass MFAs of all types, it is important to understand the pitfalls of legacy MFA and how important it is to choose the right solution for your organization.

This proliferation of threats has led the U.S. government to recently introduce a memorandum on how to achieve a zero trust architecture strategy. According to the document, agencies and organizations should integrate and enforce MFA across applications involving authenticated access to federal systems by agency staff, contractors, customers, and partners. Furthermore, the memorandum places significant emphasis on stronger enterprise identity and access controls, including the use of strong authentication and phishing-resistant MFA while specifically calling out the vulnerabilities of one-time codes and push notifications against phishing attacks.

In recent years, however, passwordless authentication has proven to be a very simple and safe alternative. Passwordless authentication solutions should provide organizations with a smooth and frictionless user experience, but not at the expense of security. Passwordless solutions vary in the technology they leverage to remove the password - some do not fully eliminate the password as it is still used for recovery while others allow for complete password elimination. It is therefore important for organizations to choose the right passwordless solution that meets their unique challenges and needs around user experience, security and risk tolerance, and technology stack.

By eliminating passwords and phishable factors, Beyond Identity offers Secure Customers, which is a secure and frictionless authentication solution. Its invisible passwordless MFA enables companies to secure access to applications and critical data with dynamic risk-based access decisions, make credential-based attacks and account takeover fraud extremely difficult to execute by fully eliminating the password, and dramatically improve the user experience with no need for one-time passcodes (OTP), push notification, and second devices.

2 Product Description

Beyond Identity was founded in early 2019. They are headquartered in New York and have offices and customers around the world. As an innovator in passwordless MFA solutions, Beyond Identity breaks down the barriers between identity, security, and device management. Launched in September of 2021, their Secure Customers solution offers a broad range of capabilities including the ability to:

- Accelerate conversions at registration, login, checkout, and recovery
- Secure customer accounts
- Protect customer privacy
- Drastically reduce account takeover fraud
- Implement adaptive access control

Today, many organizations are finding that they must deliver better digital experiences and gather more information about the customers who are using their services while providing security at the same time. The challenge for strong authentication and MFA solutions is to find a win-win solution between security and convenience. Therefore, in order to implement MFA more securely and conveniently, passwords should be removed from the equation altogether and customers should be authenticated by two strong factors - \"something you are\" and \"something you possess.\"

Secure Customers is deployed through embeddable SDKs, which are available for both native mobile and web applications. This allows companies to deliver a branded first-party native experience across all of their applications to accelerate conversions throughout the user journey while providing protection from account takeover fraud. Furthermore, as part of the registration process, public-private keys and certificates are automatically generated in order to conduct immutable identity bindings and validate two strong factors to securely authenticate the user for every authentication request**.**

Upon registration, the user receives a binding token that prompts the creation of a unique, device-bound credential with a private key generated and stored in the Trusted Platform Module (TPM) or other secure element, depending on the technical platform, and a public key sent to the Beyond Identity Cloud. This binding token can be delivered via a variety of methods including email or in-app depending on the appropriate user workflows per company requirements.

During authentication, Beyond Identity issues a challenge signed by the private keys in the device's hardware TPM, evaluates user and device security risk in real-time, and makes a risk-based access decision based on security requirements.

By employing their self-signed X.509 certificates on endpoint devices, this innovative and differentiat~~ed~~

solution extends the server-to-server chain of trust established with Transport Layer Security (TLS) to users and their devices. Following the creation of the private key, the private key is securely stored in the TPM of the personal device and used to sign the certificate. The certificate is then forwarded to the public cloud to be validated by the corresponding public key, which verifies that the certificate was issued from the same device.

Secure Customers provides an innovative implementation of asymmetric cryptography that underpins TLS to eliminate passwords from the customer experience and the organization's database. As a result, there is no need for passwords, one-time codes, push notifications, third-party authenticator downloads, or second devices required to authenticate. Using the self-signed X.509 certificate and the public-private key pairs ensures that users are in possession of only two attributes: \"something you are\" from the device biometric and \"something you own\" from the possession of a private key.

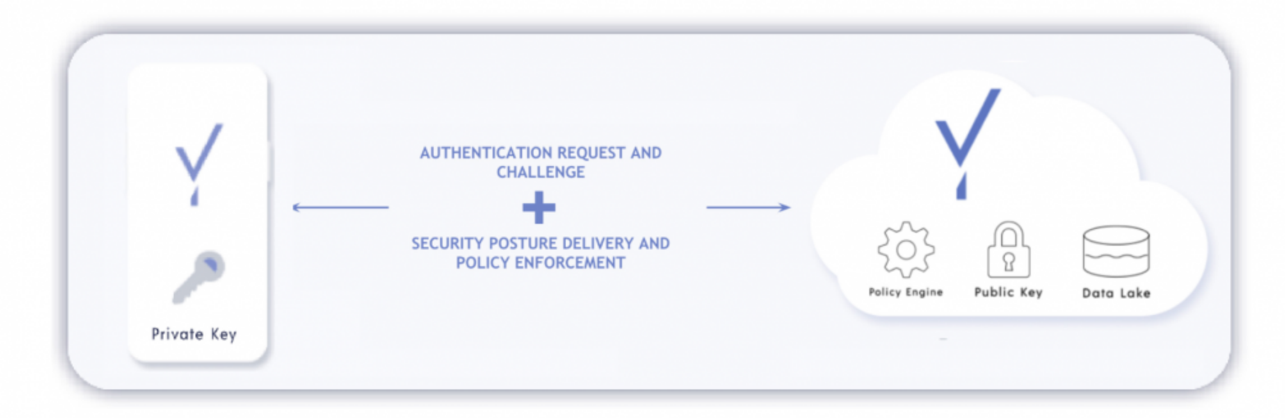
Private Key
AUTHENTICATION REQUEST AND CHALLENGE
+
SECURITY POSTURE DELIVERY AND POLICY ENFORCEMENT
Policy Engine
Public Key
Data Lake

Figure 1: The authentication flow of Beyond Identity Secure Customers [Provided by Beyond Identity]

Secure Customers also validates and ensures that each registered device is registered to a known and authorized user by continuously verifying whether or not the device meets the security requirements. The solution allows companies to capture and make dynamic access decisions based on customizable risk signals from the user and their device\'s security posture including presence of secure enclave, biometric authentication and firewall enablement, hard drive encryption status, application, and OS version, and more.

The solution is compliant with PSD2 Strong Customer Authentication, which is a new European regulatory requirement that aims to reduce fraud and make online and contactless offline payments more secure. Moreover, Beyond Identity uses OAuth 2.0 and OIDC protocols with downstream support for SAML to integrate with single sign-ons (SSOs) as a delegate identity provider. Going passwordless is not something that can be achieved in a single step, but Beyond Identity provides frictionless MFA and makes it easier for customers to authenticate and easier for development teams to implement.

As cybersecurity threats continue to ramp up, fraud and security breaches can cost businesses and organizations millions of dollars in addition to the long-term erosion of brand trust. Consequently, customers have been increasingly demanding more secure and convenient authentication methods. Secure Customers delivers a solution that makes it easier for customers to register without creating yet another password or picking up a second device. As a result, passwordless enrollment happens once and the only thing customers have to do is provide their email address to bind their identity to their device. This provides a safe, zero-friction, passwordless MFA that drastically reduces account takeover fraud and enhances the security of your organization.

3 Strengths and Challenges

Customers and organizations both want to reduce friction and increase security. One of the core challenges with passwords is that it puts the burden of authentication on customers while offering little in the way of security improvements given its inherent nature as a shared secret. With the technologies available today for passwordless authentication, businesses can offload the burden of authentication from individual customers and instead rely on proven security protocols and capabilities of modern devices including local biometrics and secure hardware enclaves.

Secure Customers makes it easier for customers and organizations to eliminate the reliance on passwords and the inconvenience of legacy MFA. However, one of the challenges facing Beyond Identity\'s Secure Customers is the capacity to be able to support legacy systems on premises that continue to rely on passwords. Also, it would be advantageous if Beyond Identity explores the application of identity proofing capabilities to strengthen the initial trust of user registration.

BEYOND IDENTITY

Strengths

- Frictionless user experience.
- Adaptive access control which evaluates user and device risk prior to login.
- Drastically reduce account takeover fraud by removing passwords from customer experience and database.
- Privacy-preserving credentials with tamper-resistant credentials backed by private keys.
- Strong authentication method with public-private key pairs and the use of asymmetric cryptography.

Challenges

- Lack of support for legacy systems that continue to rely on passwords.
- Lack of identity proofing capabilities and built-in features.

4 Related Research

Leadership Compass Consumer Authentication
Leadership Compass CIAM Platforms
Leadership Brief How to Get Rid of Passwords - Today

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.