Segmenting the legacy monolithic approach to Financial Services with Sibedge

The importance of KYC

Fintech businesses must meet the Know Your Customer challenge in a rapidly developing environment.

Financial services have rightfully positioned themselves among the leading industries in market growth for the past few decades. Organizations in this sector constantly have to adjust in order to stay competitive in such a rapidly and aggressively changing market. While actively building their client base, companies must invest heavily in their infrastructure and optimize internal processes. Users demand faster access to new services with no additional downtime or data loss, so speed remains a key factor for a successful business.

On the other hand, companies have to ensure anti-money laundering compliance and prevent identity fraud to create a long-term trusted platform. This task demands a heavy reliance on the verification process and additional manual steps with human supervision. Keeping the balance between time-to-service for new users and reducing costs for their successful verification creates a certain gap. Sibedge helps to bridge this gap with solid hands-on expertise in developing fintech solutions.

Company NDA

About company

A global leader in online trading services with a user base of over 4 million satisfied customers worldwide.

Industry

Fintech

Team

Golang Developer	1
iOS Developer	1
Android Developer	1

Duration

4 months

Technologies

- Golang

The importance of verification

Fast and automated verification is key to ensuring happy customers.

With over 30% of our clients coming from the financial sector over the past five years, Sibedge has acquired steady in-house knowledge in building, upgrading, and maintaining first-class fintech solutions. We know that behind every one of these solutions lies a complex platform that may contain inherently different types of services, from banking and gambling to blockchain. But no matter the company's core service, user verification will persist as a vital step in security enforcement and provision.

Online financial institutions must comply with a number of anti-fraud laws, such as Know Your Customer (KYC) and Anti-Money Laundering (AML). Gathering and assessing customers' or potential customers' data helps companies prevent criminals from using their apps for illegal acts.

KYC begins right at customer onboarding and usually requires valuable time to perform. By accelerating customer due diligence, companies can reduce fraud risks and increase overall time-to-service for each customer. Optimizing this process results in a better customer experience and allows clients to start provisioning their core services faster.

About Our Client

Sibedge helps a global leader in online trading successfully segment its legacy approach.

Over the past decade, one of our Clients has rapidly and successfully risen to become a global leader in online trading services. With a user base of over 4 million satisfied customers worldwide, the Company has recently faced a new challenge. Growing from a small tech startup with a single service, the Company's software has transformed significantly into a multi-service solution with large volumes of data stored within the system. However, like many tech startups, the software was based on the "monolithic architecture" approach, where the core app has different highly coupled components.

Solution

External IT audit as a basis for long-term cooperation.

Most tech companies facing a turbulent active growth stage maintain focus on external metrics: ways to grow their client base and increase market share. In such cases, keeping their solutions and data protected, fault-tolerant, and scalable might escape the premiere focus. Or in a reverse situation, the organization might understand the risks taken but lack the resources or expertise to solve the problem.

Over the past 16 years, Sibedge has become a proven expert in building and evaluating various IT services. We know from real-world experience how important it is to safeguard all existing assets.

Solution

Constantly checking that information management processes comply with IT-specific laws, policies, and standards is the right way to establish sufficiency in IT systems and associated management.

By providing an IT audit and system evaluation as the first step, Sibedge demonstrated solid expertise in the Company's subject field. Building trust is a crucial first step and became a basis for long-term cooperation. A full system review allowed the Sibedge team to test the reliability and integrity of the Company's processes, business logic, and the solution's architecture.

KYC and AML practices are the first and most crucial steps for a financial service provider. It becomes a touchstone of the onboarding process for future customers. Any emerging mistakes at this early stage guarantee failures and even prevent clients from using the trading services properly.

Extracting the KYC service from a monolithic architecture

During the growth and development stage, startups commonly build a single, unified software solution. By utilizing a monolithic architecture, the Company initially built its solution faster because it eased the coding and deployment process by allowing everything in the system to be released simultaneously.

The following shows the KYC service as a part of the monolithic system architecture:
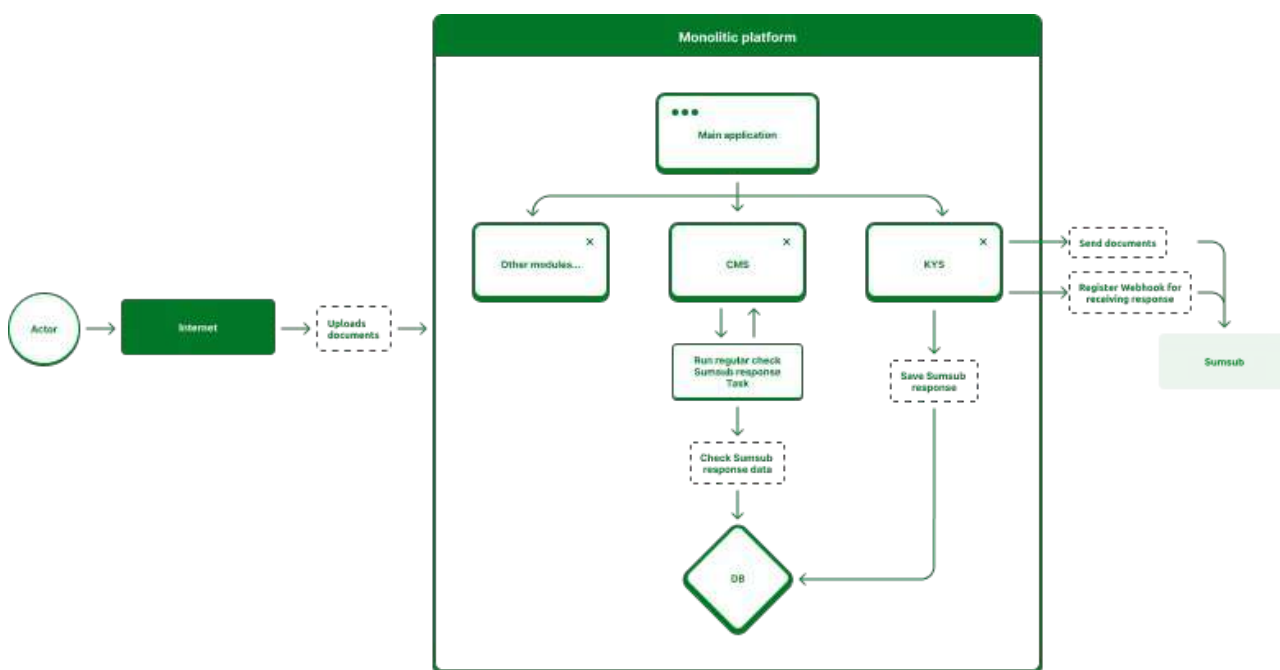
Despite being a part of the monolith, KYC is a separate process with several steps to avoid discrepancies by successfully identifying and verifying customer identities.

This task includes two main stages before the rest of the onboarding process can proceed:

- Verifying clients' identities based on a reliable, independent source like a government-issued ID document.
- Providing an interim conclusion based on the scoring model to determine if the client is eligible to trade.

These two services play a key role in the verification process, and financial companies often heavily rely on third-party solutions. The current market is saturated with different KYC services, so we highly recommend our customers stay up-to-date with recent tech trends.

The microservice architecture expedites a more seamless transition to a new service provider. The days of zero application downtime are upon us since you no longer need to stop the whole system for necessary code changes. The new versions of the microservices can be released faster with no additional costs. Supporting horizontal and vertical scaling brings opportunities to endure peak loads with more elasticity.

During a 4-month project period, Sibedge was able to gather different parts of the verification process and extract and reconfigure them into a dedicated microservice:
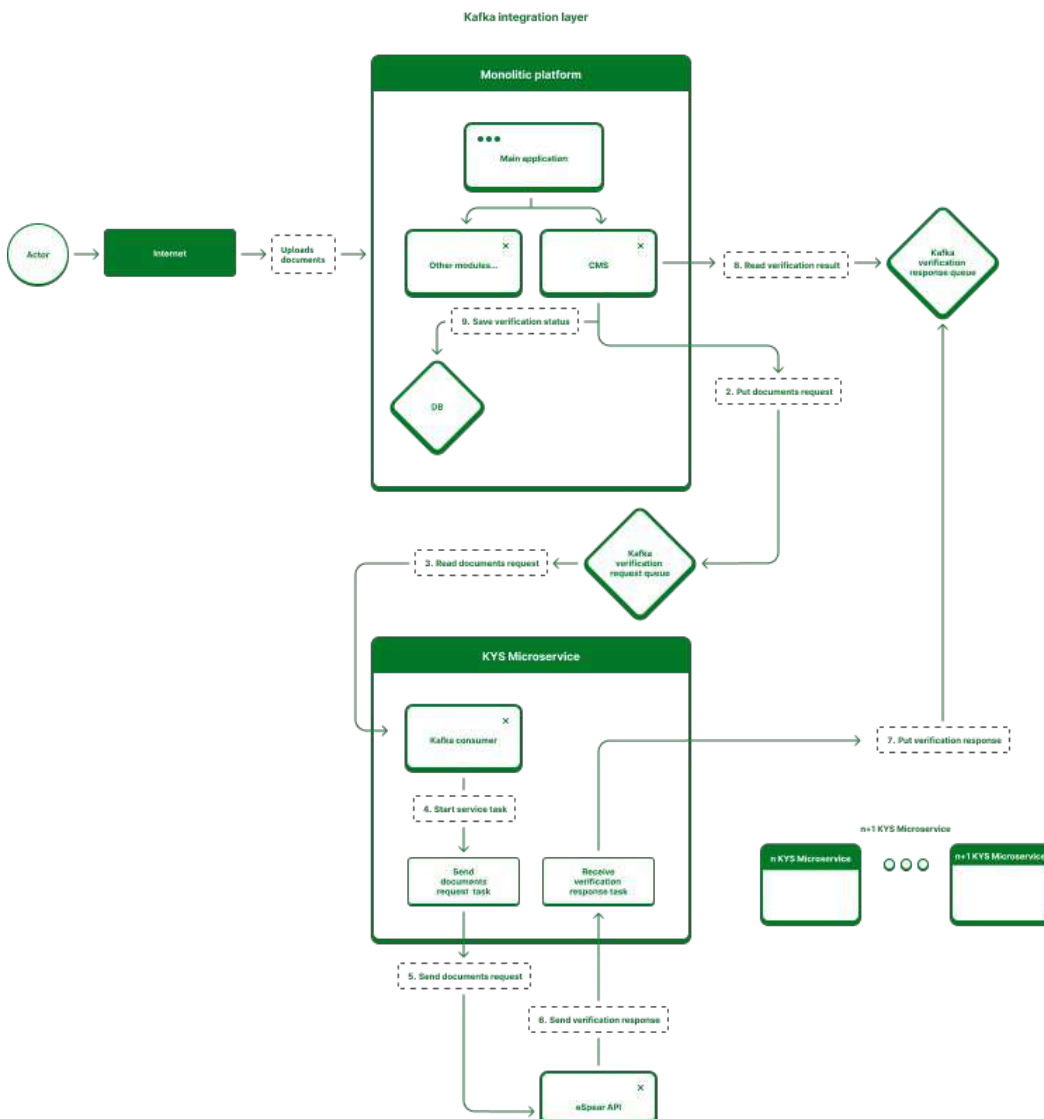
Extracting the KYC service from a monolithic architecture

While preserving the initial business logic flow, this approach allowed the Company to easily replace third-party service providers, expand its software capabilities, and match the increased resource demand. More importantly, it provided the perfect chance to transfer the existing verification services to the cloud. During peak loads, cloud hosting frees up additional CPU and memory resources to process extra requests, resulting in a more efficient way for the Company to utilize its infrastructure investments since there is no need to pay for excess capacities.

By deploying multiple instances of the KYC microservice, the system can simultaneously handle a higher volume of document verification requests, leading to faster processing times. It also empowers the development team to work on the microservice independently without being tied to the main solution. The added flexibility to implement new technologies and refactor the codebase ultimately leads to a more efficient and scalable system.

Increasing query processing

The original system, including the customer due diligence segment, was based on PHP and could sustain the service's primary goal. However, the comprehensive audit performed by Sibedge revealed a number of unstable processing and document verification issues that required manual fixing within the system.

Speeding up the KYC microservice

According to industry best practices, every separate microservice should be packaged in a standalone Docker container and deployed in a container orchestration environment, such as Kubernetes. Kubernetes must be executed like an operating system process and subject to constant health checks to monitor the health of each microservice. This approach provides continuous fault tolerance for your application. If a microservice stops responding, Kubernetes starts a new live instance of the service, and query processing continues automatically, ensuring uninterrupted service.

While our customers can still execute specific PHP scripts in the background, we highly recommend they use a compiled-based programming language for improved performance. The Company previously relied on a legacy approach of generating triggers every other minute to process the required data. However, switching to a compiled-based programming language significantly reduced the overall processing time for the KYC-microservice.

The best solution was to migrate the entire app from PHP to a Golang stack. The main advantage of Golang is its ability to process operations and data in the background mode, which reduces the number and frequency of direct requests. After implementing this solution, Sibedge balanced the overall system load, allocated important resources, and increased the KYC processing speed by 75%, reducing it from 2 minutes to only 30 seconds.

Shifting responsibility on the backend

The client verification status can be divided into 3 stages: the upcoming request for verification, the verification taking place, and the approval or denial of the status. For each stage, the application must regularly launch a set of tasks to check the status of the ID documentation, including whether the documents were sent to the third-party service, successfully recognized, translated into text, and received back as text data.

Regardless of the success or failure in the mentioned stages, the response from the third-party vendor must be received via the API and stored in the Company's CRM. Initially, the support team could keep an eye on all the statuses and perform necessary operations. However, as the user base grew, it became impossible to detect and manually handle such instances on time, thereby putting the Company's reputation at serious risk.

Launching regular tasks is the backend's area of responsibility. Due to the nature of PHP (it was designed for processing web requests), it is not the best language for running backend tasks. Keeping this approach makes it difficult to support and develop code bases for the future. Migrating the app into a more suitable Golang stack and refactoring its codebase allowed the Company to mitigate those risks. The Company gained full transparency over the process's backend, which reduced overall verification time.

Replacing the ID verification third-party service provider

The integral component of every client due diligence system is the collection of potential customer personal data, including identification documents. In this regard, financial companies rely on third-party solutions connected to the internal system via API. During the audit, Sibedge detected poor performance of the current identity verification software. The process took up to several minutes to recognize uploaded documents and return their text versions. This approach was unacceptable from the clients' perspective, as it significantly extended the time-to-service and direct access to trading services.

In approximately 15% of cases, the ID verification service could not recognize the provided documents, exacerbating the situation for the Company. In this scenario, the service reports back to the system and offers the Company the option to manually check the documentation and input the correct data into the CRM. This system placed an additional burden on the support team, taking up to 1 hour per day.

After re-evaluating the list of potential vendors Sibedge, proposed replacing the current one with a more suitable and reliable service provider. The new service provider, Sumsub, was selected after a thorough evaluation of potential vendors based on factors such as pricing, API usability and scalability, implementation cost, and query response time. Implementing Sumsub's ID verification service significantly reduced the manual verification time by 58% to only 25 minutes.

Mitigating peak load risks

The system should be designed to handle high volumes of user sign-ups and mitigate peak load risks, especially after expansion to new markets. Horizontal and vertical scaling achieve this with elasticity and increased capacity. Since the Company has migrated to a microservice architecture, they can rest assured that a surge in verification requests will not affect the overall time-to-service for clients and will not block support from other important tasks.

Furthermore, Sibedge has helped to increase the system's flexibility in integrating with other ID-verification providers. The system can seamlessly release a new version of the vendor's API or change vendors without causing downtime for the entire system, allowing for seamless and hidden changes for the system clients.

Result

- The cost of user verification decreased by 34%.
- The overall time for new user verification decreased from 2 minutes to only 30 seconds.
- The user verification process sped up by 75%.
- The percentage of successful ID verifications increased from 85% to 96%.
- Manual verification time reduced to just 25 minutes per day.
- Developing and releasing new features became easier and faster.
- The potential issue of high-loading was successfully avoided.

🌐 www.sibedge.com   in www.linkedin.com/company/sibedge/

✉ contacts@sibedge.com