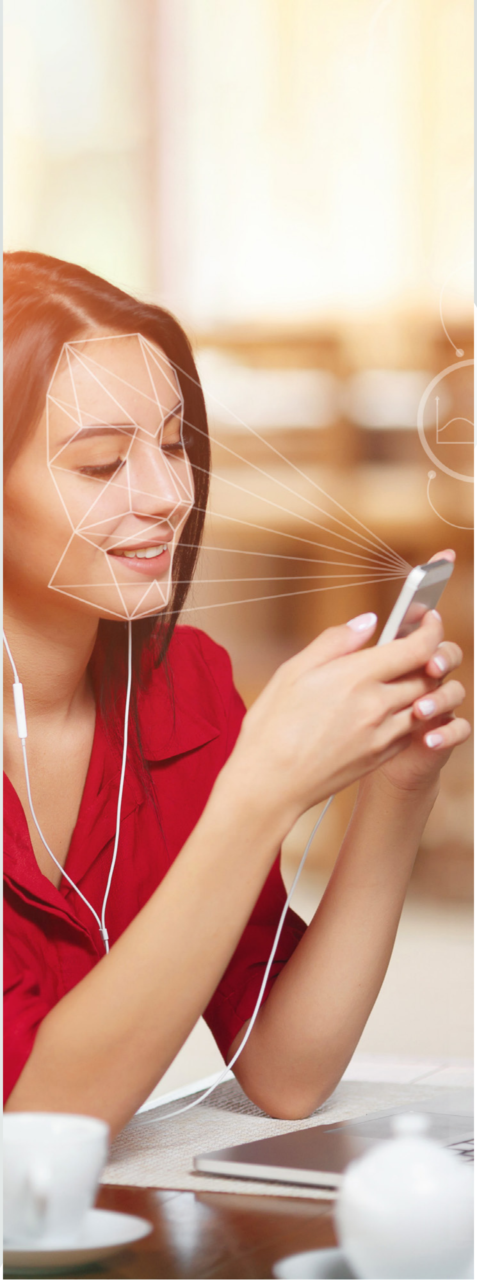
AIROME

BIOMETRIC AUTHENTICATION

Protecting the most vulnerable spots in digital channels



These days, cyber attackers constantly improve the tech they use to steal money from digital banking channels users' accounts: technical attacks, social engineering, or a mix of both come into play. These lead to financial losses for banks and their customers, or, at the very least, a much more complicated customer journey.

Unless you want to deal with frustrating calls from anti-fraud specialists or invite the client into the office for every minor change, the most innovative way to strengthen digital banking channel customer security is biometrics.

Remote banking services (RBS) security concerns:

- Insufficient RBS security level when users connect and update their signing keys.
- High level of banking fraud activity, including malware and social engineering.
- Outdated and insecure transaction authorization and document-signing technologies that use SMS and push notifications.

BUSINESS OBJECTIVES

Building digital channels that provide customers with both a convenient user experience and peace of mind that their funds are safe is no small feat. Fraudsters tend to attack the weakest spots in security systems, usually end users themselves. This means that secret codes or passwords sent via SMS or push notifications aren't effective — attackers can easily learn them by pretending to be security officers.

In terms of security, the most sensitive case is when a customer switches to a new mobile device or tries to recover access to their personal account. Without physical contact with the user, it's hard for security to identify who exactly is performing a transaction. Is it the real customer or a fraudster who managed to obtain all the necessary information and gained unauthorized access?

The PayConfirm platform with the biometric identification module lets you use an additional biometric authentication factor when customers undertake critical actions, such as updating their keys or connecting a new mobile device, or when they perform perform large transactions.

RESULTS

The advantages of a comprehensive solution:

- Lowering the volume of thefts from customer accounts several times over;
- A simplified user experience when it comes to restoring access or performing an atypical transaction;
- Significantly reduced load on the bank's anti-fraud and call center specialists;
- Enhances customer user experience;
- Reduced costs on telecom services due to SMS codes.

GET IN TOUCH WITH US

airome.tech
info@airome.tech

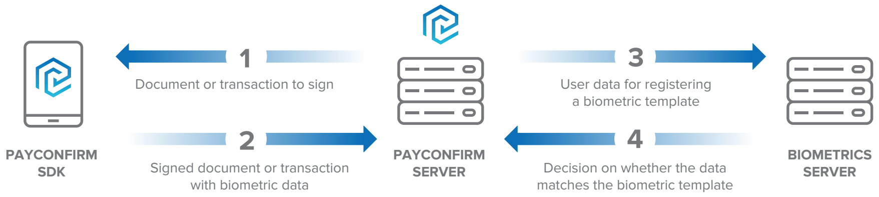
To eliminate weak spots in the security system, you first need to stop relying on one-time passwords transmitted to the customer via insecure channels. After that, you should add at least one more authentication factor for critical transactions.

One of the key requirements for a system that can solve this problem is ensuring the authorship and integrity of signed documents. Another is providing an additional biometric authentication factor.

SOLUTION DESCRIPTION

PayConfirm, a software platform that performs mobile transaction authentication signature (mTAS), is the solution that meets these requirements the best, by including a biometric identification and digital fraud protection module.

It uses mobile digital signature technology, which lets you confirm any transaction over a digital channel with a single screen tap, all the while ensuring its authorship and integrity. This mode of operation doesn't force you to send one-time passwords to customers, meaning they won't be intercepted or compromised. Integrating with the biometric identification platform provides additional security for the most vulnerable cases, such as restoring access on a new device.


PAYCONFIRM SDK
1
Document or transaction to sign
2
Signed document or transaction with biometric data
PAYCONFIRM SERVER
3
User data for registering a biometric template
4
Decision on whether the data matches the biometric template
BIOMETRICS SERVER

SOLUTION WORKFLOW

When a user connects to the system, they take a picture of their face (a selfie). This biometric template is then stored in a database on the bank's side. When trying to restore access on a new device, the user is asked to take a selfie along with the data they're usually required to provide (card number, SMS code, etc.). This selfie is then compared to the registered biometric template in order to verify liveness. If the photo matches the template, access will be restored, otherwise it won't be.

The same framework can be used to authorize high-risk transactions detected by an anti-fraud system (e.g., large amounts, to unknown accounts, from new geolocations, etc.).

Airome Technologies is willing to share its success stories, and consult banks on technical and business aspects.