![Oz Forensics logo]

![AIROME logo]

PayConfirm & Oz Forensics

INTEGRATED SOLUTION FOR THE PROTECTION OF REMOTE BANKING USERS

Convenient and safe authentication and signature for financial transactions from your smartphone

Biometric identification and protection against digital fraud

Additional biometric authentication factor for mobile banking users

ozforensics.com/en

safe-tech.ru/en

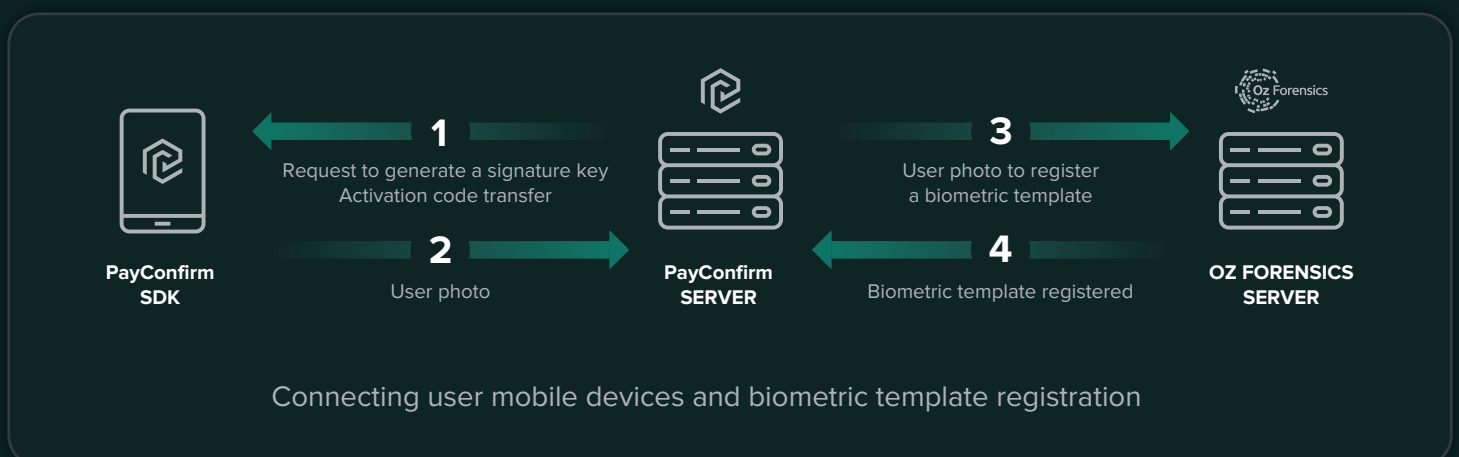# Mobile e-signature and additional biometric authentication factor

Biometric technologies and e-signatures on users'mobile devices to provide convenient and safe operations via digital channels.

A fully integrated solution developed by Oz Forensics and SafeTech protects remote banking clients when they perform critical actions or large transactions.
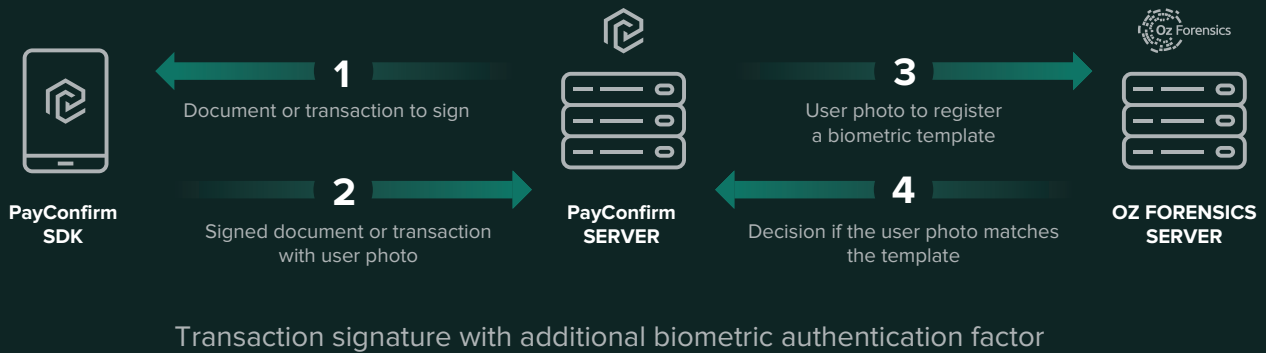
The solution is based on the OzForensics platform for biometric identification and protection against digital fraud and the PayConfirm software package for mobile authentication and e-signature. The integrated PayConfirm and OzForensics solution effectively defend attempted fraud in remote banking systems, without relying on how well resistance bank clients may be themselves and what mobile devices they use.

Frameworks and Operation of the Integrated PayConfirm and Oz Forensics Solution

The mobile part of PayConfirm is integrated into the mobile banking application on remote banking clients'devices. The server part of he solution includes the PayConfirm and OzForensics server. The latter stores user biometric templates and decides whether a user photo provided to the system matches the user's registered template.

PayConfirm SDK

1 Request to generate a signature key Activation code transfer

2 User photo

PayConfirm SERVER

3 User photo to register a biometric template

4 Biometric template registered

OZ FORENSICS SERVER

Connecting user mobile devices and biometric template registration

When a user mobile device connects to the server, the PayConfirm mobile client receives an e-signature key(or a request to generate a unique signature key) while receiving an activation code (e.g. reading a QR code) through a second interaction channel. After the key is received and activated (generated), the system prompts the user to provide a photo (take a selfie), passes it to the Oz Forensics server, and registers it there as the user biometric template. As a result, an exact match between a given user, their unique signature key,and their authentication biometric template is created.

1 Document or transaction to sign

PayConfirm SDK

2 Signed document or transaction with user photo

PayConfirm SERVER

3 User photo to register a biometric template

4 Decision if the user photo matches the template

OZ FORENSICS SERVER

Transaction signature with additional biometric authentication factor

While a given financial transaction is being created and signed, the server part of PayConfirm receives the transaction data from the remote banking system and provides the user with the details to generate the signature on their mobile device. If an additional biometric authentication factor is required (e.g., when a critical action is being undertaken, such as keys being updated or connecting new mobile devices to the system, as well as in the event of large transactions), a user is asked to take and provide a selfie (in the form of a photo and/or a video). The user biometric data, together with the signed translations or document, is sent to the PayConfirm server, and then to the OzForensics server, which compares this information to the registered biometric authentication template.

Based on the results of the analysis, the Oz Forensics server makes a decision as to whether the provided data matches the user biometric template. This information, together with the signed transaction, is returned to the remote banking server, so that a decision can be made as to whether the transaction should be completed or whether an immediate response should be made to the incident.

The Advantages of the Integrated PayConfirm and Oz Forensics Solution

Based on the results of the analysis, the Oz Forensics server makes a decision as to whether the provided data matches the user biometric template. This information, together with the signed transaction, is returned to the remote banking server, so that a decision can be made as to whether the transaction should be completed or whether an immediate response should be made to the incident.

> The solution creates a synergetic for banks: with the integrated solution, they can provide their users with an additional biometric authentication factor when they perform critical actions (such as updating keys or connecting a smartphone to the system) or large transactions.

> Configurable adaptive authentication (automatic background sign in, request and complete additional authentication, block a signature and the completion of the transaction) based on the level of importance of user actions and the a mount of the transaction to be completed.

> Ease of implementation: banks get a ready-made tool for user biometric authentication for their remote banking system.

> Reduced costs: significant savings on system implementation, integration, operation, and technical support.

OzForensics

A SOFTWARE PLATFORM TO AUTHENTICATE DIGITAL DOCUMENTS AND PHOTOS, PROVIDE BIOMETRIC IDENTIFICATION AND PROTECT AGAINST DIGITAL FRAUD

The basic OzForensics modules perform a multifaceted analysis of scanned or photographed documents (passports, IDs, driving licenses, certificates etc.), use facial biometrics algorithms to analyze images received from photos and video channels containing images from documents or the existing databases, and can extract text from digital passport copies and confirm passport copy authenticity.

> Fewer defaults on loans for banks and micro-finance organizations

> Lower risk of fraud when authenticating clients remotely

> Reduced company costs

> Automated remote authentication

PayConfirm

MOBILE AUTHENTICATION AND E-SIGNATURE PLATFORM

PayConfirm is a software platform that performs digital signature in a smartphone to sign any types of operations, including transaction confirmation or e-documents right in a mobile device. Quick and user-friendly e-signature on mobile devices. Comparing to such methods of transaction confirmation as SMS, One-Time Password, scratch-cards, MAC-tokens and others, PayConfirm makes the procedure more secure, user-friendly and cost-effective for a bank.

> User-friendly — no more passwords retyping from SMS

> Secure — trusted service based on cryptography

> Cost-effective — reasonable economy on SMS and OTP

> Easy-to-integrate – no more hardware-based solutions, available iOS and Android devices

Learn more about PayConfirm:
https://airome.tech/payconfirm

About Oz Forensics:
ozforensics.com/en
order@ozforensics.com

About Airome:
www.airome.tech
info@airome.tech