KuppingerCole Report

EXECUTIVE VIEW

By John Tolbert

September 30, 2021

Keyless Biometric Authentication

Keyless specializes in advanced authentication technologies to help customers increase authentication assurance and decrease risks of data leakage. Keyless delivers passwordless authentication utilizing state-of-the-art biometrics and innovative cryptography that improves enterprise and consumer security and is user friendly.

By **John Tolbert**
jt@kuppingercole.com

Content

1 Introduction

As the number and severity of data breaches rise, businesses, governments, and other organizations seek to improve the authentication experience and raise assurance levels to mitigate against continuously evolving threats. Cyber-attacks put personal information, state secrets, trade secrets, and other forms of intellectual property at risk. Fraud against consumers and consumer-facing businesses has ramped up significantly. Increasing security and improving usability are the twin goals of modular authentication service upgrade projects. Data owners and IT architects have pushed for better ways to authenticate, based on changing business and security risks as well as the availability of newer technologies. Businesses have lobbied for these security checks to become less obtrusive and provide a better user experience (UX). Legacy IAM systems sometimes struggle not only to meet changing business requirements but also to keep up with the latest authentication technologies. This is especially true regarding legacy IAM solutions used by consumer-facing organizations. Many enterprises are choosing to augment their IAM systems by logically separating authentication from the IAM stack and utilizing discrete services that offer Multi-factor Authentication (MFA) with extensible risk analysis features informed by various types of intelligence. Many organizations are opting to deploy these capabilities in conjunction with their Identity-as-a-Service (IDaaS) solutions or as part of a "cloud-first" strategy.

MFA is the employment of multiple methods of determining that a user is who they are purporting to be in the context of an access request. Risk-adaptive authentication is the process of gathering additional attributes about users and their environments and evaluating those attributes in the context of risk-based policies. The goal of risk-based adaptive authentication is to provide the appropriate risk-mitigating assurance levels for access to sensitive resources by requiring users to further demonstrate that they are who they say they are. This is usually implemented by "step-up" authentication and/or the acquisition of additional attributes about the user, device, environment, and resources requested. Different kinds of authenticators can be used to achieve this, some of which are unobtrusive to the user experience. Examples of step-up authenticators include phone/email/SMS One Time Passwords (OTPs), mobile apps for push notifications, mobile apps with biometrics, Smart Cards or other hardware tokens, and behavioral biometrics.

Behavioral biometrics can provide a framework for login, in-app authorization (e.g. for online payments) and/or continuous authentication, by evaluating user behavior to a baseline set of patterns. Behavioral biometrics usually involves keystroke analysis, mobile "swipe" analysis, and even mobile gyroscopic analysis. These methods generally require the use of client-side agents, either standalone or embedded into applications as SDKs.

Solutions in this space can present multiple authentication schemes, methods, and challenges to a user or service according to defined policies based on any number of factors, for example, the time of day, the attributes of the user, their location, or the device from which a user or service attempts authentication. The

factors just listed as examples can be used to define variable authentication policies. User Behavior Analysis (UBA) employs risk-scoring analytics algorithms to first baseline regular access patterns and then be able to identify anomalous behavior which can trigger additional authentication challenges or attribute collection.

A wide variety of MFA mechanisms and methods exist in the consumer authentication market today. Examples include:

- Strong/Two-Factor or Multi-Factor Authentication devices, such as mobile biometric apps, and/or mobile apps that leverage operating system biometric capabilities,
- One-time passwords (OTP), delivered via phone, email, or SMS,
- Out-of-band (OOB) application confirmation, usually involving push notifications to mobile devices,
- Identity context analytics, including
    - IP address
    - Geo-location and geo-velocity
    - Device ID and device health assessment
    - User Behavioral Analysis (UBA)

Authentication and the related identity and context assurance values, then, can be considered a pre-cursor to authorization. The evaluation of these additional attributes can be programmed to happen in response to business policies, changing risk factors and regulation.

In the case of regulation especially, strong authentication and/or MFA are often required, with some industries more regulated than others -- for example, the financial industry. The EU Revised Payment Services Directive (PSD2) dictates that service providers in this sector must use "Strong Customer Authentication" (detailed below). In the US, the New York Department of Financial Services 23 NYCRR 500 has similar provisions for MFA.

Financial institutions are also subject to Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations in various jurisdictions globally. Compliance with these regulations requires collecting personal information about customers.

However, many countries and states within countries have regulations that are designed to protect the privacy of their citizens and residents when acting as consumers. The EU General Data Protection Regulation (GDPR) is one of the best-known privacy regulations, which imposes stiff penalties for non-compliance. In the US, the California Consumer Privacy Act (CCPA) and follow-on California Privacy Rights Act (CPRA) are models that are being enacted and/or explored by other states. Thus, the collection of personal information by consumer IAM and authentication systems must adhere to an expanding number of

privacy regulations.

In light of the above, one of the more recent additions to the authentication armory is "Passwordless" authentication. It is a popular term among product and service vendors today. Some passwordless options have been around for a while but are starting to be implemented more at enterprises and consumer-facing businesses. Passwordless options include the aforementioned biometrics and mobile push apps as well as simple possession of registered devices. Passwordless can also mean the evaluation of contextual risk factors without interrupting the user flow (in happy path flows). Passwordless methods provide security advantages and usability benefits. In the consumer facing market especially, innovation in authenticators that improve user-friendliness can be a competitive advantage.

A final, yet key consideration for authentication solutions is account recovery: when users forget passwords, lose credentials, or change devices, they need ways to get access to their accounts. Account recovery techniques include Knowledge-Based Authentication (KBA; but it is recommended to avoid this method as it is usually even less secure than password authentication), email/phone/SMS OTP, mobile push notifications, and account and device linking. Help desk assistance may also be needed on occasion, but it is a costly measure.

2 Product Description

Keyless was established in London in 2019 and is backed by leading VCs. They also have offices in Rome and Singapore. Keyless is focused on improving identity assurance by eliminating the use of passwords in the authentication process and leveraging tokenized authentication events. To that end, Keyless has developed biometric authenticators that can operate independently of operating systems and use advanced cryptographic methods to protect the authentication process and user privacy. Keyless adheres to many relevant standards and packages their product within platform specific SDKs. Keyless is available as both workforce/enterprise authentication and consumer authentication solutions.

The Keyless solution comprises three components: the Keyless Network, Authenticator and SDK.

The Keyless Network is SaaS that is hosted in AWS and Azure across APAC, EU, and NA regions. On-premise and private cloud deployment options are also available. Keyless is therefore geographically distributed to reduce latency and improve availability as well as being multi-cloud, which allows for continuous operation if a single IaaS provider has outages. The Keyless Network scales linearly on demand to handle surges in customer traffic. The Keyless Authenticator and SDK feature facial recognition biometrics as the primary modality. Other modalities are on the roadmap. Mobile push notifications are also supported.

The Keyless Authenticator is a standalone app designed for B2E use cases. The Authenticator can run on Android 7+, iOS 12+ operating systems, and Windows devices. The app is available on Apple and Google app stores. Support for MacOS and web is on the roadmap. Keyless facilitates Bring Your Own Device (BYOD) use cases in enterprise scenarios, allowing customers to support expanding remote access, Work From Home or Work From Anywhere initiatives. The Keyless Authenticator, when deployed for workforces and contractors, handles login requests, and enables SSO to enterprise applications via support for OAuth, OIDC, and SAML. In addition to supporting these standards, Keyless has integrations with Auth0, ForgeRock, IBM, Keycloak, Microsoft, Okta, OneLogin, and Ping Identity IAM and IdaaS solutions.

The Keyless SDK works on Android 7+, iOS 12+ operating systems, and Windows 10 devices (MacOS support is on the roadmap). Both the Keyless Authenticator and SDK support user registration, user authentication, device identification and authentication, and utilize their API to the Keyless Network. Each authentication event encompasses both user verification and device challenge/response authentication, allowing the originating device to serve as a second factor. Keyless Network nodes and Authenticator app/SDK instances use Zero-Knowledge Proofs for device identification and authentication. To deploy Keyless Biometric Authentication in consumer contexts, customers write their apps utilizing the Keyless SDK to manage authentication.

Users can register multiple devices and associate them with a single account. Doing so provides alternate account recovery mechanisms that don't need to involve customer support in cases where users lose or

upgrade devices. Registration of multiple devices is a self-service feature. Keyless uses proprietary facial recognition to identify, register, and subsequently authenticate users. Thus, front-facing cameras are required.

The Keyless Authenticator App and SDK can, through existing partnerships, do remote ID document verification. Users can take photos of ID documents which are then compared to selfies for remote identity verification. Keyless can read in addresses, DOBs, etc., via OCR. This capability is equally useful for remote employee onboarding and consumer use cases where Anti-Money Laundering (AML) and Know Your Customer (KYC) regulatory compliance is required. Recent updates to AML regulations (such as EU AMLD5) and ENISA's eIDAS Remote ID Proofing guidance, allow for remote ID document verification.

Keyless' facial recognition functions independently from the underlying operating systems. It does not rely on Apple FaceID or any Android facial recognition software. To prevent presentation attacks, Keyless has implemented liveness detection in passive and active forms. In passive mode, Keyless analyzes short videos of subject faces looking for subtle signs of movement. Keyless can detect and reject with high probability the use of videos in tests where would-be hackers attempt to play back a recording of a subject. In active mode, users are asked to perform a specific action, such as looking in a certain direction, blinking, etc. Using active liveness detection offers even stronger protection against played back videos. Keyless adapts to gradual changes in user appearance by updating the biometric templates after successful logins.

Biometric authentication systems typically take one of two approaches to storing templates (samples): local or centralized. Local storage of biometric templates has the advantages of enabling the user to authenticate when authentication servers are not available (device is offline) and reducing the attack surface on the server side. The disadvantage is that the biometric templates may be at risk if the user's device is compromised or lost. The advantage to server-side storage is that templates are not tied to specific user devices, increasing flexibility for users. However, the disadvantage is that if attackers fully compromise the servers, they may be able to decrypt users' biometric templates, rendering server-side encryption ineffective.

User biometrics are protected in a unique way in the Keyless system. After a biometric template (sample) is taken at registration time, the biometric data is encrypted and broken into shareable pieces. These shared secret fragments are sent by the Keyless SDK to the Keyless Network which are then distributed among the nodes according to the Keyless Protocol. Biometric templates on the user's device are deleted after registration. This protects individual users if their devices are lost or stolen. The Keyless Protocol is an implementation of Shamir's Secret Sharing framework, which creates more shared secret fragments than are necessary to execute the unlock operation (and in this case, match biometric templates for authentication). As long as a sufficient number of shared secret fragments are available on the Keyless Network, authentication event evaluations may proceed. The shared secret fragments are evaluated while still encrypted, using Secure Multi-Party Computation (SMPC) methods, and the nodes on the Keyless network never have direct access to the unencrypted biometric data. The multi-cloud horizontal scaling architecture of the Keyless Network guarantees 99.99% availability, which is less than an hour per year.

User data on the Keyless Network is therefore protected from disclosure, even in the event of a data breach, and provides the user with maximum privacy and control over their personal information.

Cryptographic keys are generated and managed by the Keyless solution. Derivative keys can be created to support digital signing and management of Decentralized Identities on customer devices. Additionally, Keyless can interoperate with keys generated by other IAM solutions.

These rigorous methods enable Keyless to support EU GDPR, PSD2 SCA, CCPA, the upcoming CPRA, and other privacy regulations by providing CIA (Confidentiality, Integrity, and Availability). Moreover, Keyless adheres to the principles of purpose limitation and data minimization for maximum GDPR compliance, in that no PII is stored in order to preserve the privacy of the user. The emphasis in product design with regard to security and privacy also deter phishing and fraud, especially Account Takeovers.

In addition to biometrics, Keyless incorporates risk-based authentication elements. Keyless assesses device health and detects whether devices are jailbroken. Keyless also calculates certain behavioral biometrics, which is the ability to analyze metrics of users' physical interactions with devices for comparison against registered samples. For mobile devices, the SDK allows for collection of information on screen pressure, swipe analysis, gyroscopic orientation, etc.

The EU Revised Payment Service Directive (PSD2) mandates that financial consumers must be authenticated strongly (Strong Customer Authentication, or SCA). This is defined as two of the following: 1) something you know, 2) something you have, or 3) something you are. Keyless Authenticator and/or SDK combine the something-you-have (phone) with something-you-are (biometrics), which meets the PSD2 SCA criteria. Risk-based authentication is a further requirement under the EU Revised Payment Service Directive (PSD2), in that, to obviate the need for per-session authentication, ongoing transactional risk analysis must be performed. The risk-based methods employed by the Keyless solution help customers meet those objectives of PSD2 as well.

Keyless Biometric Authentication achieved FIDO 2.0 certification for the Authenticator in July 2021. The FIDO Alliance maintains specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services. The FIDO protocol is also privacy enhancing, in that, new key pairs are generated for each Relying Party, meaning that data for one Relying Party is not visible to others.

Furthermore, Keyless is one of a relatively small number of vendors who have obtained FIDO Biometric Subcomponent certification. Prior to the FIDO Biometric certification program, key attributes about biometric authenticator devices had not been standardized for comparison. This made it difficult to assess security and usability between these devices and to validate vendor claims. The FIDO Biometric Component certification process uses independent labs to measure and publish False Acceptance Rates (FAR) and False Rejection Rates (FRR) of certified products. FAR is how often an illegitimate user could gain access to the device, whereas FRR is how often a legitimate user will be improperly prevented for gaining access to the device. The FIDO Biometric Component Certification process also sets standards for Presentation Attack Detection (PAD), sometimes called Liveness Detection as referenced above. During the testing for FIDO Biometric certification, Keyless attained an impressive 0.0% FAR (threshold = 0.01%) and FRR of 0.3265% (threshold = 3%). It also correctly identified and prevented 500 illegitimate attempts to gain access.

3 Strengths and Challenges

Keyless Biometric Authentication presents a compelling set of features in the authentication market segment of IAM. Keyless Authenticator supports B2E / workforce use cases with not only strong and user-friendly authentication methods, but also by enabling passwordless SSO to most common business applications by providing IAM connectors and supporting standards. The Authenticator App allows remote employee onboarding via selfie match and identity document verification. This has been particularly useful during the pandemic, as many companies have come to rely on such remote employee onboarding solutions.

Keyless is equally useful in consumer authentication scenarios, providing basic KYC and identity verification for newly registering users. Biometrics modalities are greatly preferred in the consumer side of the market over passwords, which are not even present within the Keyless solution. Keyless can reduce the costs of consumer IAM not only by eliminating password resets, but by allowing consumers to register multiple devices, account recovery processes and costs are minimized.

Keyless employs state of the art technology and cryptographic methods, such as Shamir Secret Sharing and Secure Multi-Party Computing to deliver secure and easy-to-use solutions for customers. The FIDO 2.0 and FIDO biometric subcomponent certification demonstrate their commitment to open authentication standards.

Keyless is likely to extend their platform to include support for SIEM integration as well as to external fraud and risk intelligence sources. The ability to import users in bulk in consumer scenarios could be enabled by supporting standards such as LDAP or SCIM.

Any organization that is looking to modularly upgrade authentication capabilities, utilize advanced cryptography for privacy, and go passwordless should look into Keyless Biometric Authentication in more detail.

KEYLESS

Strengths

- Fully passwordless authentication solution
- Biometric templates not stored on devices; Shamir Secret Sharing and encrypted Secure Multi-Party Computing
- Product architecture promotes privacy regulation compliance including EU GDPR and CCPA/CPRA
- Secure and user-friendly authentication service that serves both B2E and B2C
- FIDO 2.0 and Biometric Authenticator certification
- Remote ID document verification for employee onboarding and consumer KYC
- OAuth, OIDC, and SAML for SSO
- 99.99% uptime SLA; 0.3s per transaction processing time

Challenges

- No direct support for SIEMs
- No integrations with fraud/risk intelligence services
- LDAP and/or SCIM support would enable bulk provisioning
- Additional biometric modalities planned

4 Related Research

Leadership Compass Enterprise Authentication Solutions

Advisory Note Identity Authentication Standards

Leadership Brief How to Get Rid of Passwords - Today

Executive View FIDO 2

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.