KEYLESS

Zero-Knowledge Biometrics™

The Future of Authentication

The Status Quo

Biometric authentication is a type of security authentication that uses a person's unique physical characteristics such as their face or fingerprint to verify their identity. Biometric authentication solutions compare the biometric data captured from the individual with previously stored data to determine if there is a match.

The biometric authentication industry is currently dominated by two distinct approaches for storing and processing biometric data. Each approach impacts the privacy and usability of the resulting system, and affects how those systems are regulated in most jurisdictions.

Local Biometrics

Device-native, or 'local' biometric systems store and process biometric data on the user's device. The technology behind Apple Face ID, local biometrics ensure that a user's biometric template never leaves the device. The operating system (e.g., Apple iOS) does not rely on an external cloud provider (e.g., Amazon AWS). This gives local biometrics the advantage of privacy; an iPhone user knows that their biometric data will never leave their device. However, this comes at the cost of usability. If an iPhone is lost, any biometric template is lost with it and the user will need to re-enroll. It also does not support identity portability - an employee cannot enroll on an iPhone and then use their biometrics to log into a Samsung tablet.

Centralized Biometrics

Server-side, or 'centralized' biometric systems store and process biometric data on remote servers (also known as the cloud). When a user enrolls, their device will upload their biometric template to the cloud server. When a user authenticates, they generate a new biometric sample that is compared to the existing template on the cloud. The advantages of this authentication system is that it is much more usable and convenient for the user than local biometrics. If a user loses their device, they can retrieve their biometrics from the cloud. Centralized biometrics are also device-agnostic. An employee can enroll on one device and authenticate on any other device with a front-facing camera. However, server-side biometrics come at the cost of privacy. The entity that manages the cloud, such as Amazon, will have access to all of the user's data, which can include health status and personal traits. Although data at rest can be encrypted, data in use cannot be encrypted with traditional methods. What's more, a decryption key will always need to be stored on the system and any unencrypted biometrics taken during authentication will exist in memory. Put simply, local biometrics favor privacy and centralized biometrics favor usability and flexibility. Device-native biometric authentication systems protect data; server-side biometrics prioritize user experience. As of yet, neither system has been able to achieve both.

A New Approach

At Keyless, we have built a third type of biometric authentication system that combines the best of both worlds, which we call Zero-Knowledge BiometricsTM. ZKB is a new biometric category that offers the privacy of local biometrics with the usability and flexibility of centralized biometrics. An industry first, ZKB is the only biometric authentication system that does not store biometric data anywhere—not on the device or the cloud.

To describe how this is achieved, we must first clarify what does and does not constitute biometric data. In the context of facial recognition, biometric data includes the selfie itself, any biometric features extracted from the selfie, and anything that can link these features back to the user. On the other hand, any piece of data that cannot be linked back to the user is not biometric data.

The Zero-Knowledge Biometrics system adds the privacy offered by local biometrics to the usability and flexibility of centralized biometrics. Data leaves the device and is sent to the Keyless Cloud Service. However, unlike other centralized systems, this data is transformed before leaving the device in such a way that it no longer qualifies as biometric data, fully preserving the privacy of the biometric data within. The Keyless Cloud Service cannot read the transformed data nor extract any biometric information from it.

The Zero-Knowledge Biometrics system is made possible using the Secure Multi-Party Computation (SMPC) protocol, which transforms biometric data into encrypted data. SMPC allows multiple parties to perform computations on encrypted data without revealing the data to each other. Consider two millionaires who are interested in knowing who is richer without revealing their actual wealth. SMPC allows them to find this information out without revealing their answers. In Keyless' context, SMPC allows a user to send and retrieve their biometric data from the Keyless Cloud Service without revealing their data to anyone, including Keyless.

How it works

Let's look at a practical application of ZKB, involving a user (Jane), her device, her cryptographic key, and a cloud server (the Keyless Cloud Service). Jane's bank has just integrated Keyless. Before she can authenticate, Jane must first enroll with Keyless through her banking app, which takes between four and five seconds.

Enrollment

1. Jane logs in to her banking app and is prompted to enroll with Keyless.

2. Jane takes a selfie.

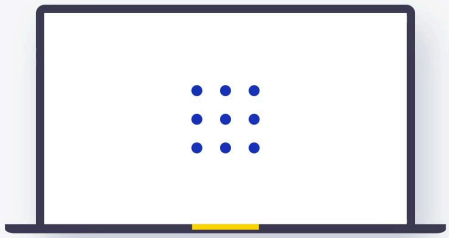
3. Jane's device checks the selfie using the Keyless antispoofing liveness detection engine, which runs locally on Jane's device.

4. Jane's device runs Keyless' proprietary machine learning pipeline to extract biometric features from the live selfie and transforms her biometric template using ZKB.

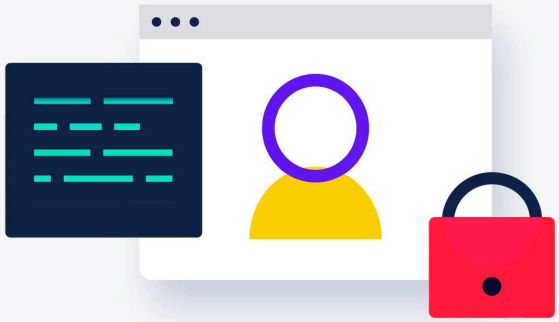
5. Jane's device creates a public and a private key.

6. Jane's device sends the transformed data and the public key to the Keyless Cloud Service.

7. The Keyless Cloud Service registers the transformed data and Jane's device, creating two distinct authentication factors, inherence and possession.



Steps 5-7 do not involve biometric data.



Steps 4-6 do not involve biometric data.

Authentication

1. Jane opens her banking app and positions her face in front of her device's camera.

2. Jane's device runs Keyless' anti-spoofing liveness detection engine.

3. Keyless' proprietary machine learning pipeline extracts biometric features from the live selfie.

4. Jane's device transforms the biometric data using ZKB and sends it to the Keyless Cloud Service to confirm that Jane's selfie matches the one taken during enrollment. As with enrollment, Keyless is not able to see or access Jane's biometrics.

5. The Keyless Cloud Service confirms both selfies match (inherence) and that Jane's device is the same as the one registered (possession).

6. Jane accesses her bank.

A New Future

Thanks to the zero-knowledge biometric system, businesses no longer have to choose between device-bound and server-side biometrics. Organizations can now offer their customers and employees the usability and flexibility of centralized biometrics without putting their biometric data at risk.