WHITEPAPER

Revolutionising FSCS SCV Reporting: Ensuring Data Accuracy and Integrity by Resolving Technology Challenges.

macro global®
creating value through innovation

SASF

Table of Contents

Introduction

The FSCS Single Customer View reporting system is critical in the financial industry as it consolidates and presents a complete, accurate picture of a single customer's service interactions across several channels. This type of reporting is critical for developing consumer insights, ensuring regulatory compliance, and optimising risk management tactics. In an era where data-driven decisions are critical, SCV reporting enables organisations to successfully exploit customer data, resulting in personalised offerings and stronger customer connections.

Many present systems rely on manual operations, which causes concerns with data integrity, accuracy, and timeliness. These methods frequently suffer from silos of customer information, leading to data duplication and ineffective data aggregations. Furthermore, regulatory standards are growing stricter, exposing organisations to the dangers of noncompliance and data breaches. As a result, traditional systems are frequently insufficient in giving a comprehensive perspective of consumer interactions, thus impeding decision-making processes.

Given these challenges, there is an urgent need for a more effective, accurate, and secure SCV reporting solution. Current landscapes require solutions that not only expedite data integration and validation procedures, but also improve data security through strong encryption technologies and advanced data validation methodologies.

An innovative approach to SCV reporting is required to satisfy the changing expectations of the financial industry, ensuring that organisations remain compliant, effectively manage risk, and nurture long-term client relationships. The creation of a sophisticated automated SCV reporting system is thus a critical step toward meeting these pressing industrial needs.

Objectives

Macro Global's R&D team aims to improve the efficiency, accuracy, and security of the banking industry's Single Customer View reporting process. The initiative's objectives are as follows:

- **Automate the FSCS SCV Reporting Process:**
  Create an advanced automated platform that simplifies the SCV reporting workflow, minimising manual intervention, and allowing for faster data processing. This automation will make way for real-time updates, increase operational efficiency, and reduce human errors associated with traditional reporting techniques.

- **Improve Data Accuracy:**
  Use AI-powered data validation technologies to assure the integrity and correctness of customer data. The system will use powerful algorithms to discover and fix inconsistencies, duplication, and errors in the data, offering a more dependable perspective of customer interactions and improving overall data quality.

- **Ensure Data Security:**
  Implement strong security measures, such as hybrid encryption methods (AES and RSA), to secure sensitive customer data during transmission and storage. This entails developing effective key management policies, access controls, and rigorous data sanitisation procedures to protect against potential data breaches and compliance violations.

Better Data Integration:

Make it easier to integrate with Core Banking Systems so that the SCV reporting system can effectively aggregate data from several sources, developing a uniform customer profile and increasing the overall efficiency of the reporting process.

Meet Regulatory Compliance:

Create a system that complies with the demanding regulatory requirements that financial institutions face, such as data protection regulations. By assuring compliance, the system reduces legal risks and builds trust among stakeholders.

Technological Challenges and Gaps in Existing Systems

The development of Macro Global's FSCS SCV (Single Customer View) Reporting Solution faced a variety of technological challenges. These challenges highlighted significant gaps in existing systems and emphasised the complexities involved in creating an integrated and secure reporting framework. Here's an analysis of those challenges and gaps:

Complex Key Management

Challenge:

Implementing hybrid encryption using AES and RSA required complex key management processes. This brought about potential security risks due to the intricacies of generating, storing, and rotating encryption keys. Performance overhead was also a concern.

Gap in Existing Systems:

Many legacy systems lack robust key management capabilities, exposing organisations to risks related to key exposure, misuse, or loss.

Compatibility Issues

Challenge:

Updating various frameworks and libraries, such as Bootstrap, resulted in compatibility problems with existing code and third-party dependencies.

Gap in Existing Systems:

Legacy applications often do not support modern libraries or frameworks, making upgrades challenging and sometimes leading to software stagnation.

Data Sanitisation

Challenge:

Achieving comprehensive data sanitisation while preserving data integrity proved difficult, with the risk of over-sanitising, which could lead to loss of essential data distinctions.

Gap in Existing Systems:

Many existing data processing systems do not have tailored sanitisation methods, resulting in either excessive data loss or vulnerabilities.

Rate Limiting for Email Flooding Attacks

Challenge:

Preventing email flooding attacks required sophisticated rate-limiting algorithms and infrastructure changes that complicated system architecture.

Gap in Existing Systems:

Existing systems often have basic or insufficient rate limiting, making them vulnerable to abuse and attacks.

Content Security Policy

Challenge:

Configuring an adequate Content Security Policy was complicated by diverse browser compatibilities and complex setups.

Gap in Existing Systems:

Lack of uniformity in content security policies across different systems leads to vulnerabilities, making them susceptible to content injection attacks.

HTML Injection and XSS Protection

Challenge:

Protecting against HTML injections and XSS attacks required stringent input validation and significant refactoring of legacy code.

Gap in Existing Systems:

Many older systems lack thorough input validation mechanisms, rendering them vulnerable to attacks that exploit unsuspecting user inputs.

Integration of Microsoft Single Sign-On

Challenge:

Integrating Microsoft SSO necessitated significant changes to authentication flows and data handling mechanisms.

Gap in Existing Systems:

Existing systems often do not accommodate modern authentication methods like SSO, leading to a fragmented user experience and increased security risks.

Systematic Approach of Macro Global to Address Technological Challenges

Macro Global's R&D team employed a systematic and structured methodology to address various technological challenges encountered during the development of their advanced financial solutions. This approach involved a combination of thorough analysis, strategic planning, and innovative implementation, ensuring effective and timely resolutions to complex issues. Below is a detailed overview of this systematic approach.

Identifying Technological Limitations

Comprehensive Analysis:

The initial phase involved a thorough assessment of existing technologies to identify gaps and inefficiencies. The team critically reviewed traditional systems and their limitations, particularly in areas like security, performance, and interoperability.

Stakeholder Feedback:

Engaging with stakeholders—including clients, industry experts, and regulatory bodies—allowed the team to gather diverse insights. This feedback was instrumental in understanding real-world challenges and expectations.

Market Research:

Continuous monitoring of industry trends and emerging technologies enabled the team to stay updated on new developments and best practices, further informing their analysis.

Establishing Clear Project Objectives

Goal Definition:

Based on the identified limitations, the R&D team set specific and measurable objectives aimed at enhancing the capabilities of the financial solutions. Primary objectives included improving transaction speeds, enhancing security features, and ensuring regulatory compliance.

User-Centric Focus:

The project objectives emphasised not only technological advancements but also the importance of user experience. This ensured that solutions were designed with end-users in mind, fostering greater acceptance and satisfaction.

Innovating Advanced Solutions

To fulfil the set objectives, Macro Global concentrated on incorporating advanced technology into the FSCS SCV system.

Hybrid Encryption (AES + RSA):

The R&D team intended to combine modern encryption algorithms to provide strong data security. AES would offer efficient symmetric encryption for data at rest, whilst RSA would enable secure key exchanges and asymmetric encryption for sensitive data transit. This hybrid architecture would balance security and performance requirements, addressing complaints about standard encryption methods. Thus, this maintains a high standard of compliance and data security across the whole regulatory life cycle and secures your SCV output files with a sophisticated and highly encrypted authentication mechanism.

AI-Driven Data Validations:

To address concerns about data accuracy and integrity, the team implemented AI-powered data validation frameworks.

By employing algorithms, formulas, and logic that are consistent with established business regulations, AI-based validation eliminates human error. It simplifies account and customer rule management, improves data enrichment, and assures validation.

AI algorithms detect incorrect customer and account holder information, account segregation, data duplication, and other anomalies.

Automated reconciliation can take place at any time during the accounting period, generating a complete audit record of all reconciliations.

Reliable methods for checking various data points across numerous sources are provided via integration with reputable third-party databases, such as FCA DB, Companies House, Royal Mail DB, Charities Register, BFPO Address, and OFAC Sanction checks. This procedure intends to improve data accuracy, decrease fraud risk, and enhance business operations.

Moreover, third-party platforms provide a variety of integration possibilities, such as APIs for automated validation, bulk upload tools for large datasets, user-friendly web services, and batch processing for offline verification.

Robust Integration with Existing Banking Systems:

In recognition of the necessity for seamless interoperability, the team developed a system that can be integrated with any primary banking system or external data sources, such as legacy platforms or Excel-based data.

It facilitated the effortless import of the necessary data and identify the individuals & organisations that need to be reported, like exclusion, effectiveness, and completeness reports.

Adapting current Frameworks:

The implementation strategy involved using current software frameworks to improve performance and scalability. By utilising flexible web design and microservices architecture, the team guaranteed that the SCV system was not just adaptive but also ready for future updates.

Macro Global aims to establish a safe, dependable, and user-friendly FSCS SCV reporting system by integrating innovative technologies comprehensively, thereby creating a new benchmark for data management in the financial services industry.

Tackling Scientific and Technological Uncertainties

As Macro Global's R&D team began construction of the Single Customer View reporting system, they met a slew of scientific and technological uncertainties that jeopardised the project's success. Addressing these concerns through new solutions was critical to the system's operation, security, and overall efficacy. The following are important areas where the team concentrated their efforts in solving the aforementioned issues.

Robust Key Management Practices

The R&D team acknowledged the importance of secure key management in hybrid encryption using AES for symmetric encryption and RSA for asymmetric encryption. AES offers excellent security and speed for encrypting consumer data during transmission, whilst RSA enables safe key distribution and authentication.

This combination assures that sensitive customer information such as customer ID, account number, aggregate balance, and other personally identifiable information, is fully protected, solving important security and performance concerns in the financial industry.

They implemented strict access controls, allowing only designated personnel to interact with the key management system.

To further mitigate risks, the team adopted periodic key rotation protocols, ensuring that even if a key was compromised, the potential damage would be limited.

Rigorous Testing and Refactoring for Compatibility

As the development of the SCV reporting system progressed, integrating modern frameworks and libraries such as Bootstrap led to compatibility issues with existing code and third-party dependencies. The R&D team understood that a seamless user experience relied on maintaining functionality across all components.

A meticulous and structured testing and refactoring process was adopted. Each component of the system underwent rigorous compatibility testing, which allowed the team to identify issues before they could escalate.

They employed an incremental upgrade strategy, carefully replacing outdated libraries with modern alternatives while ensuring that existing functionalities remained intact. This approach emphasised consistency and robustness in the system architecture.

Custom Data Sanitisation Routines

The challenge of ensuring comprehensive data sanitisation, while simultaneously preserving the integrity of critical information, required a nuanced understanding of the data flow within the system. The R&D team explored how to balance these competing needs without incurring significant risks.

The team has developed an AI-Powered Data Validation approach to address data sanitisation challenges within the Single Customer View reporting framework. This approach uses advanced artificial intelligence algorithms to enhance data accuracy and reliability by identifying and correcting errors, inconsistencies, and duplicates.

The system uses machine learning models to classify data entries according to established rules and patterns, ensuring high data quality across multiple entry fields.

Real-time error detection minimise the risk of flawed data being incorporated into the SCV.

Inconsistencies are identified and corrected, with the system alerting users to inconsistencies and suggesting corrections based on learned patterns from historical data.

Fuzzy matching algorithms are used to detect duplicate records effectively, ensuring data integrity.

Clustering techniques are integrated to group similar data entries, identifying duplicates and streamlining the deduplication process, enhancing efficiency and accuracy while maintaining a clean and reliable database.

Dynamic Rate Limiting Algorithms

The need to protect the system against email flooding attacks led the R&D team to investigate rate-limiting solutions that would not impede legitimate user interactions. They recognised that effective rate limiting required a balance between security and usability.

The team developed dynamic rate-limiting algorithms that adjusted thresholds based on real-time user behavior and traffic patterns. By employing machine learning principles, the algorithms could identify anomalies in traffic and adapt accordingly.

This methodology enabled the system to respond proactively to potential attacks while maintaining a fluid and responsive user experience, demonstrating the team's commitment to security without sacrificing usability.

Comprehensive Configuration of Content Security Policy

Recognising the critical role of CSP in mitigating content injection threats, the team delved into the complexities of configuring this security measure. They faced the challenge of ensuring CSP compatibility across diverse browsers and environments.

The R&D team embarked on extensive testing of CSP configurations across various browsers to refine settings meticulously. They utilised tools to simulate different browser behaviors and evaluated how CSP rules reacted under various circumstances.

This exploratory testing process enabled the team to create a solid and adaptable CSP, thereby significantly reducing vulnerabilities while ensuring consistent functionality across platforms.

Meticulous Input Validation for HTML Injection and XSS Protection

Understanding the risks posed by HTML injection and XSS attacks required a comprehensive review of the existing codebase, particularly focusing on input fields that were susceptible to user tampering.

The team employed a dual approach that combined rigorous input validation techniques with substantial refactoring of legacy code. They meticulously analysed existing user input paths and enhanced these with validation checks designed specifically to thwart injection attempts.

This proactive enhancement not only fortified the system against vulnerabilities but also set a new standard for input validation that would be integrated into future development efforts.

Seamless Integration of Microsoft Single Sign-On

The R&D team understood that the success of this integration hinged on effective token management and session handling.

The team redesigned the authentication flow to accommodate SSO requirements, focusing on secure handling of authentication tokens and streamlined session management.

User journeys were mapped out to ensure that from the moment of authentication to accessing the SCV reporting system, users would encounter minimal friction while still benefiting from enhanced security measures.

Technological Breakthroughs and Solution Development

Hybrid Encryption

A hybrid encryption system has been developed by the R&D team to improve data security by combining asymmetric encryption (RSA) with symmetric encryption (AES).

AES: Effective at encrypting huge volumes of data quickly. It uses the same key for encryption and decryption, making it ideal for data storage and bulk encryption processes.

RSA: Employs a pair of keys, such as a public key for encryption and a private key to decrypt, to securely exchange encryption keys, rather than directly encrypting big datasets.

Integration: The AES algorithm encrypts sensitive data during transmission, and the RSA algorithm subsequently encrypts the associated encryption key. Therefore, even if a hacker intercepts the encrypted data, they are unable to access it without the decryption key.

Content Security Policy

The team used CSP to protect web apps from XSS attacks and data injection.

CSP is a security feature that controls how and where resources can be loaded in a web application. By setting a whitelist of content sources (e.g., scripts, styles), the danger of loading harmful content is reduced.

Configuration: HTTP responses include a CSP header that specifies permitted sources.

Effectiveness: By enforcing such criteria, even if an attacker discovers a means to inject code into the web application, the browser will only execute scripts from trusted sources.

Microservice Architecture

The usage of a microservices architecture allows the FSCS SCV reporting system to be scalable and maintainable.

A microservices architecture divides a large application into smaller, independently deployable services that execute specialised functions. Microservices can be designed, implemented, and scaled separately.

In the SCV reporting system, real-time data processing provides rapid insights for operational decision-making. For example, as consumer transactions occur, they can be analysed to identify trends, anomalies, or patterns that might inform business strategies.

Automatic Reporting Processes

The team developed automated reporting technologies to make report generation and delivery more efficient.

Data Aggregation: Data from multiple sources is gathered, converted to assure consistency, and then combined for reporting using ETL (Extract, Transform, Load) procedures.

Scheduled Tasks: Automation tasks can be scheduled to be executed at predetermined intervals, guaranteeing that reporting is current without the need for manual intervention.

Notifications: Integrating alerting systems enables stakeholders to receive automatic notifications when reports are ready or abnormalities are spotted, hence improving responsiveness.

User-Centric Design Enhancements

Improved design principles were used to increase user experience and accessibility.

Personalised Dashboards: The system architecture offers user-specific setups, allowing users to customise their dashboards with metrics, graphs, and reports that are relevant to them.

The successful development of the SCV reporting system yielded substantial improvements in efficiency, accuracy, and security. Below is the key performance indicators used to measure the project's success:

Impact of Technological Advancements

Efficiency Enhancements

- **Data Processing Speed:**
  The time to generate SCV reports decreased by approximately 30%, reducing average report generation time from 30 minutes to 21 minutes.

- **Error Rate in Data:**
  The error rate in reporting data was almost nullified, due to advanced data validation mechanisms.

Accuracy Gains

- The implementation of AI-powered data validation mechanisms led to a significant decrease in data duplication, which improved data integrity and consistency in reports. Accuracy in customer data processing saw a big jump.

Security Improvements

- **Security Incident Rate:**
  Post-implementation, the frequency of security incidents fell significantly, highlighting the effectiveness of the rigorous input validation, encryption protocols, and CSP configurations.

- The system achieved full compliance with relevant data protection regulations, reducing vulnerability to potential fines and sanctions.

Potential Cost Savings

- **Operational Cost Reduction:**
  The automation of reporting processes resulted in saving labor costs associated with manual data entry and reporting tasks.

- **Reduced Costs of Errors:**
  A decrease in error rates has led to significant savings. With the previous error rate, the company incurred costs associated with data correction and reprocessing, which have now been minimised.

- **Infrastructure Costs:**
  Optimised system performance allowed for better server utilisation, leading to considerable savings on infrastructure costs related to server maintenance and hosting services.

Risk Reduction

- Enhanced security through robust encryption, meticulous input validation, and a properly configured CSP substantially reduced data breach risks, decreasing the likelihood of financial losses associated with breaches, which can range from millions to tens of millions of dollars, depending on the severity of the incident.

Conclusion

The development of the FSCS SCV reporting system by MG's R&D team marked a significant advancement in the automation and security of data processing within financial institutions. The implementation of an AI-driven FSCS SCV reporting system has remarkably transformed traditional reporting processes by enhancing data integrity, security, and operational efficiency.

The integration of advanced technologies has addressed key challenges such as complex data management, security compliance, and the need for efficiency gains, positioning organisations to thrive in a competitive and regulated environment.

Looking ahead, there are promising avenues for further research and development, including the incorporation of advanced analytics, blockchain technology for data integrity, real-time processing capabilities, and tailored reporting solutions.

By continuously adapting to emerging technologies and security threats, the SCV reporting framework can ensure sustained compliance, security, and efficiency, empowering organisations to navigate the complexities of the modern data landscape effectively.

We are here to help you

macro global®
creating value through innovation

Please click on the web link below to access our sales desk telephone numbers and email and we will be in touch straight back to you.

https://www.macroglobal.co.uk/contact-us/

Microsoft Gold Partner

amazon web services | Partner Network
TECHNOLOGY PARTNER

ISO 9001:2015 Quality Management System Cert. #: 0922900102

ISO 27001:2013 Information Security Management Cert. #: 09222700102

ISO 27701:2019 Privacy Information Management Cert. #: 09222770102

ISO 27018:2019 PII Protection in Public Clouds Cert. #: 09222701802

Macro Global (MG) is the trading name of Macro Infotech Limited, Inca Infotech Ltd & Macro Technology Solutions Pvt Ltd. Macro Infotech Limited & Inca Infotech Limited have Registered Office at 25, Cabot Square, Canary Wharf, London – E14 4QZ and these companies are registered in England & Wales under the registration number 06477763 & 04017901.