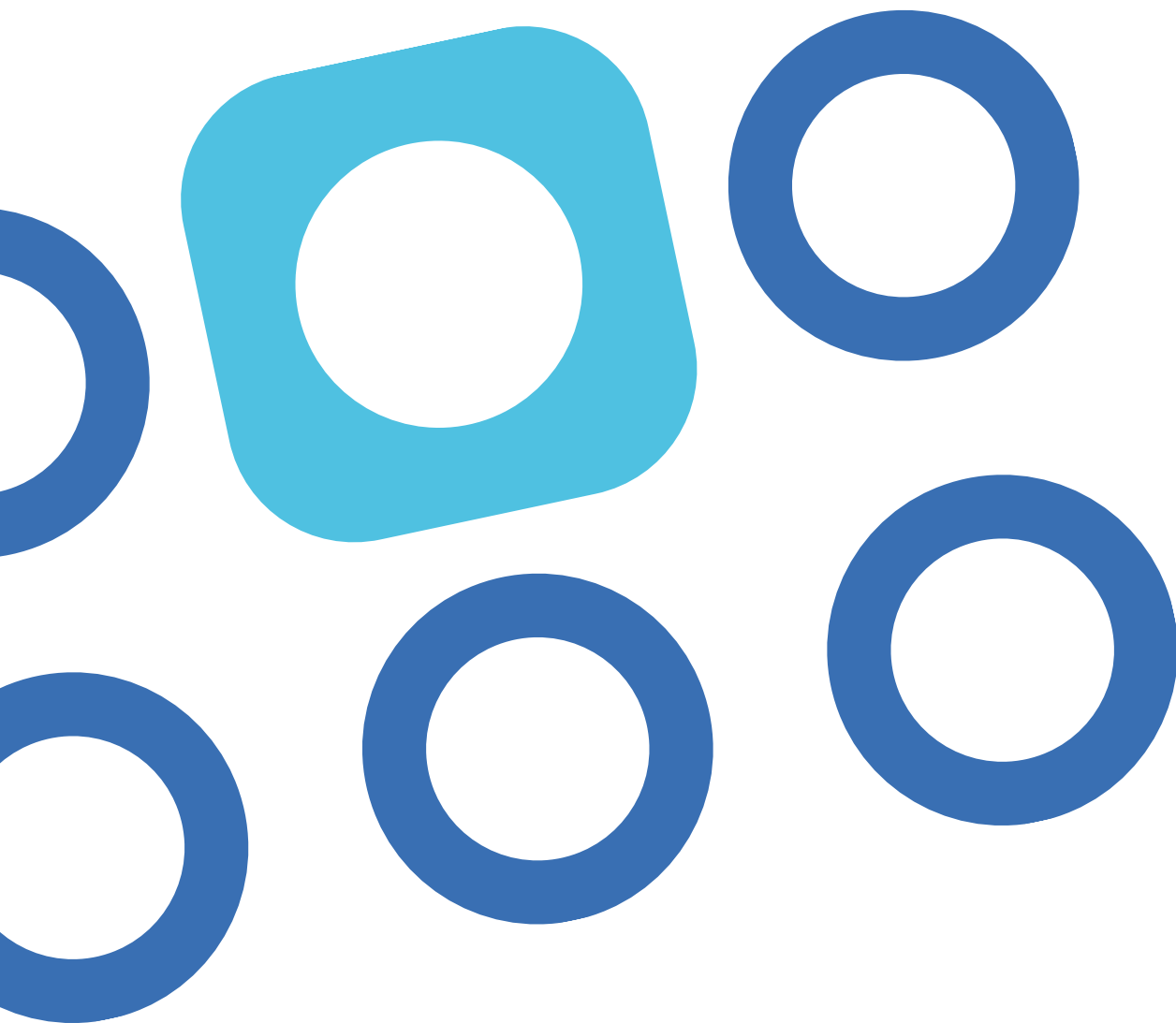




USE CASES

See how Polygon's **Biometrid** can be used in different usage settings





USE CASE

Web/Mobile Authentication

Digital user authentication using biometrics

Password management is increasingly harder for the user. We all tend to forget our passwords with each site requiring their own security rules. Statistically, we forget more than 70% of our passwords and even worse, it's a type of authentication highly subject to phishing attacks and high levels of fraud.

Our solution combines awareness and physical properties such as voice, fingerprint and facial features to enable verification of user's identities, allowing security and performance depending on the context of our client needs.

We are also able to estimate a user age, gender and emotions whilst guaranteeing his/her full anonymization.

Benefits

Business:

- Guarantee that the digital relation with a customer is being done with a specific living customer on real time;
- Increase the business confidence on decision making;
- Reduces frauds;
- Prevents phishing attacks;
- The increased security is perceived by the customer;
- Very high levels of accuracy. Statistically superior to human operating solutions;
- Privacy guaranteed.

Technological:

- Secure Cloud Infrastructure: Scalable and flexible, logical and physical separation;
- Quick Startup: API Integration to service, integration with no biometric data;
- Flexible Design: Open to new modalities and adaptive to the use case specific needs;
- Out of the box biometric engines: Keep a wide range of a biometric engines to offer the best solution for each scenario.

Markets

- Banking
- Insurance
- Retail
- Healthcare
- Utilities
- Government
- Service providers

Onboarding

Remote contracting of products or services for new or existing customers

We facilitate the process of creating and validating a digital identity of a new (or existing) customer, allowing for remote user identification.

By using a camera from a smartphone or computer, the customer only needs his European Union National ID card (or passport) and a selfie to “open an account”.

From this point onwards, the customer will be able to authenticate and verify his identity using the enrolled biometric data (face and/or voice).

This technology include document validation and OCR, face matching and liveness detection, document uploading, video conferencing and OTP for explicit consent.

Benefits

- Decrease fraud levels (KYC);
- Biometrics data secure collection for future use in authentication;
- Low validation time and costs with our Backoffice;
- Positive and pleasant customer journey;
- Convenience for both parts.

Markets

- Banking & Fintechs
- Insurance
- Retail
- Healthcare
- Utilities
- Government
- Service providers

Call Centre

Customer strong authentication in call centres

Using voice recognition biometrics, the IVR (or operator) will prompt the customer for a password. The customer answers and his/her voice are recognised by the IVR that welcomes using his/her name.

Benefits

For the contact centre:

- Allows administrative attending time of 0 (zero) seconds;
- The operator is more motivated (lower routine tasks);
- Immediate access to client's info whilst he is being called by the name through the IVR;
- Contact time between client and operator is more productive;
- Client positive referrals;
- Higher potential for First Contact-resolution
- Higher security levels. Absolute certainty of caller ID;

For the customer:

- Immediate and personalised treatment (after authentication);
- Better call experience;
- Lower answering wait time perceived (after hearing his/her name he is more loyal to the caller);
- Gets immediate attention to his/her problem and with a higher potential for resolution;
- Innovation and ease of use;
- The Voice is non-transferable and unforgettable. Confidence that only he/she uses is close to absolute.

Markets

- Call centres