EASY WAY TO REDUCE 75% OF DIGITAL BANKING FRAUD IN 3 MONTHS

When financial services went digital, a digital bank client became the most vulnerable point of banking experience. While the bank system itself is well-protected, bank's clients are permanently under attacks by fraudsters.

Major attacks that almost all the banks face are man-in-the-middle on mobile banking app, phishing, social engineering, OTP hijacking. The aim of all of these attacks is to get access to the bank account and operate the finance.

HAVE YOU EVER THOUGHT THAT IMPLEMENTING PROPER AUTHENTICATION SOLUTION, YOU CAN COVER 75% OF FRAUD IN YOUR DIGITAL BANKING CHANNELS?

Here is step-by-step description how we achieved it with PayConfrim implemented in 70 banks.

WHAT SORT OF AUTHENTICATION SOLUTION YOU NEED?

To reduce most of the security risks in digital banking channels, there are several points that should be taken into consideration. Authentication solution should perform encryption of all the operation – that's why many OTP-based authentication solutions simply do not fit into this criterion.

The one that performs non-repudiation and integrity control of every operation. From this perspective, so-called WYSIWYS (what you see is what you sign) approach is strongly recommended – otherwise, how bank's client can be sure what s/he is actually confirming.

Definitely, such a solution should be easy to implement and maintain and also it should be super-easy for the bank's clients. Unified omni-channel authentication experience for the clients also one of the critical point as for the clients, as well for the bank – it is simpler for both parties to use one and the same solution for all the channels while for the bank it is also cost-effective.

BRIEF SOLUTION INTRO

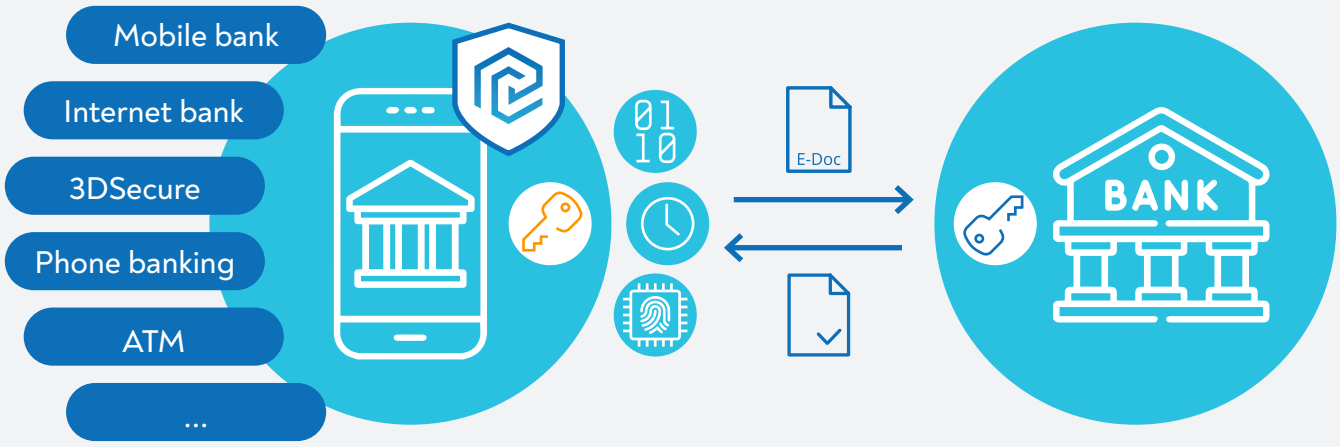
PayConfirm is a fully software authentication solution based on asymmetric cryptography. It can be used for log-in, money transfer or any type of secure confirmation in any digital banking channels: internet bank or simple web-based cash-management system, mobile bank, online card payments operations, phone call requests or even ATM.

Techwise, there is a key pair – private key and public – split between the server installed on the bank's side and mobile banking app installed in client's device. Private key is stored in a double encrypted way on a smartphone and used every time when client is trying to confirm a transaction. The private key can work on the exact client's device only, cannot be extracted. It isprotected with the secret known by the user only – it can be static password, touch ID/face ID.

Every confirmation is generated just with one tap on the smartphone screen while technically it is cryptographically calculated authentication "signature" based on exact transaction details and timestamp, exact device finger-print and private key value. All this information is sent to the server side in an encrypted way where it is verified with public key.

Device finger-print helps to perform the linkage with the exact device – so bank security team always can easily identify any attempt of money transfer confirmation from a different device. As well, with this opportunity up to 70 security parameters about the device will become available as a raw date that can be provided to anti-fraud installed inside the bank. Any potentially suspicious activity, malware installed on the device and etc. will be easily identified with device-fingerprint feature. And also it will be easy to identify attempts to log-in into the user's account from a different device and react accordingly.

Being based on more than 10 years of international experience, it combines user-experience and strong security features and helps to protect from a number of the most popular attacks like man-in-the middle, OTP hijacking, SIM swap, social engineering, phishing.



HOW CAN PAYCONFIRM HELP WITH PHISHING ATTACKS PROTECTION

Phishing is a type of attack when bank clients receive SMS or email aimed to forward clients to any kind of a fake page. The purpose is usually to get money, get client's details and then take over the account or sometimes – to install in a hidden way any kind of malware to hijack OTP codes of the bank or perform any acts to get access to client's bank account.

While PayConfirm performs integrity control check and WYSIWYS (what you see is what you sign) principles, in case of attempts to transfer money, provide credentials, change account phone number, this will be easily detected on the confirmation step – bank client simply will see the real operation s/he is willing to confirm.

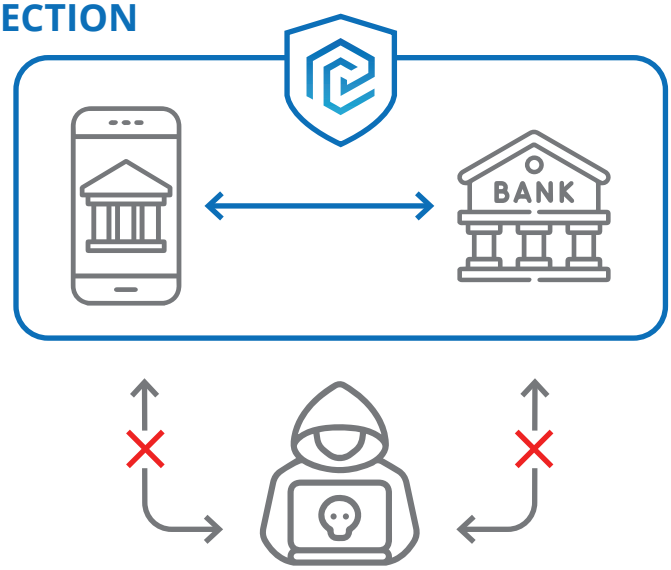
At the same time, device fingerprinting will help bank security team to identify any malware installed on the client's device.

HOW CAN PAYCONFIRM HELP WITH MAN-IN-THE-MIDDLE ATTACKS PROTECTION

MIMT has been around or a few years so far and already can be easily defeated on tablets and laptops. But moving to mobile-centric services, the problem of interception and replacement of data in communication channel between the banking app and bank system has become crucial for many banks.

It does not matter how exactly attacker could interfere into the communication channel – through vulnerabilities on the bank or client side – in most cases responsibility will be on the bank's side.

While simple authentication solutions based on OTP are not able to help with MIMT because of the technological approach in core, with PayConfirm it is completely different. It is based on asymmetric cryptography. It means that there is a key pair split between the app with private key and server with a public key. Thus, all the data is transferred from a



smartphone to the sever in the encrypted way, so it can be decrypted only on the server side using public key.

HOW CAN PAYCONFIRM HELP WITH SOCIAL ENGINEERING ATTACKS PROTECTION

By social engineering in this case we mean all the calls bank clients receive from scammers introducing themselves as bank security team, bank client relation team, any online shop with special promo. The aim of these attackers is to get the OTP-code to transfer money, change account passwords or simply buy something expensive or even gift vouchers that can be easily exchanged for money after.

The secret of PayConfirm is that there is no OTP or any other code sent to the client. Can you imagine scammers calling bank clients and getting nothing because technically there is no OTP that can be shared with anyone?

Moreover, in case of attempt to change account passwords by any scammer, this also will be received by the client as an authentication request with real operation details: someone is trying to change your account log-in details – would you confirm that it is really you?

HOW CAN PAYCONFIRM HELP WITH SIM SWAP ATTACKS PROTECTION

SIM swap is a way of attack on bank clients aiming to make a clone of a SIM card to take a control over the user's account. But If bank uses an authentication solution operating independently from mobile operator traffic, SMS channel, the risk of this attack will be minimized. This is the way it works with PayConfirm. Moreover, with PayConfirm onboard transactions can be confirmed from the exact device only, because device finger-print (unique device characteristics) are one of the necessary component used during the transaction confirmation.

HOW CAN PAYCONFIRM HELP WITH INTERNAL BANK FRAUD PROTECTION

While in PayConfirm private key is used as one of the key component of transaction confirmation and it is stored on the client side, none of bank employees can get access to it or use for non-sanctioned transaction confirmation. On the bank side there are only public keys stored. Each public key is unique and can be matched only with the exact private key from the key pair.

With such an approach it has become easy to border the responsibility between the bank and the user as each party is responsible only for the key stored on their side.

Meanwhile, every transaction can be confirmed only from the user's side using the secret known or kept by user only (password, touch ID/face ID)

HOW CAN PAYCOFNRIM HELP WITH ATM FRAUD PROTECTION

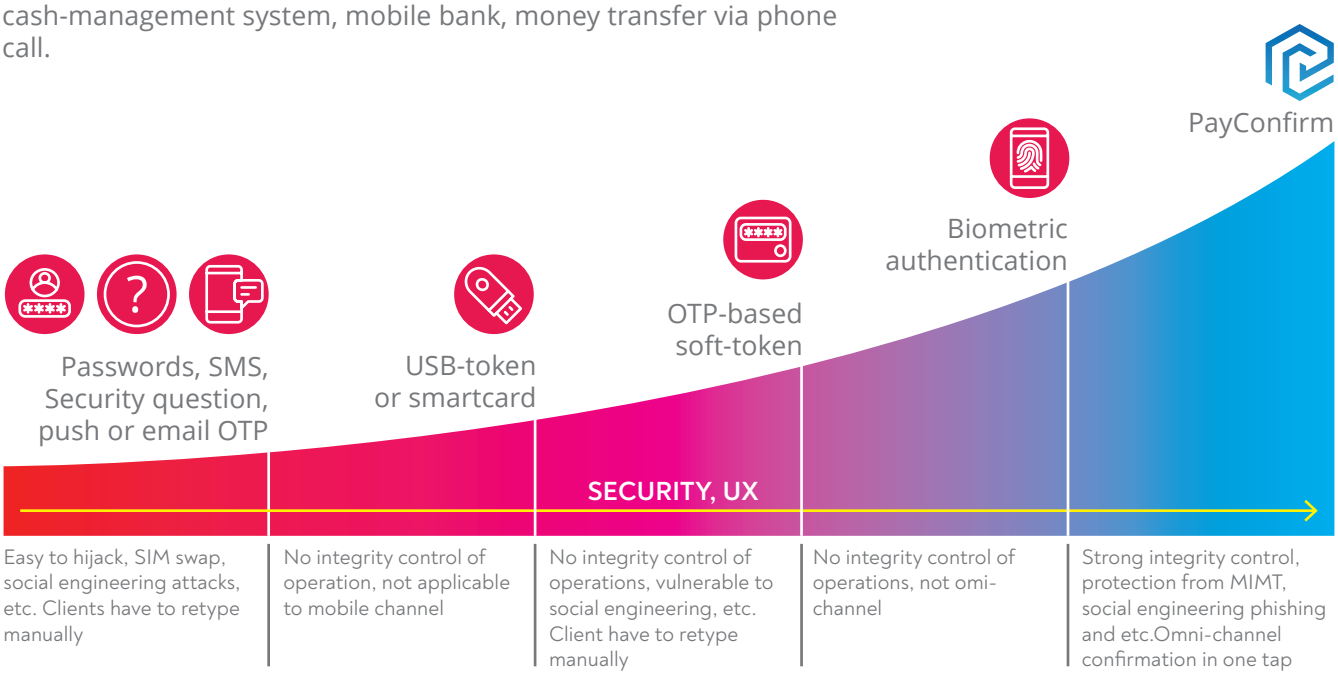
One of the most popular way of ATM fraud is skimming which is really popular around touristic area. This type of attack means an attempt to get card details and PIN or swipe data from magnetic stripe or card's chip. This is the reason why many banks are moving to mobile payments options via virtual cards and NFC-based ATM machines to provide their client cardless ATM. In this case they often face high price for hardware upgrade of their ATM machines on one hand, and on another hand – not all the users have NFC reader onboard their smartphone.

With one of the add-on feature of PayConfirm – QR log-in – it is possible to interact with ATM without any plastic card. For log-in client uses a banking app QR-scanning feature, scans the dynamic QR on the screen of ATM and confirms log-in operation from the smartphone with the same level of security as in general cases of using PayConfirm. Further interaction with ATM – money withdrawals – will be confirmed directly via a banking app on a smartphone.

In this case the risk of card-fraud via ATM channel is minimized but at the same time there will be no need to upgrade hardware of ATM machine. In addition, bank clients get the same user-experience as in other cases.

SUMMARY

PayConfirm can cover the most popular cases of digital banking fraud. Being implemented in 70 banks globally, it has never been hacked yet. The good point about PayConfirm is that it can be used a universal authentication solution for all the digital channels: internet bank, cash-management system, mobile bank, money transfer via phone call.



ABOUT US

Airome Technologies is a Singapore-based developer of cybersecurity solutions for digital banking and e-document management systems. The company provides 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 unauthorised 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 services.

Recognized by Gartner

GET IN TOUCH WITH US

airome.tech
info@airome.tech