Security Essentials for FinTech Apps

5 features to make your product sustainable to fraud and hacker attacks.

velmie

INTRODUCTION

Mobile penetration changed the way we do things and build new products, and finance management is not an exception. In Europe alone, fintech app usage is up 72% since the beginning of pandemic in 2020. Neobanks like Monzo and Revolut are quickly expanding their user base, Coinbase becomes a public company, Robinhood opens the doors for retail investors and Lemonade is knocking at the door of insurance. Furthermore, the Global Fintech Market is projected to grow by a CAGR of 23.58% by 2025.

Being such a promising and still undisrupted industry, FinTech attracts hundreds of entrepreneurs who rush to deliver an MVP to the market to see if "they catch". To get to the pace, companies on this stage often cut all sorts of corners including security and compliance concerns. Once the product is released, the company starts getting even more pressure from user requests and feedback. Obviously, no one asks to improve the back office by implementing an extra layer of security. The teams are facing product roadmap dilemmas, on one side there are clients and on the other one there are security features that will take months to build and none of the clients will ever notice this enhancement. This way, security and compliance concerns remain either underestimated or ignored.

The study by ImmuniWeb reveals that, despite being well-funded, 98% of the world's top 100 fintech startups are vulnerable to web and mobile application attacks. 100% of them have security, privacy, and compliance issues relating to applications and application programming interfaces (APIs). All of the fintech mobile apps tested in the research contained at least one security vulnerability of medium risk, while 97% have at least two medium or high-risk vulnerabilities.

INTRODUCTION

Based on our experience of building financial and banking products, we can state that there are corners FinTech companies should never cut. The past shows that core security features and software compliance should be an integral part of any MVP coming to the market. Therefore, you either put it in the MVP backlog from the very beginning or use a prebuilt software that already comes with the core security components.

In this playbook, we summed-up the security and compliance essentials for FinTech startups to consider and implement them on an architecture level while building their products.

Sincerely,
Velmie Team

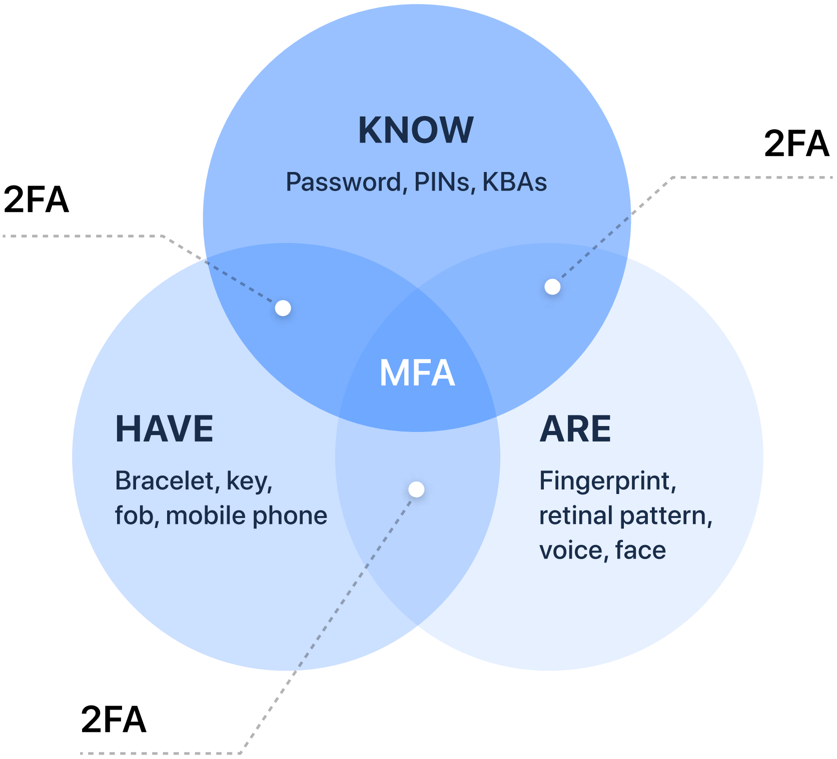
CONTENTS

1 | STRONG CUSTOMER AUTHENTICATION

Strong Customer Authentication (SCA) is the requirement of most of the regulations and policies and must be a default approach to customer authentication. Nowadays, mobile devices provide plenty of opportunities to build strong and secure authentication mechanisms. It can be implemented as a 2-factor authentication (2FA) or multi-factor authentication (MFA). 2FA or MFA means an app is using any 2 or 2-3 factors to identify the user's identity respectively:

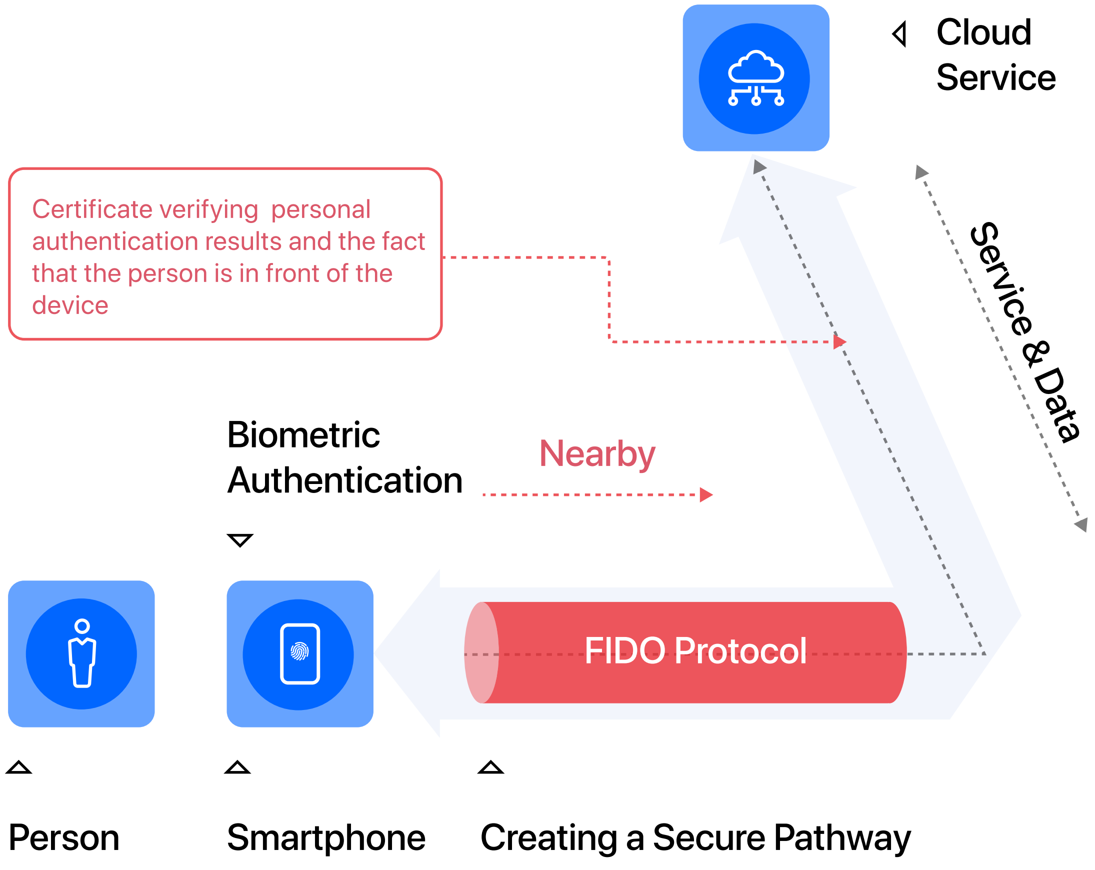
- Something a user knows (such as a password);
- Something a user has (such as a cell phone or other piece of hardware);
- Something a user is (such as fingerprint, retina, or facial features).

For example, in addition to a password that user "knows" 2FA can use a cell phone or other device user "has" or ask him to present a biometric, such as a fingerprint.



1 | STRONG CUSTOMER AUTHENTICATION

The FIDO Alliance, a non-profit organization that seeks to standardize authentication at the client and protocol layers, is defining a standardized architecture by which a user's local authentication to the device (e.g., laptop, phone) can be communicated to a server. When that local authentication is biometric (e.g., a scan of the user's fingerprint by a phone sensor or a facial scan), then the FIDO model's advantage is that the biometric template doesn't have to be stored on the server, with attendant privacy risk.


Cloud Service
Certificate verifying personal authentication results and the fact that the person is in front of the device
Service & Data
Biometric Authentication
Nearby
FIDO Protocol
Person
Smartphone
Creating a Secure Pathway

1 | STRONG CUSTOMER AUTHENTICATION

1.1. Transactions Confirmation

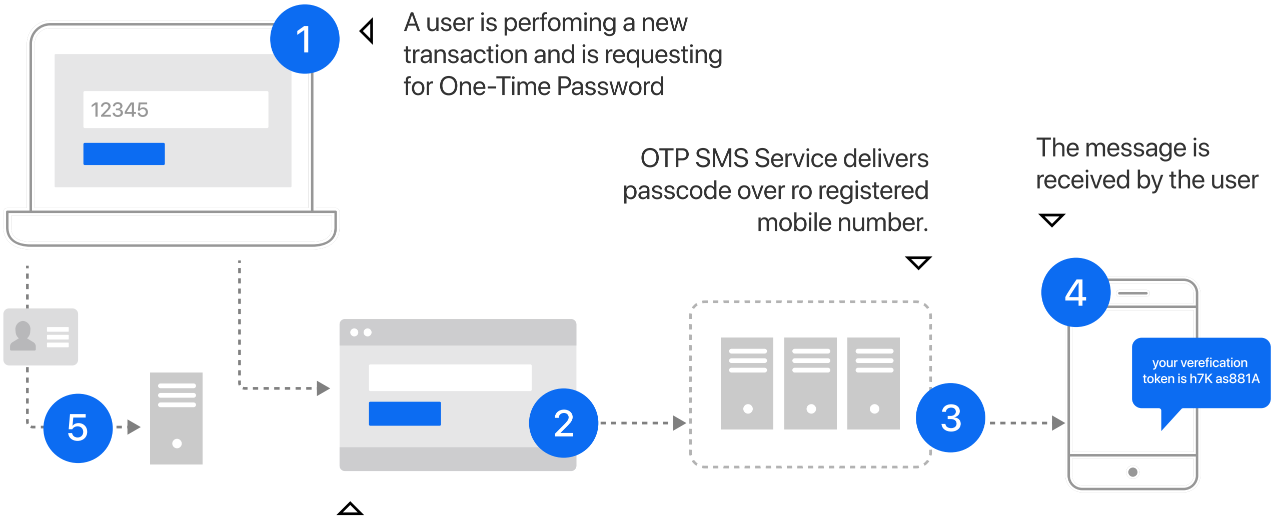
Transactions confirmation is an extra layer of authentication that protects the most critical and potentially vulnerable functions such as sending money, deposits, withdrawals. It can be implemented multiple ways, but the most commonly used approach is one-time password (OTP) delivered via SMS. However, it is proven to be one of the less secure methods of authentication. While the SMS OTP option has certain advantages and many of SMS providers claim to have all possible security certificates, there are certain facts to consider:

- It was never designed for security;
- It relies on operator practices around number porting;
- It doesn’t protect against phishing, although it does force attackers to implement a real-time attack;
- It doesn’t have the sort of delivery guarantee that authentication demands — a delay in delivery of minutes can effectively lock the customer out.

So, at Velmie we suggest passcodes function as a default approach to transaction authentication. Passcode is specifically designed for security and has no “middlemen” involved. This makes things much harder for potential attackers, as they would not only need the username and password, but would also need possession of a 2FA device (phone or other hardware). Passcode is stored as an encrypted token on the user's device and ensures that he is the person who can perform certain actions such as deposits and withdrawals.

1 | STRONG CUSTOMER AUTHENTICATION

OTM SMS TransactionsConfirmation



A user is perfoming a new transaction and is requesting for One-Time Password

The application server receives the request and generates a One-Time Password. The password is sent using messagin API.

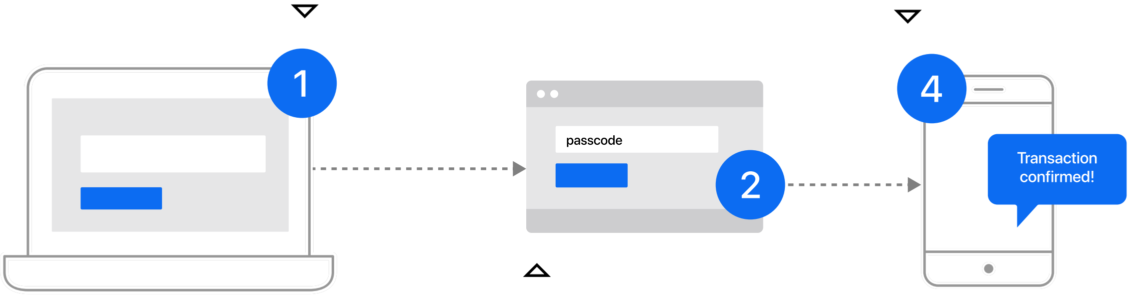
OTP SMS Service delivers passcode over ro registered mobile number.

The message is received by the user

your verefication token is h7K as881A

Passcode Transaction Confirmation

A user is perfoming a new transaction and is requested to enter a passcode



A user enter the passcode and clicks submit

The message is received by the user

Transaction confirmed!

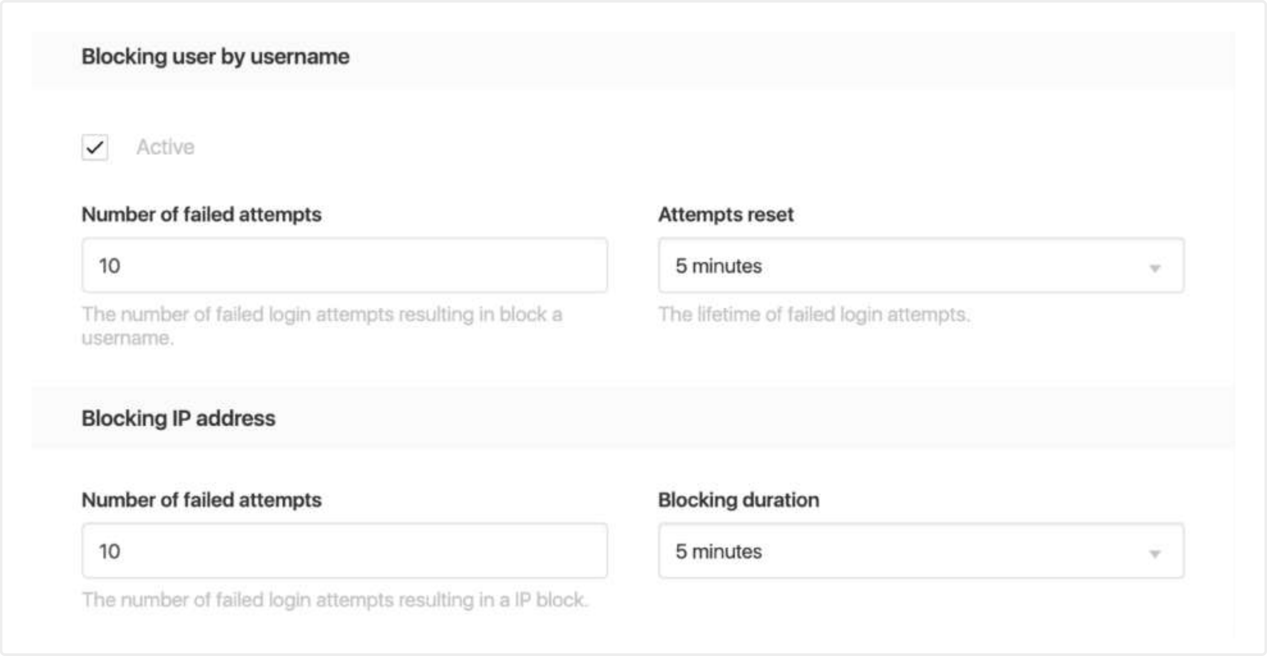
1.2. Login Security

Once the security features mentioned above are implemented, it is also crucial to extend them with administration tools so as to effectively orchestrate the operations. We strongly suggest adding the following features to your software:

1

Ip block

Blacklist or whitelist certain IP addresses or IP range to make sure there is no unauthorized access.



Blocking user by username

☑ Active

Number of failed attempts: 10

The number of failed login attempts resulting in block a username.

Attempts reset: 5 minutes

The lifetime of failed login attempts.

Blocking IP address

Number of failed attempts: 10

The number of failed login attempts resulting in a IP block.

Blocking duration: 5 minutes

Source: Velmie Digital Banking Platform

1 | STRONG CUSTOMER AUTHENTICATION

2 Failed attempts management

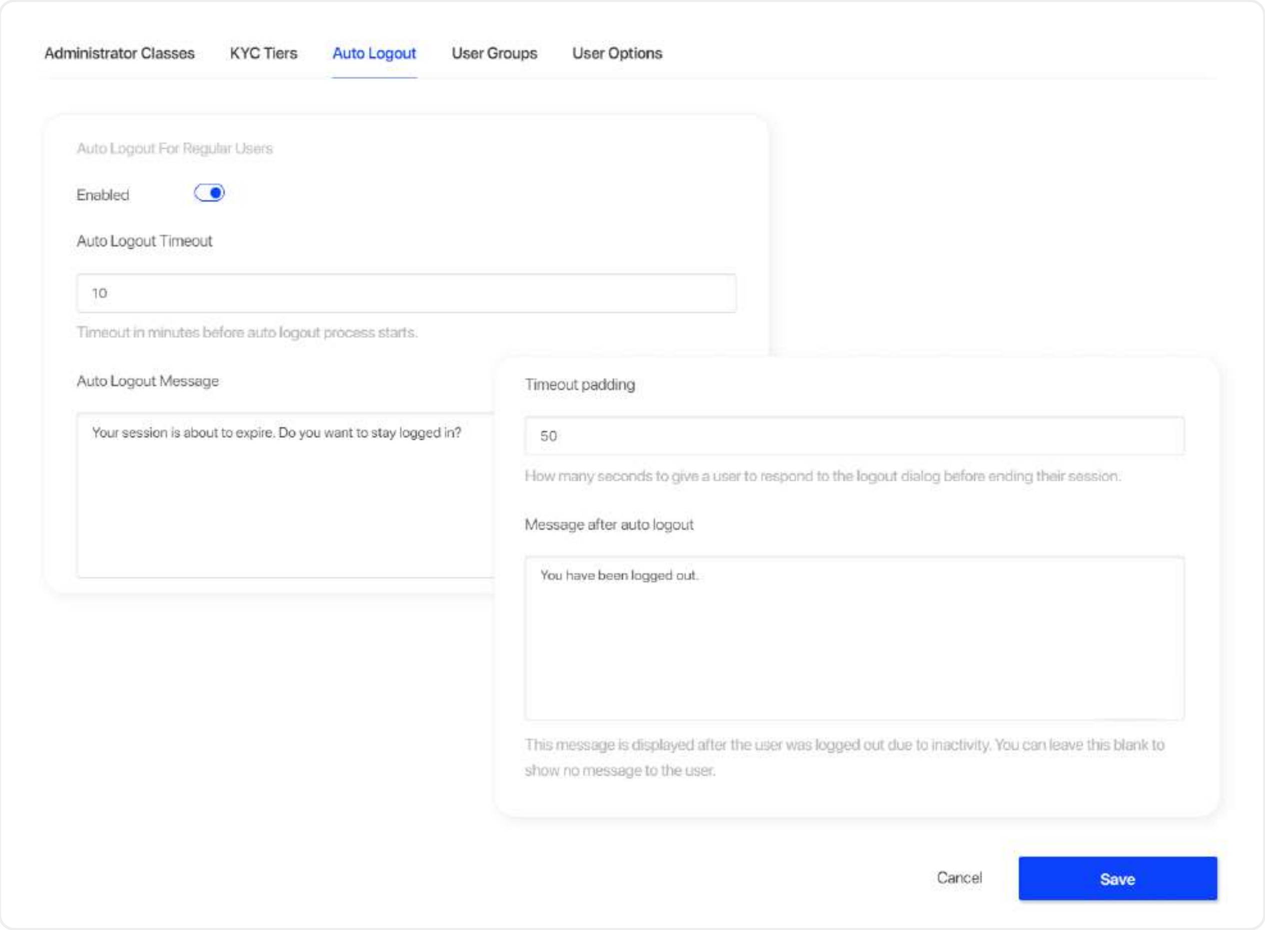
Manage the number of failed login attempts and the timeout between them in order to prevent so-called brute force attacks.

3 Data logging

See who entered the system and when to be able to trace the actions. Keep in mind you’re going to bring all the keys to the hands of your customers and this is the biggest threat. Once you receive complaints of unauthorized access or transactions you will have the right tools to investigate what happened. See more about the audit trail further.

1.3. Idle Timeouts

Idle or inactivity timeout defines the amount of time a session will remain active in case there is no user activity. Upon termination of the defined time frame since the last request received by the application for a given session ID, the system closes and invalidates the session. An application that does not enforce a timeout-based log out is often considered insecure, unless it is required by a specific functional requirement.



Auto Logout For Regular Users

Enabled ●

Auto Logout Timeout

10

Timeout in minutes before auto logout process starts.

Auto Logout Message

Your session is about to expire. Do you want to stay logged in?

Timeout padding

50

How many seconds to give a user to respond to the logout dialog before ending their session.

Message after auto logout

You have been logged out.

This message is displayed after the user was logged out due to inactivity. You can leave this blank to show no message to the user.

Source: Velmie Digital Banking Platform

1 | STRONG CUSTOMER AUTHENTICATION

The most appropriate timeout should be a balance between security (shorter timeout) and usability (longer timeout) and heavily depends on the data sensitivity level handled by the application. For instance, a 60 minute log out time for a public forum can be acceptable, but such a long time would be too much for a banking application. The recommended maximum timeout for such solutions is 15 minutes.

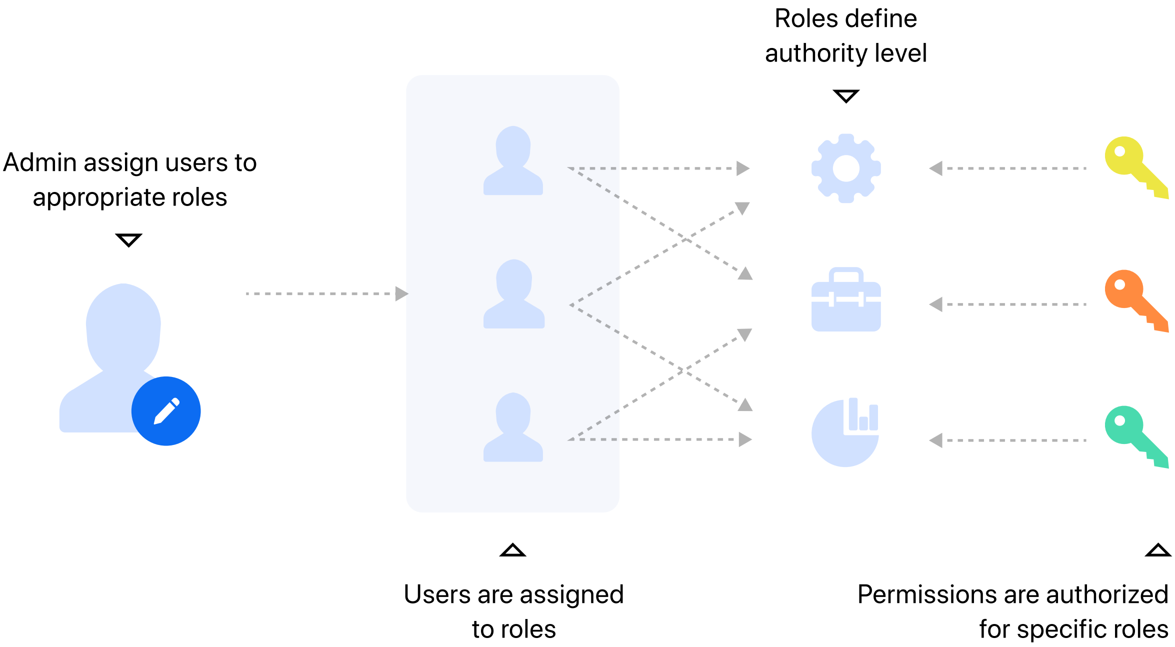
The idle timeout limits the chances that an attacker has to guess and use a valid session ID of another user. However, if the attacker is able to hijack a given session, the idle timeout does not limit the attacker's actions, as he can generate activity on the session periodically to keep the session active for longer periods of time. Session timeout management and expiration must be enforced server-side.

If some data under the control of the client is used to enforce the session timeout, for example using cookie values or other client parameters to track time references, an attacker could manipulate these to extend the session duration. So the application has to track the inactivity time on the server side and, after the timeout is expired, automatically invalidate the current user's session and delete all data stored by the client.

It is specifically useful to keep the sessions management under the app setting to be able to constantly track the user experience and adjust it when needed.

2 | ROLE-BASED ACCESS CONTROL

Roles with different privileges and responsibilities are central features of most organizations. Some computer applications dating back to at least the 1970s had limited forms of access control based on the user's role in an organization. These early role-based systems were typically ad hoc and application-specific, but general-purpose models for role-based access control (RBAC) began to emerge in the 1990s. Today, most large firms are using some form of RBAC, and its popularity continues to grow. However, organizations often support thousands of users and permission controls, leading to complex systems with security and interoperability issues that must be addressed in designing a role structure.



Roles define authority level

Admin assign users to appropriate roles

Users are assigned to roles

Permissions are authorized for specific roles

A key feature of the RBAC model is that all access is through roles. A role is essentially a collection of permissions, and all users receive permissions only through the roles they're assigned, or from roles they inherit through a tree-like role hierarchy.

2 | ROLE-BASED ACCESS CONTROL

Controlling all access through roles therefore reduces the administrative burden for security managers and improves the auditing of controls. Conceptually, the RBAC model enforces three rules:

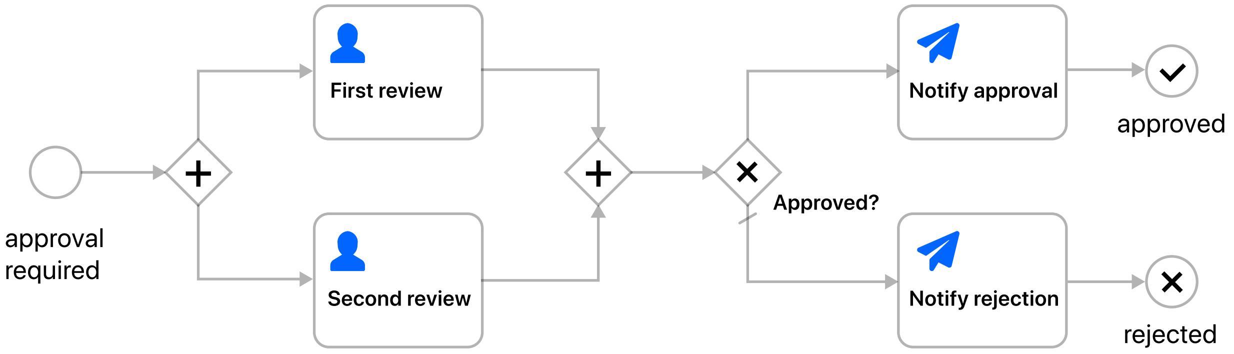
- role assignment – a user can access a permission only if he or she has been assigned a role;
- role authorization – a user's active role must be authorized;
- permission authorization – a user can access a permission only if the permission is authorized for that user's active role.

Together, these rules ensure that users have access only to permissions authorized for them. However, for practical applications, extra controls might be needed. 4-eyes rule or maker-checker operations are probably the most common additional constraints used in large organizations. A typical requirement is that a user can't both initiate and approve a large transfer amount – which RBAC enforces by prohibiting any user from having a collection of roles that give access to both the "transfer initiation" and "transfer approval" permissions.

Other constraints, such as the number of users allowed in a role, or more complex issues, like access authorization by time of day, can be supported by different RBAC systems.

3 | MAKER-CHECKER

Maker-checker (or Maker and Checker, or 4-Eyes) is one of the central principles of authorization in the information systems of financial organizations.

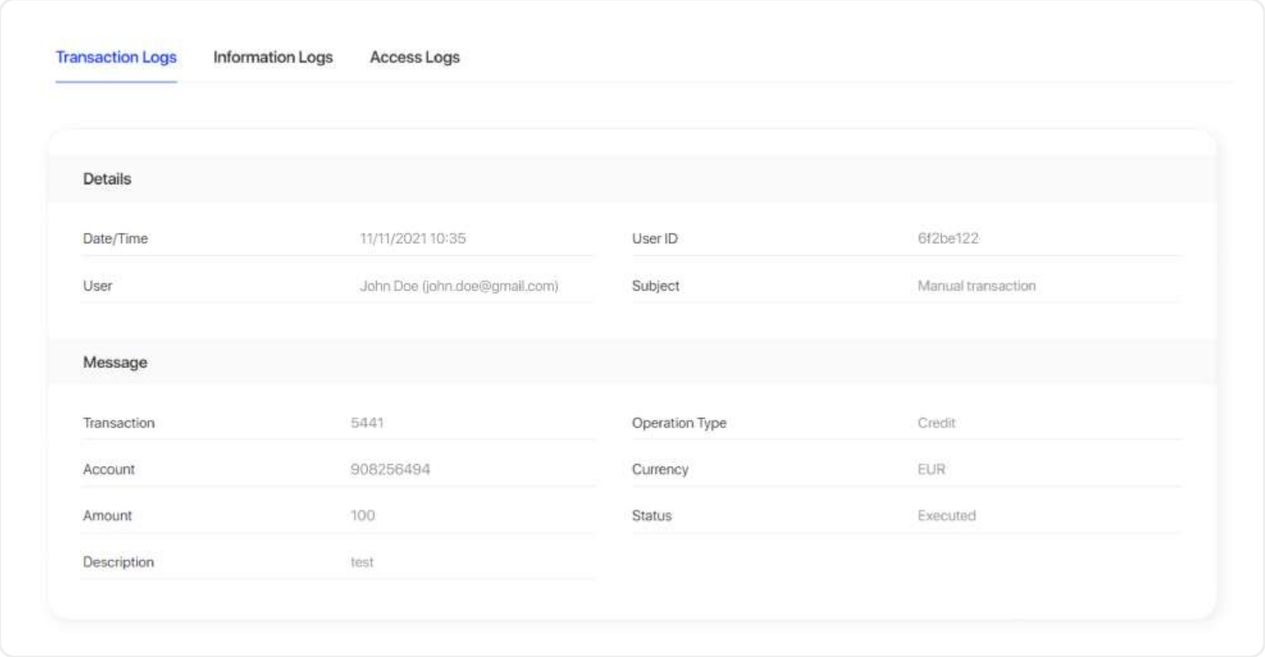


Segregation of duties is critical to preventing fraud and errors. Treasuries deal with large sums of money on a daily basis and two of the key operational risks are fraud and error. Segregation of duties is the notion that no employee should be in a position both to commit and to conceal fraud or errors – whether deliberately or accidentally – in the usual course of their duties.

When considering how to prevent error or fraud, the maker-checker principle is to involve several people and/or technology throughout the cycle of a transaction in order to minimise the risk of fraud or undetected errors slipping through.

4 | AUDIT TRAIL

Logging is an important asset of the application architecture security since it can be used to detect flaws in applications as well as sustained attacks from rogue users. Logs are typically properly generated by web and other server software. It is not common to find applications that properly log their actions to a log and, when they do, the main intention of the application logs is to produce debugging output that could be used by the programmer to analyze a particular error.



Details

Date/Time	11/11/2021 10:35	User ID	6f2be122
User	John Doe (john.doe@gmail.com)	Subject	Manual transaction

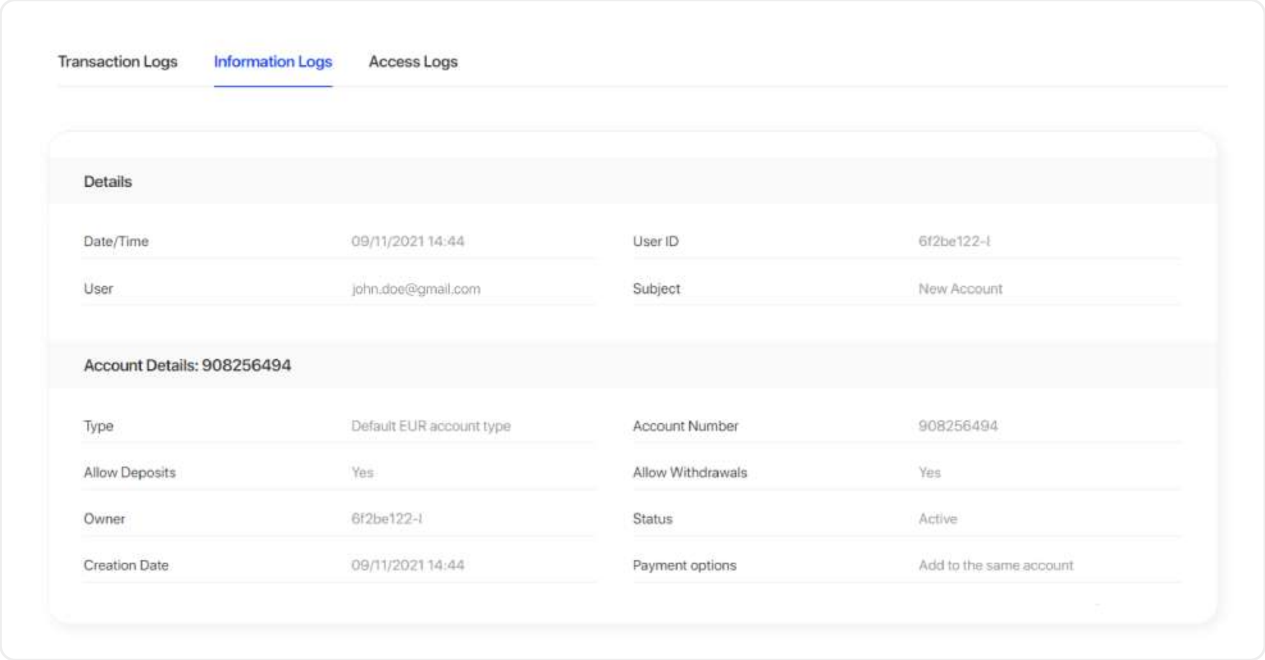
Message

Transaction	5441	Operation Type	Credit
Account	908256494	Currency	EUR
Amount	100	Status	Executed
Description	test		

Source: Velmie Digital Banking Platform

Event log information should never be visible to end users. Even product administrators should not be able to see such logs since it breaks separation of duty controls. Ensure that any access control schema that is used to protect access to raw logs and any applications providing capabilities to view or search the logs is not linked with access control schemas for other application user roles. Neither should any log data be viewable by unauthenticated users.

4 | AUDIT TRAIL



Details

Date/Time	09/11/2021 14:44	User ID	6f2be122-l
User	john.doe@gmail.com	Subject	New Account

Account Details: 908256494

Type	Default EUR account type	Account Number	908256494
Allow Deposits	Yes	Allow Withdrawals	Yes
Owner	6f2be122-l	Status	Active
Creation Date	09/11/2021 14:44	Payment options	Add to the same account

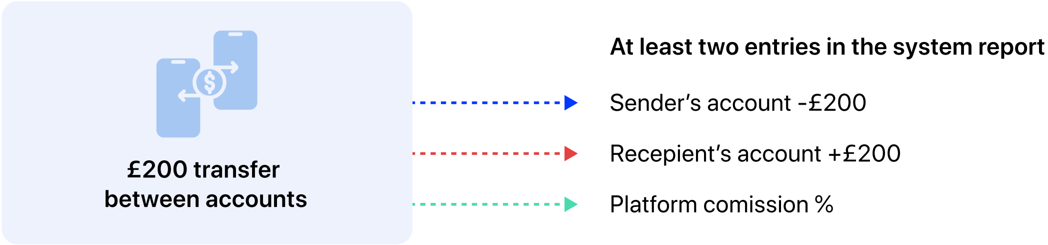
Source: Velmie Digital Banking Platform

Velmie recommends to have logs at least for the following information:

1. Logs of transactions which come with all transactions and transaction requests made by users or staff. The record should include timestamp, type of transaction, user, currency and amount.
2. Events log which represents changes made to user profiles and accounts either by them or platform staff. It should include information such as timestamp, user, type of action, list of changes to be able to view the current and past records.
3. Access log should give the information about all logins made by users across all supported devices. The log tracking should show an IP and a timestamp.

5 | DOUBLE-ENTRY BOOKKEEPING

The basic concept of double entry is that a single transaction, to be recorded, will hit two accounts. For example, when someone borrows money from a bank, the cash account will increase as well as liability account loans payable will increase. Double entry also allows for the accounting equation (assets = liabilities + owner's equity) to always be in balance.



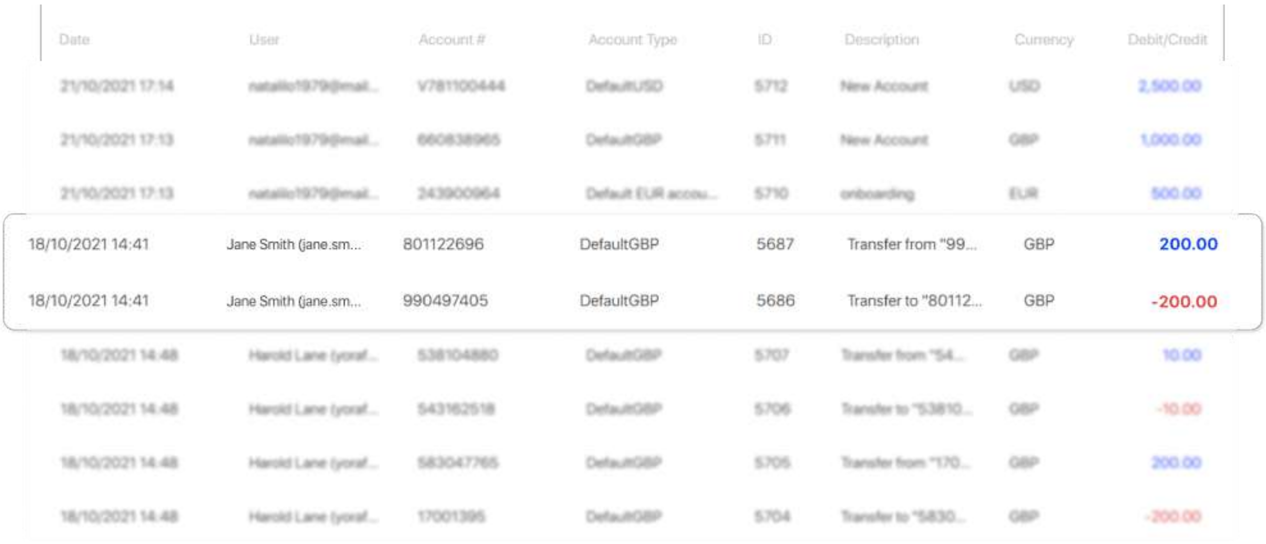
£200 transfer between accounts

At least two entries in the system report

Sender's account -£200

Recepient's account +£200

Platform comission %



Date	User	Account #	Account Type	ID	Description	Currency	Debit/Credit
21/10/2021 17:14	natalilo1979@mail...	V781100444	DefaultUSD	5712	New Account	USD	2,500.00
21/10/2021 17:13	natalilo1979@mail...	660838965	DefaultGBP	5711	New Account	GBP	1,000.00
21/10/2021 17:13	natalilo1979@mail...	243900964	Default EUR accou...	5710	onboarding	EUR	500.00
18/10/2021 14:41	Jane Smith (jane.sm...	801122696	DefaultGBP	5687	Transfer from "99...	GBP	200.00
18/10/2021 14:41	Jane Smith (jane.sm...	990497405	DefaultGBP	5686	Transfer to "80112...	GBP	-200.00
18/10/2021 14:48	Harold Lane (yoraf...	538104880	DefaultGBP	5707	Transfer from "54...	GBP	10.00
18/10/2021 14:48	Harold Lane (yoraf...	543162518	DefaultGBP	5706	Transfer to "53810...	GBP	-10.00
18/10/2021 14:48	Harold Lane (yoraf...	583047765	DefaultGBP	5705	Transfer from "170...	GBP	200.00
18/10/2021 14:48	Harold Lane (yoraf...	17001395	DefaultGBP	5704	Transfer to "5830...	GBP	-200.00

Source: Velmie Digital Banking Platform

Advantages of a Double-Entry Bookkeeping System

- **Scientific.** Double-entry system has its own set of principles and rules. Under those principles and rules, two aspects of every financial transaction are recorded.

- **Systematic.** A systematic technique is followed in recording financial transactions in a double-entry bookkeeping system. It records financial transactions in a systematic and chronological order with suitable narration of the financial transaction.

- **Complete.** It records not only each and every financial transaction, but also each aspect of the transaction.

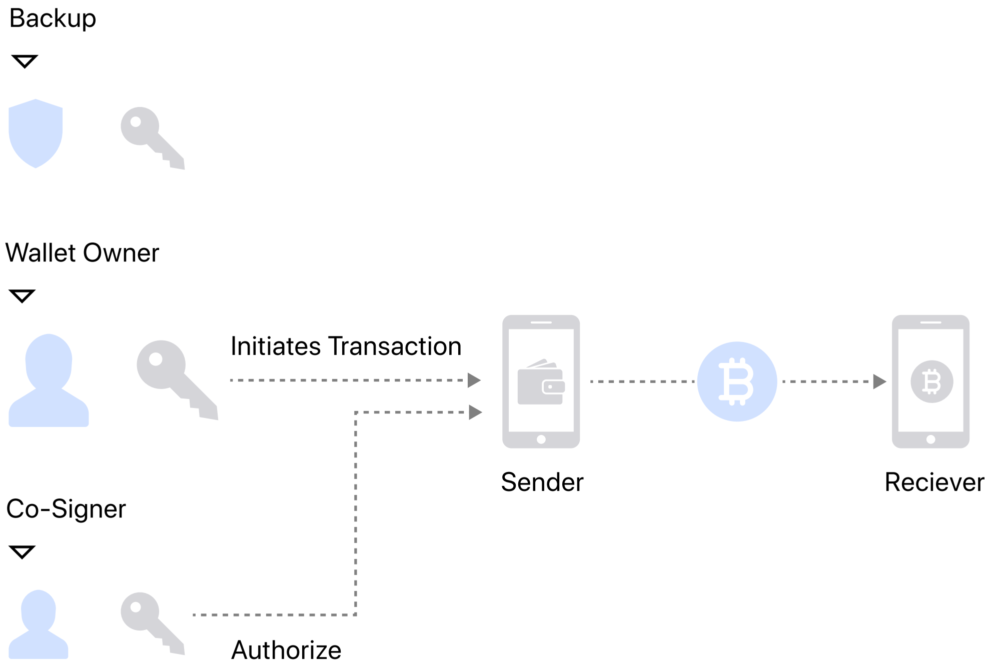
- **Accuracy.** Double-entry book-keeping system is based on the double-entry principle which means for every debit amount there is a corresponding credit amount. Such a method of debit and credit can help ensure arithmetical accuracy of the recordings of financial transactions.

- **Profit or Loss.** The system helps to ascertain the true profit or loss of a business by preparing the profit and loss account for a given period.

BONUS: MULTISIGNATURE TRANSACTIONS

In cryptocurrencies, multisignature features (also known as multisig) allow users to sign a transaction with more than one private key. Funds protected with multisignature can only be spent by signing with M-of-N keys. M-of-N is a concept, according to which you take the private key in a public-private key pair, and you make it necessary for a group of people to be involved in using it, rather than just one.

In traditional business, "key person risk" refers to when a company relies too much on one individual to succeed. Cryptocurrency businesses are prone to a very literal version of this risk when handling funds. Fortunately, multisignature cryptocurrency wallets offer a built-in way to manage this sort of risk.



1 The wallet owner initiates a transition. 2-of-3 signatures are required to complete a transaction

2 A co-signer must authorize the initiated transaction. The pending transaction get confirmed and moves to the receiver.

3 Only authorized transactions will be approved and sent to the receiver.

BONUS: MULTISIGNATURE TRANSACTIONS

Multisignature wallets are cryptocurrency wallets that require two or more private keys to sign and send a transaction. The process in overall is similar to the maker-checker feature mentioned above as both require one or more trusted persons to verify a transaction. Thanks to blockchain, this function can now be delivered to clients in a user-friendly way to guarantee extra security.

Properly used, multisig can mitigate the hazards of dealing with digital bearer assets where transactions are irreversible. Most notably, crypto exchanges, brokers/OTCs, investment funds and other crypto companies use multisignature storage to secure their cold storage funds. Exchanges, brokers and the like distribute admin keys for their funds in order to distribute the risk. If hackers want access to their reserves, they're going to need several keys to do so. Similarly, multisig ensures no one person in the firm is able to unilaterally withdraw funds from the account. The more signatures you need to execute a transaction, the more distributed the decision-making process can be. Other specific use cases may involve setting up a shared account among family members or an escrow account.

Relatively speaking, multisig is still a niche custody practice among cryptocurrency holders. Still, that doesn't mean a typical crypto user doesn't use it to custody their coins.

4 | ABOUT VELMIE

Velmie is a banking technology provider with more than 10 years of expertise in developing software and providing professional services. We power enterprise banks and mobile wallet companies globally, setting up the clients with sophisticated products that are secure and regulatory-compliant.

Email: hello@velmie.com
Visit Website: velmie.com

United States

501 Silverside Road
Suite 105 Wilmington, DE 19809

United Kingdom

120 High Road
East Finchley London, N2 9ED

Lithuania

Saltiniu g. 5-101 Vilnius,
LT-03214

Belarus

Liebknecht street 66
Minsk, 220036