WSO2 Reimplementation

Product Requirements Document

May 14,2024

Document Version Control	**1.0.0**
Document Title	Reimplementation of WSO2
Published Date	May 14,2024
Document Classification	Internal
Next Review Date	
Document Location Primary	Project Management Office/Share Folder
Owner(s)	Esther Martey
Reviewer(s)	Matthew Kafui Kartey
Document Type	Project

Table of Contents

1 INTRODUCTION

1.1 Purpose

The bank requires an enterprise middleware to provide an open-source software tool to construct enterprise systems that allow businesses the freedom to set up services and apps in hybrid environments, on-premises, or on private or public clouds, and to move between them with ease as necessary. Additionally, this will ensure a standardized standardised feature and functionality are provided. Moreover, to mitigate the risk associated with managing the current legacy systems.

2 OVERVIEW

2.1 Business Problem Statement

The current WSO2(3.2, 7.1) deployed in the 2021 was only able to migrate the ATM services. However, due to lack of experts to manage the current WSO2. It is imperative to have skilled personnel and reimplement WSO2 with the upgraded version 4.3.0 to ensure the bank factors other Application Programming Interface (API) in the legacy system.

2.2 The Business Goals and Benefits

The reimplementation of the WSO2(4.3.0) is to ensure that all APIs in the bank's ecosystem are routed through the middleware and ensure rregular security upgrades and proactive patching. The bank seeks to ensure configuration-driven design allows for early/frequent deployment, smooth change management, and agile incremental solution development.

2.3 Key Success Indicators

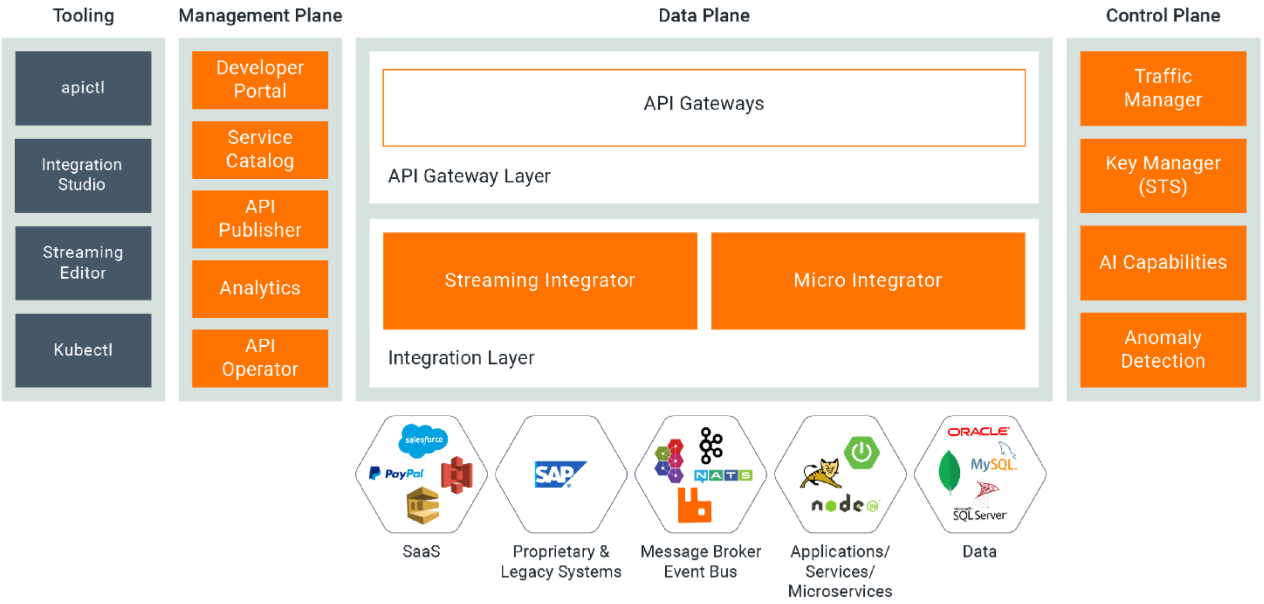
- Documented architecture of all the APIs and Webservices of the bank based on SOA and BIAN principles and Framework.
- Successful implementation of API Manager (4.3) to ensure high availability and Disaster Recover Implementation.

- Implementation of Micro Integrator to ensure service integration using an intuitive low-code graphical design interface and enable greater flexibility, deployment options include both ESB style and microservices.

- The deployment of all the redesigned APIs and webservices on the WSO2 platform that has been implemented.

3 KEY FEATURES OF WSO2

3.1 API Manager



3.2 Micro Integrator

The Micro Integrator uses an intuitive low-code graphical design interface to simplify integration between apps, services, data, and the cloud. For greater flexibility, deployment options include both ESB style and microservices.

3.3 Technical Requirement

Technical Requirements for WSO2	
S. No	**Features**
1	System should support English language
2	Integrate with existing DBMS & Hardware
3	Data backup and archiving
4	Test environment
5	Audit trails and logging features available in Web Server, application server and database server.
6	Audit and log activity through all the application tiers

4 DESCRIPTION OF KEY REQUIREMENTS (TOOLS):

4.1 API Manager

#	Core Functional Requirements
4.1.1	Develop, Deploy and Manager APIs/API Products: The API publisher will enable users follow the specification of each API while providing guidance on the construction and publishing of APIs.
4.1.2	Discoverable APIs- Ability to create categories or use tags to categorize APIS.

4.1.3	Secure APIs- Ensure there is API payload validation, adherence to clear protocols, rate limiting restrictions, and API verification against specifications, in addition to API authentication and permission, can help to completely secure the bank's APIs.
4.1.4	Developer -Friendly APIs: -Ensure developers can build application using aa well-documented and easy -to -use API system.
4.1.5	Rate Limiting: Balances the load to avoid system outages.
4.1.6	Dashboards: Provides dashboards which gives insights on the bank's APIs.
4.1.7	Integrate microservices: Hosts composite microservices that can harness the power of a low-code integration approach, while reaping the benefits of microservices architectures.
4.1.8	Integrate systems in the bank: Message routing, transformation, message mediation, service orchestration, as well as service and API hosting needs will be evident.
4.1.9	Real-time data: A stream flow designer and a stream processing engine with robust analytics and monitoring capabilities. This must apply to all APIs in the bank.
4.1.10	Security Information and Event Management (SIEM) integration: All the systems logof WSO2 must be integrated with the bank's SIEM.
4.1.11	Observability: The implementation should ensure access to dashboards and report to monitor both transactional and system logs. Data is made available for further insights.

4.2 Micro Integrator

#	Core Functional Requirements
4.2.1	Routing and Transformation: Routes the ideas of mediators and endpoints and facilitates use cases as the intermediary system bridging the communication gap among the systems.
4.2.2	Service Orchestration: A single coarse-grained service encapsulating the various fine-grained services activated in the process flow will be the only one the service client can access.

4.2.3	Asynchronous Message Processing: Queue messages in the system without an immediate response required and solves the problem of intermittent connectivity.
4.2.4	Software as a Service (SaaS) and Business-to- Business (B2B) Integration: Ensures interaction with SaaS applications on the cloud, databases, and popular B2B protocols.
4.2.5	Data Integration: The Micro Integrator's built-in data services capability allows for the decoupling of data from the data source layer and their exposure as data services.
4.2.6	Protocol Switching: Enables straightforward message routing to complex systems utilizing integrated solutions, provided by the Micro Integrator.
4.2.7	File Processing: Capacity to extract relevant information from local file system or a remote location which can be accessed over protocols such as FTP, FTPS, SFTP, SMB.
4.2.8	Periodic execution of integration processes: Automation of a message medication process to run periodic tasks.
4.2.9	Security Information and Event Management (SIEM) integration: All the systems log of WSO2 must be integrated with the bank's SIEM.

4.3 SYSTEM SECURITY

The WSO2 Tool will protect the business from Data breaches, provides sufficient backup processes, and meets rising performance demands as the need changes. Users are configured in the solution to have different access levels to the application.

The Solution will also support third party security software (e.g., Web Application Firewall) and hardware that meets industry standards. With its open web -based technology, existing and new security technology can be utilized as it becomes available therefore making the security aspect independent of the underlying operating system hence the security is greatly improved.

The solution will have below security features:

- Security must be implemented on each layer/module of the system.
- All components of the solution must be aligned with the bank's information security policies.
- System does Role-Based UI Display since the front-end module is to be used by various user categories e.g. Users, Supervisors, Auditors and Administrators. Specific menus must be generated and presented to users based on the user's role.
- Ability to restrict user access to defined roles.
- Audit Trail
- Maintain event log of all activities with read only permission.
- Provide comprehensive audit trail features of activities undertaken in the system.

- Application Security: All aspects of the system must conform to the highest standards of security to avoid security vulnerabilities e.g., OWASP Top-10 application security checklist.

4.4 USER MANAGEMENT

A user management system for user data storage and authentication will be included in the WSO2.

- ✓ User authentication
- ✓ registration process,
- ✓ Application password
- ✓ Management of all user account operations (including modifying user properties, resetting passwords, enabling, or disabling users, granting rights, and more).
- ✓ Application of the Bank's LDAP to authenticate the users.
- ✓ External user management will be authenticated with a locally generated user.

➢ **Password Complexity**

- The Password complexity should contain at least one letter, one number and one special character.
- Minimum password length should be Eight (8) characters.
- Maximum password length should be thirty (30) characters.

5. NON-FUNCTIONAL REQUIREMENTS

5.1 Performance

The application should be of high performance.

5.2 Exception Handling

There should be a fallback option in the event the portal is inaccessible. Reports can be generated from the backend and shared with stakeholders.

5.3 Usability

The system should be available to authorized users. The user interface should be friendly and interactive.

5.4 System Availability

The system should be available 24/7.

5.5 Contingency and Disaster Recovery

The solution shall be delivered with Disaster Recovery Setup (DR) in place.

5.6 Help and Training

There will be training at various levels to aid the teams to support the solution effectively and efficiently.

5.7 Information Security Requirements

5.7.1 General Information Security

A full audit trail will be available in the system to capture the history of transactions, what items were changed and by whom and when (timestamp). User profiles ensure that only functions assigned to those users (or group of users) are available when that user logs in.

Below is a list of some security requirements that will be considered and employed if possible, in the development of the system.

- Use HTTPS and only HTTPS to protect your users from network attacks.
- Serve cookies with the 'Secure' attribute to protect your user from network attacks.
- Generate HTML safely to avoid XSS vulnerabilities.
- Use JavaScript safely to avoid XSS vulnerabilities.
- Serve API responses with a proper Content-Disposition header to avoid reflected download vulnerabilities.
- Avoid XML vulnerabilities by configuring your parsers properly.
- Use Web Application Firewall

5.8 Authorization and Access Control

Following shall be some of the users of the Solution and will therefore have accesses that are related to their job roles.

- Business Solution Unit
- Testing unit
- Applications Support
- Middleware and Switch team
- CBA team
- Information Security
- Internal Control
- Audit

5.9 Audit Logging and Alerts

Below shall be the minimum audit fields to be contained in audit logs.

- User Activities
- Date and time stamp for all user induced requests.
- User IP address
- Any other details not stated that can be logged.

5.10 Security Administration

Per the information security governance policy of Consolidated Bank Ghana Ltd.

5.11 Regulatory, Audit and Data Retention Requirements

Audit and data retention requirements in line with Consolidated Bank Ghana Ltd policy to be discussed and agreed. An update mechanism to take care of changes in rules/regulations/documents/procedures which need to be reflected our procedures and processes.

6 DOCUMENT APPROVAL

Approval of this document represents approval to proceed with development.

The following represent the minimum approvals required to proceed; Additional approvers may be added if determined to be necessary by the Project Manager or Owner.

Name	Designation	Signature	Date Approved
Alex Opoku	Snr. Manager IT Business Solutions		30th May 2024
Andy Quarcoopome	Senior Manager, Information Security Services		31/05/2024
Jameel Nettey	Manager, IT Control		31/05/2024
Paul Nartey			
Jeremiah Kwei Osekre			
Bill Kyeremeh			
George Mensah			