KEY POINTS

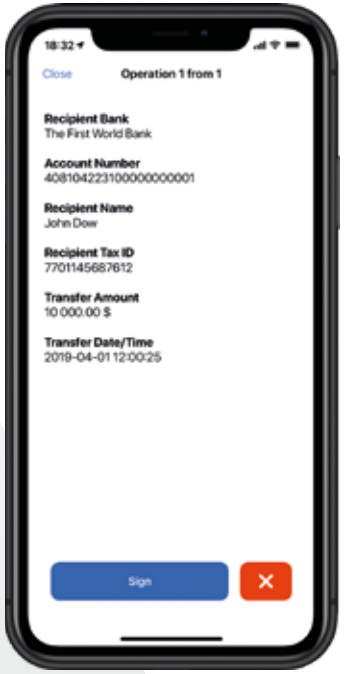
Confirm any types of operations on-the-go with PayConfirm:

— No more codes retyping from SMS, PUSH notifications and OTP generators;

— Trusted solution based on cryptography;

— No deny of service in roaming and off-line modes;

— Real-time notification right in a smartphone.



High level of security:

— Protection from phishing, social engineering, data switching;

— SMS interception and SIM swap attack protection.

General principles of PayConfirm are premised on security best practices and customer experience in digital banking and e-document confirmation systems development.

Our technology is already successfully adopted and used by more than 60 banks worldwide.

ABOUT US

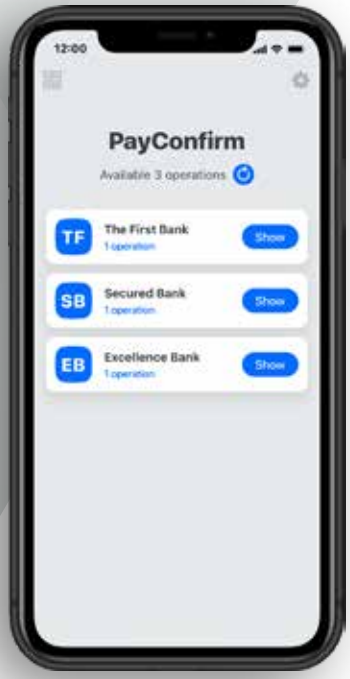
Airome Technologies is a Singapore-based developer of cybersecurity solutions for digital banking and e-document management systems. The company provides a secure client-server software to confirm or digitally sign any type of operations, including bank transactions or e-documents, on a mobile device. Our solution lowers the risk of unauthorized transactions caused by man-in-the-middle, phishing, or social engineering attacks.

Our mission is to enable our customers to provide user-friendly, secure and cost-effective digital banking services.

GET IN TOUCH WITH US

airome.tech
info@airome.tech

PayConfirm



MOBILE TRANSACTION AUTHENTICATION SIGNATURE (mTAS)

AIROME

GENERAL OVERVIEW

PayConfirm is a software platform that performs mobile transaction authentication signature (mTAS) to authenticate or confirm any type of operations, including transactions or e-documents, on a mobile device. Comparing to such methods of transaction confirmation as SMS, One-Time Password, scratch-cards, MAC-tokens and others, PayConfirm makes the process more secure and user-friendly.

PayConfirm consists of two parts:

- Server part that is implemented into bank's IT infrastructure;
- Mobile client or application for smartphones based on iOS (8.0 and above) and Android (4.0 and above).

mTAS PayConfirm can be easily embedded into the banking mobile application or work as a customized stand-alone app.

In the core of a signature, generated by PayConfirm, there are asymmetric cryptographic algorithms, which means that a bank itself doesn't store clients' key, while digital keys — so-called "private keys" — are generated and stored in client's smartphone and cannot be "intercepted" as well as reproduced by any third party.

AREA OF USE

PayConfirm can be applicable for a variety of digital services provided by bank or government but generally the solution is used in the following areas:

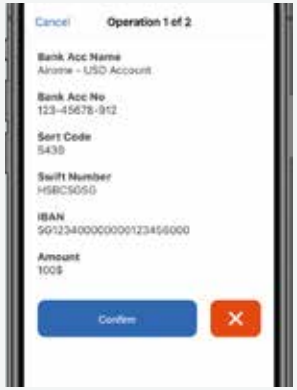
- Internet/Mobile Banking;
- E-commerce;
- E-document management.

Unlike OTP, mTAS is bound to the payment details and user's smartphone. This solution protects from the most common security threats in digital banking such as SIM swap fraud, social engineering, phishing, bank account details replacement and many others.

PayConfirm can be integrated directly into the mobile banking app and perform not only secure but also user-friendly interaction. There is no more need to go to a branch-office and sign manually any paper documents.

TRANSACTION CONFIRMATION

Follow the push notification



Get the operation's details

Confirm using password or biometry

Done!

AIROME

SECURITY

- **PayConfirm features to secure transactions:**
  - In PayConfirm transaction authentication signature is generated on the basis of four components: exact transaction details and timestamp, smartphone fingerprint (unique smartphone characteristics) and a private key stored in client's smartphone;
  - Fraud monitoring systems integration significantly increases accuracy of any potentially fraudulent transactions detection;
  - Unlike OTP, in mTAS PayConfirm full transaction details or agreement data are displayed to the client before confirmation as well as confirmation result;
  - No OTP or any other codes are use in mTAS PayConfrim and this reasonably decreases the risk of fraud caused social engineering.
- **Private key's security:**
  - The private key is generated in the user's smartphone and stored encrypted in safe;
  - Two independent communication channels are used to activate PayConfirm app in a user's smartphone.
- **Transactions non-repudiation:**
  - User not just "confirms" payment details, but authenticates the transaction, so as a result it is easy to answer when and what exact data was confirmed, who did it and what was a result of the confirmation process.

USER EXPERIENCE

- Confirmation of any operation just in one tap;
- No OTP or codes input;
- No transaction delays or cancellations connected with PUSH notification and SMS delivery time;
- Fully software-based — no additional hardware required: no hardware token, OTP generator, scratch-cards, etc.;
- No dependency on mobile service — stable work in roaming or out of mobile operators' coverage.