CANADIAN WESTERN BANK

CWB Architecture

CWB Digital Customer Onboarding
Technical Solution Design

TITLE:	CWB Digital Customer Onboarding
REVISION:	0.1
REVISION STATUS:	Pending review and approval
DATE OF ISSUE:	05/01/2020
DATE OF NEXT REVISION	
OWNER:	Architecture and Service Delivery
CUSTODIAN:	AMS Manager
ORGANIZATION:	Application Development
INFORMATION CLASSIFICATION	Internal
RISK CLASSIFICATION:	Medium
RETENTION PERIOD:	RETAIN FOR ONGOING USE
MASTER STORAGE LOCATION:	SharePoint Project folder.

REVISION RECORD

Table 1 Revision Record

Revision	Reviewed by	Endorsed by	Approved By	Date

DOCUMENT CHANGE CONTROL

Table 2 Document Control Change

Revision	Author	Date of Issue	Brief Description
Draft	Reinhardt Tonn	Feb 18, 2020	Document creation
Draft	Reinhardt Tonn	May 12, 2020	Distribution of document to Joggi Nijjar
Draft	Reinhardt Tonn	April 13, 2021	Added Okta Authentication and Single Sign-On
Draft	Fujian He	Nov 17, 2022	Updated the sections below to align with our current status. • 2.1 Current State (included 2.1.1 business flow) • 2.2 Target State • 2.3 Context Diagram • 2.5 Solution Components • 2.6.1 Product Catalogue • 2.6.2 National Occupational Classfication Code Search

DISTRIBUTION LIST

This document has been distributed to:

Table 3 Distribution List

Name	Role
Jose Barril	Solution Architect
Darren Bryks	Senior Manager, Infrastructure Delivery
Mark Doubinin	Manager, Application Development
Vikram Singh	Senior Security Analyst
Roney Simon-Mathews	Security Analyst
Jogi Nijjar	Digital Program Manager

TABLE OF CONTENTS

1. Document Summary

1.1. Purpose

The purpose of this document is to outline the technical solution design of the CWB Digital Customer Onboarding, powered by the Temenos Journey Platform. It includes the technology and infrastructure, system integration, and configuration options for implementation, maintenance, and support of the Digital Onboarding Environment.

1.2. Objectives

To configure and implement the Temenos Infinity Digital Onboarding solution to address the immediate digital onboarding requirements for new Motive customers. Subsequent enhancements of this document will address the immediate and long-term solution for the onboarding of personal, small business and commercial customers to Motive Financial and CWB.

1.3. Project Contacts

Table 4 Project Contacts

Roles	Name
Project Sponsor:	Christina Mullen Christina.Mullin@cwbank.com Jason Bond Jason.Bond@cwbank.com
Project Lead:	
Project Manager	Jogi Nijjar – Senior Project Manager Jogi.Nijjar@cwbank.com
Business Analyst(s):	Steve Kelcher – Business Analyst Steve.Kelcher@cwbank.com
Project Coordinator:	Genevieve Parrent Genevieve.Parrent@cwbank.com
Systems Integration Architect	Mark Doubinin Mark.Doubinin@cwbank.com
End user Services:	N/A
Security Advisor:	Roney Simon Mathews Roney.SimonMathews@cwbank.com
Infrastructure Manager:	Darren Bryks Darren.Bryks@cwbank.com
Infrastructure Analyst:	
Database Admin:	N/A
Solutions Architect(s):	Reinhardt Tonn Reinhardt.Tonn@cwbank.com
Application Manager	

1.4. Intended Audience

This document is to be used by the applications development and infrastructure operations team to assist in the creation of the release plan for the implementation of the applications, servers, storage and networking components.

1.5. Revision and Feedback

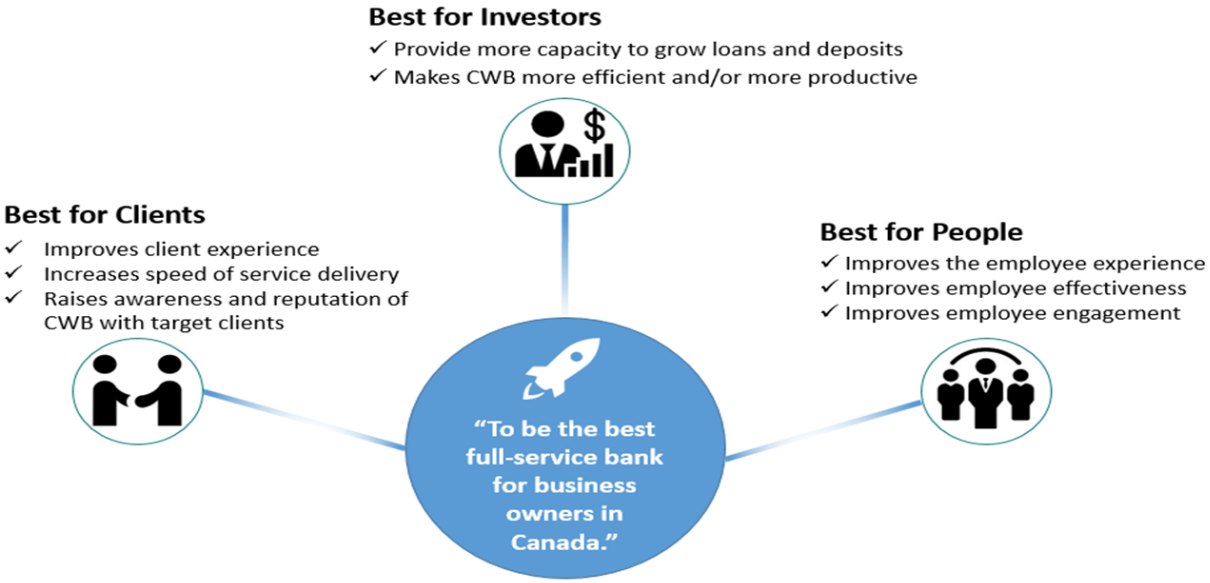
This is a living document and should be revised and updated periodically to reflect changes as they occur in the CWB IT infrastructure environment.

2. Business

The key goal of the Digital Program is to implement Digital Client Onboarding processes and be a disrupter in offering unique online banking products and services for Personal, Small Business, and Commercial clients for Motive Financial and and Canadian Western Bank customers.

The first key project phase is Motive and Personal Digital Client Onboarding (DCO), which includes new front-end web pages (using Temenos Infinity) for prospective personal clients to select a product, enter their personal data and submit a request for approval. New back-end capabilities utilizing specialized services from thirdstream (a fintech broker) and internal capabilities to CWB will be developed to facilitate identity validations, AML and fraud checks and customer/account creation processing without human intervention. Exception processing will be supported with some manual intervention using a sophisticated employee facing portal.

Key Objectives:



Best for Investors:

- Attracting new clients which will increase loans and deposits will benefit investors.
- Reducing manual efforts that are currently required to open new accounts will improve efficiency and productivity.

Best for Clients:

- The modern and distinct products/services that will be delivered by the Digital Program will improve client experience though improving the functionality of the online systems, and offering clients tools they don't have access to elsewhere.
- Digital Client Onboarding will offer personal and small business clients a much faster way to open a new account remotely, which will benefits prospective new clients who are outside of CWB's current geographic branch footprint.

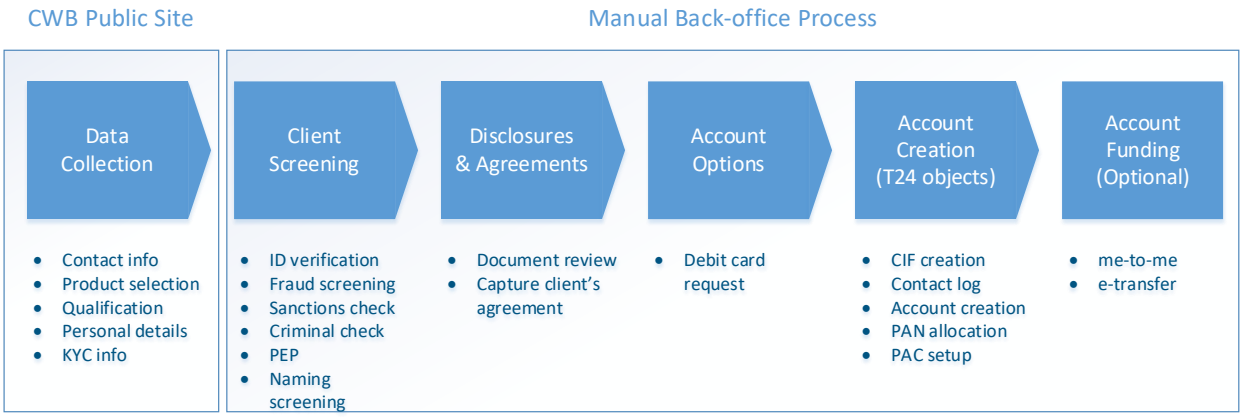
Best for People:

- Reducing manual efforts required by CWB staff will improve the employee experience and allow them to focus on more value-add activities.
- Staff are clients of the bank, and will benefit from the improved experience that will be delivered by the personal changes in the Digital Program, and in particular the enhancements to personal online banking.

2.1. Current State

The Personal DCO for new to bank customers, the In-Branch Personal (CWB) for new to bank customers, and the Motive DCO have already been released, and the Small Business DCO will be released in 2022 Q4.

2.1.1. Business Flow



2.2. Target State

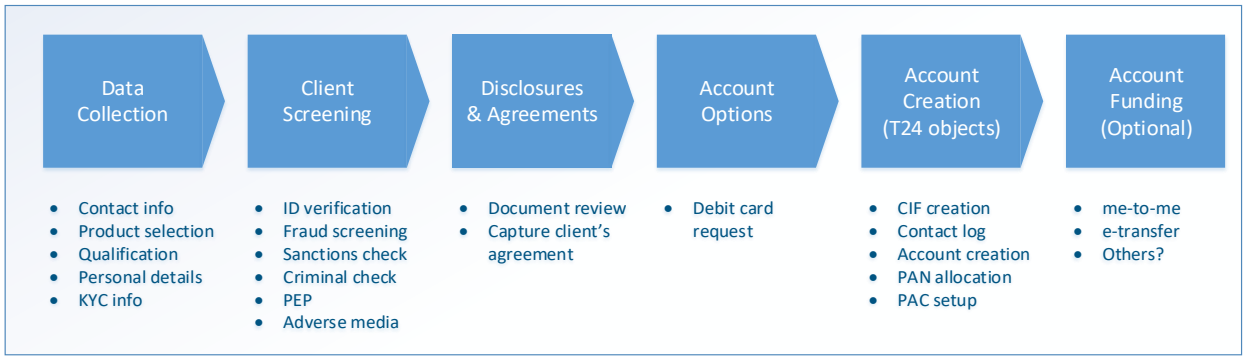
The target state solution will automate the product selection, product recommendations, data collection, client screening, disclosures and agreements, account options, client and account provisioning and account funding. Manual intervention by CWB employees will be limited to application scenarios that trigger compliance, fraud or other rules that require CWB oversite. CWB employees also need to handle exceptions when the API errors occur. Third parties with sophisticated capabilities in fraud prevention, compliance, identity verification will be fully integrated into the onboarding workflow, providing an exceptional experience and a high opportunity for straight through processing and near real-time access to newly provisioned accounts in online banking.

Onboarding will not only include new capabilities for Motive, but also CWB personal, small business and commercial lines of business. Once new Digital Banking channels are developed on the Temenos Infinity Platform, new account creation will also be supported by the digital onboarding process that utilize customer information and account holdings to optimize the new account creation experience.

Onboarding will be developed as a reusable service that can be leveraged end-to-end in both new customer and existing customer scenarios.

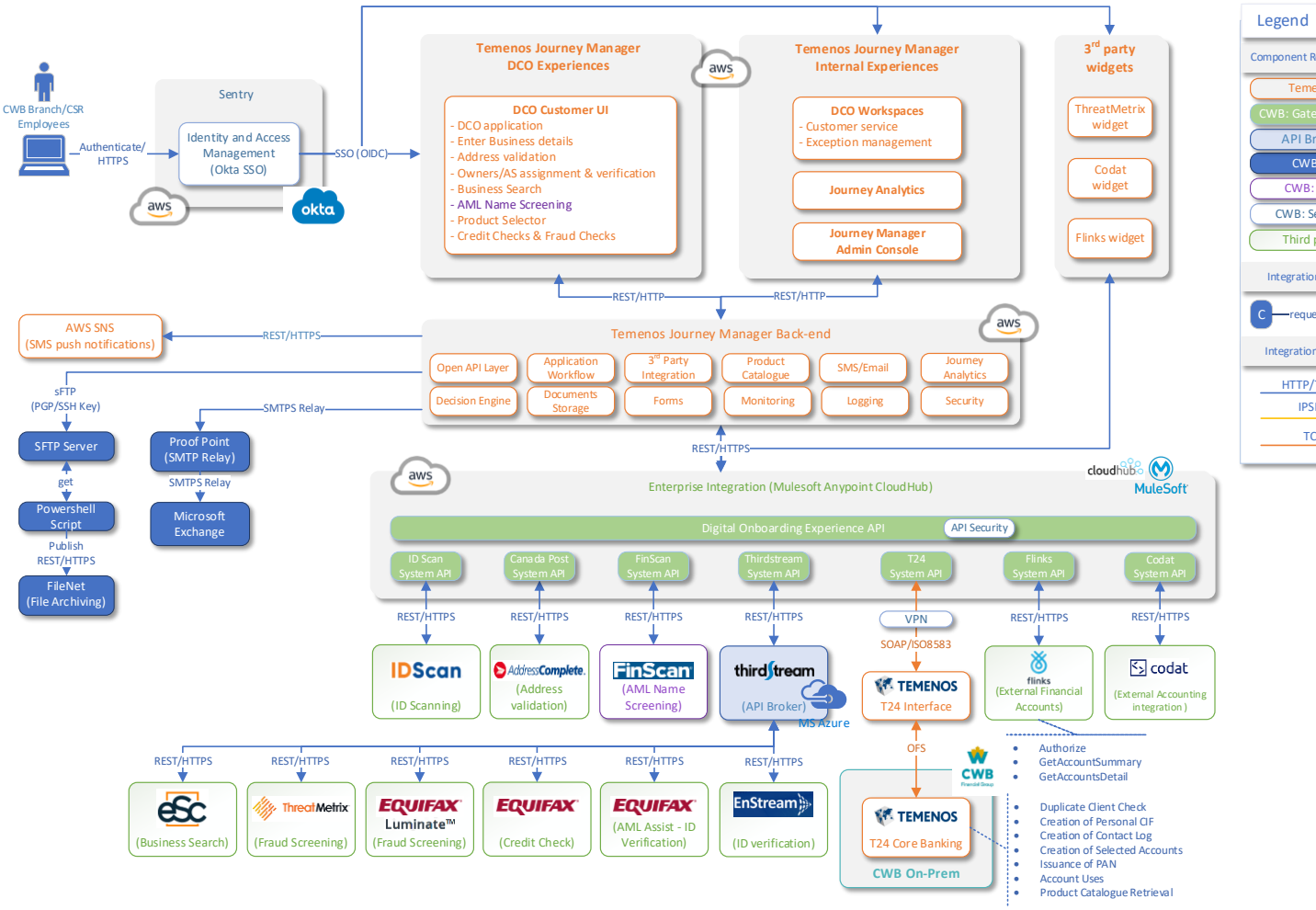
2.2.1. Business Flow

Automated Process – Manual intervention for Exceptions Only



Solution Architecture

2.3. Context Diagram



2.4. Architectural Decisions

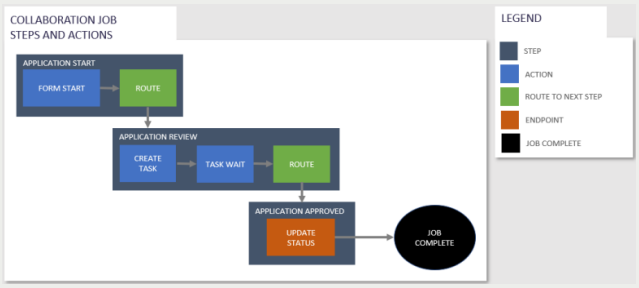
Name	Status	Responsible Party	Purpose	Location
T24 Integration	Approved	Reinhardt Tonn	To formalize the integration approach between Mule and T24.	Sharepoint
Mulesoft Deployment	Approved	Mark Doubinin	To formalize the production deployment model for the Mule runtime.	Sharepoint
Secure Handling of Credentials	Approved	Reinhardt Tonn	To determine special handling of credentials to ensure they are not exposed in transit from Avoka to T24.	Sharepoint
Production Hosting	Approved	Reinhardt Tonn	To recommend the production hosting alternative (and additional guidelines) acceptable to CWB Architecture and Security teams	Sharepoint

2.5. Solution Components

Component	Status	Responsibilities
Customer Onboarding Experience	New	Customer facing onboarding experience. This is comprised of several notable components: ***Product Selector*** This component is responsible for both guided and self-guided multi-product selection. The product(s) selected in this component are passed to the Customer Onboarding component. ***Customer Onboarding*** This component is responsible for customer data collection, identity validation, fraud prevention, compliance, account application and funding. ***Flinks Connect Widget*** Flinks Connect is a 3rd party widget embedded into the Customer Onboarding flow that assists all customers in connecting their bank accounts in a secure and intuitive way. All the complicated bank multi-factor authentication, edge cases and errors are handled — all while keeping credentials from ever hitting your server. ***Threatmetrix Javascript*** This javascript library is provided by Threatmetrix and embedded into the Customer Onboarding flow to collect detailed device information and transmit this directly from browser to Threatmetrix servers.
Internal Experiences	New	**Customer Onboarding In-Branch** CWB staff use the in-branch version as a "shortcut" to onboard new clients in a branch/banking center. **Customer Support Portal (Workspaces)** Employee support portal (otherwise called Workspacers) for digital onboarding. **Insights** An analytics platform integrated with the Journey Manager platform. **Admin Console**

		Console dedicated to configuration of the Journey Manager platform.
Legacy Customer Channels	Enhanced	**Public Website** The public site is the launch point for the customer onboarding experience. Changes will be required to this website to integrate effectively with the Onboarding solution.
3rd Party Experiences	New	**Flinks** Connects users' bank accounts by allowing the customer to authenticate with their non-CWB banking credentials. This experience is driven directly by Flinks and integrated with the Digital Onboarding Experience as a self-contained widget. This is used as part of the funding process where the applicant makes initial deposits into the newly opened accounts by way of an inter-bank transfer. **Codat** CODAT is a cloud-based SaaS offering that provides seamless integration capabilities with all the major accounting platforms. It acts as a data processor when building integrations, mapping data in a standard format independent from the accounting software that CWB customers use.
Temenos Journey Platform	New	The platform on which the Digital Onboarding applications are built. Springboard is the reference implementation utilized by Temenos to build the CWB solution. Journey Manager comes with services providing specific business-related functionality such as: • Data prefill for existing customers • Address look-up and validation • Identity verification, KYC, OFAC • Deposit and credit decisions • Save and resume • Follow-up leads. • User consent capture • Channel cross-over • Core system integration • Cross-sell next product  **The platform is generally composed of the following:** **Open API Layer** Journey Manager exposes APIs to the Digital Onboarding UX. This Single-Page Application calls server-side APIs to invoke Journey Manager functionality. **Application Workflow** A series of tasks that Journey Manager creates for the users to complete, review or reject. It consists of several steps each containing actions or endpoints. An applicant fills and submits a form which starts a collaboration job. The job processing completes this action and immediately routes to the next step. The workflow ultimately culminates in in delivery of a data package by secure FTP, resulting in provisioned customer and accounts in T24. Any workflow requiring

review will be directed to a workflow that must be completed by internal CWB/Motive staff.



Product Catalogue
The Journey Manager will initially be configured with a small product catalogue representing the products that can be selected during onboarding. This product catalogue will be the central product catalogue for all digital services. The products are configured in an XML file stored on the Journey Manager server.

SMS
The Journey Manager Platform has a direct integration with AWS and will leverage this for Multi-Factor Authentication when a prospective customer resumes a saved application.

Email
The Journey Manager Platform utilizes emails to communicate with *applicants*.

Journey Analytics
Journey Manager collects a broad range of data related to user's interactions with forms, such as form submissions, and visualizes it with via the following charts.

- Transactions trends
- Forms activity
- Referer submissions
- Form submissions
- Device types submissions
- Reader Versions

Decision Engine
Journey Manager analyzes responses from 3rd party integrations and the data collected and applies decision on logic on whether an application can proceed through to auto-provisioning, or if human interaction is required to move the workflow forward to a final state.

Data / Documents Delivery
Manager comes with highly customizable data retention management capability to suit CWB's data requirements. This is instrumental in achieving the following:

- Control the growth of database tables.
- Maintain high system performance.
- Purge transaction form data which contains form users' Personally Identifiable Information.

Manager collects important information in relation to data retention management, which includes the status of any individual transaction to keep track of PII data that has been purged or is due for purging.

Forms
A Maestro form is a document designed to capture and presentment data. A form is built by a Form Builder, based on a template, and contains components that implement the form's design. A Maestro

		form may be created for individual purposes, or semantic versioning may be used to extend the life of individual form versions. **Monitoring** Temenos is responsible for application monitoring and assurance that the application is performing as expected. **Logging** Manager captures a wide range of system and service run-time information and stores it in different log files. It provides a convenient interface for viewing this information, making it easier to troubleshoot diverse production problems. Manager maintains the following logs, which reside both on the file system and in the database: • Event Log • Error Log • Error Log Trend • Database Version Log • Import Log • Audit Log **Security** CWB will leverage the security capabilities of Journey Manager to enforce 2 Factor Authentication, Roles and Permissions based authorization model, and multi-tenant organization support to control access across Motive and CWB. Provides data security architecture to protect customer transaction data in transit and at rest.
Enterprise Integration (Mulesoft)	New	Integration platform for APIs. Utilized to build out 3 layers of APIs: **Experience APIs** Innovation and ease of integration with consuming applications **Process APIs** Agility and new value creation **System APIs** Unlock assets and decentralize access. System APIs developed during this project phase will include T24, thirdstream and Flinks.
External Providers	New	**Fraud Prevention** ***ThreatMetrix*** Provides device-level fraud prevention. ThreatMetrix ® is an enterprise solution for digital identity intelligence and authentication powered by insight from billions of transactions, embedded machine learning, and a powerful decision platform. ***Equifax Citadel Fraud*** Provides shared, multi-sector fraud data and advanced analytics, Equifax Citadel keeps abreast of changing fraud trends. **FinScan** Screening the new customers and companies against sanctions and watch lists. **Identity Verification** ***Enstream Mobile Verification Service*** Improves online account opening using verified customer information from trusted sources, reducing identity theft and account takeover fraud. ***Canada Post DPOI***

		Improves online account opening using verified customer information from trusted sources, reducing identity theft and account takeover fraud. **Credit Checks** ***Equifax Credit Check*** Providing credit bureau and information reports for businesses, including the financial sector. General credit scoring, fraud avoidance are the key features deployed. **Compliance** **Equifax AMLAssist** Designed to align with FINTRAC's intent and expecations, empowers CWB to: meet compliance requirements for identity verification, identify risks, reliable sources for identity verification, unique ID to assist with record-keeping for audit purposes. **Account Aggregation, Income Verification & Account Funding** ***Flinks*** Connects users' bank accounts by allowing the customer to authenticate with their non-CWB banking credentials. Provides customer and account details that can be utilized to validate the information provided by a potential customer during onboarding and provide validated account information in support of electronic funds transfers. **Codat** CODAT is a cloud-based SaaS offering that provides seamless integration capabilities with all the major accounting platforms. It acts as a data processor when building integrations, mapping data in a standard format independent from the accounting software that CWB customers use. **Utilities** ***ID Scan*** Reads AAMVA barcode from Canadian Driver's Licence. ***Canada Post Address Verification*** Enables intelligent and rapid searching across Canadian address dataset. **Google reCAPTCHA** Google reCAPTCHA protects DCO websites from fraud and abuse. It is a turing test to tell human and bots apart. It is easy for humans to solve, but hard for "bots" and other malicious software to figure out.
Internal Providers	Enhance Enhance	**T24 Transact Core Banking** T24 Transact is CWB's core banking system, supporting both Motive and CWB customers and accounts. This application is the system of record for all customers, accounts and funding. T24 will be enhanced to support SOAP services to facilitate onboarding, funding, product catalogue, etc. **Proof Point** CWB's Proof Point instance serves as an external facing secure SMTPs relay. Emails generated by Journey Manager, are routed through Proof Point to the internal email capabilities of CWB.

	Enhanced New New (Future)	**Centralized Logging (Elastic Search Stack: Elastic, Logstash, Kibana)** CWB centralized logging and SIEM platform **Filenet** CWB Document Storage. All application data received from JM in the form of a secure PGP encrypted .zip file is stored here. **SAS AML** Real-time screening service against watchlists issued by various authorities and internal lists. Onboarding watchlists are focused on fraud, terrorism, and sanctions. **Identity and Access Management (IAM)** A new employee and customer facing Identity and Access Management solution. Currently out of scope of the onboarding solution, but when operationalized, employee access will be migrated to this component and new customer identities will be created in this component.

2.6. Solution Details and Key Decisions

2.6.1. Product Catalogue

The *Product Catalogue* is an xml config file which is stored in the Journey Manager server. It hosts all of the details necessary to identify product categories, accurately present product, identify complimentary products, identify mutually exclusive products, identify product instance limits, identify product bundles, identify discontinued products and support non-financial products. The Journey Manager Platform read this XML file to obtain the product information and display a dynamic and user-friendly representation of the Product Catalogue to the user.

2.6.2. National Occupational Classification Code Search

National Occupational Classification Codes (NOCS) are required by T24 when creating a Customer (CIF) record. It is collected as part of the onboarding process and accurate information is required for various internal processes, including Anti-Money Laundering.

It is challenging to provide a good user experience for this large (40K+ records) hierarchical dataset, resulting in several UX options that present the data in ways that will allow users to identify their own personal NOCS code. The preferred CWB user experience is to allow for a type-ahead search capability on the NOCS job description. This predictive search would present a list of possible matches as the user types and allow the user to choose the best match. Specific requirements will be specified for the search capability, but at first blush the search should:

- Mandatory: respond in < 500 ms
- Mandatory: be case insensitive
- Mandatory: assume a wildcards at the beginning and end of the term(s) entered
- Mandatory: support changes to the list approximately every 5 years, with the first change to the list anticipated for 2021.
- Desirable: support fuzzy search capabilities that help find matching records despite improper spelling, equivalent terms, etc.

CWB provided Accutive a spreadsheet which already contain all the NOCS, so no integration to CWB systems will be required. The approved NOCS list is available through the Government of Canada NOCS Website, but CWB will consult on the job title description data quality, ensuring the list presented to the user is consistent, concise and appropriate for presentation in a search/drop-down list.

Note: although a common reusable API was proposed for this solution, it was determined that CWB did not have any known reuse scenarios and that the Journey Manager solution was in the best position to provide a positive user experience, keeping both data and search capabilities as close to the user as possible.

2.6.3. Password Strength Enforcement

Avoka Journey Manager and the Change Password API hosted by Mule will enforce password strength rules when capturing the password from the user and setting the online banking password associated with a user's PAN in T24. A regular expression will be designed that can be enforced in these platforms utilizing standard and proven regex libraries.

Password Rules:

Requirement	Business Rule/Logic
Password Length	8-30 Characters
Minimum Numeric	1
Minimum Upper Case	1
Minimum Lower Case	1
Minimum Special Characters	1
Valid Special Characters	!@#$%*

Regular Expression:

/^(?=.*[a-z])(?=.*[A-Z])(?=.*\d)(?=.*[!@#$%*])[A-Za-z\d!@#$%*]{8,30}$/g

2.6.4. SMS

AWS Simple Notification Service (SNS) will be utilized to send SMS messages from the customer onboarding application in support of Multi-factor Authentication when a customer resumes an onboarding application after saving and leaving an application mid-stream. This approach will be re-evaluated post-launch to determine what the enterprise SMS capability will be and how it will be best leveraged across CWB. In discussion is the potential to utilize a CWB Short Code, or a Toll Free Number for SMS.

When deciding between a short code and Toll-Free SMS, the important thing to keep in mind is that they rely on separate sets of infrastructure and spam filters. A responsible communications provider should have a series of checks and balances built into its contract process to ensure that the Toll-Free SMS channel remains spam-free. Though short codes both send and receive messages, the reality is that short code SMS is routed through a different infrastructure than Toll-Free SMS. Consequently, the deliverability of these two forms of communication can differ widely.

Short Code vs Toll-Free SMS

	Short Code	Toll-Free SMS
Type of messaging	One-way and Two-way communications	One-way and Two-way messaging
Throughput	High	Low-High
Digits	5-6 Digits	10 Digits
Customization	Vanity Short codes available	Brandable options
Cost	$$	$
Carrier Filtering	No	Yes
Provisioning time	8-12 weeks	Instant
Ideal Use-cases	High-volume, alerts, notifications, marketing, and reminders	Customer service, and chat applications
Voice Capable	No	Yes

2.6.5. Email

Avoka will send all email transmissions via the Microsoft Office 365. All communication will be secured via TLS (SMTPS).

2.6.6. Employee Authentiation / Authorization

Avoka will implement an SSO configuration for the Employee Facing User Experiences based on the SAML v2.0 SP-Initiated Protocol/FLow. CWB will utilize the established capabilities of the Identity and Access Management Team and adopt these capabilities once the newly acquired Okta capabilities are operationalized. Okta SAML 2.0 capabilities to will be leveraged to authenticate employees (inclusive of MFA) and populate the SAML Response according to the Journey Manager requirements.

Group membership will be configured in Azure AD as per the requirements of each application. Avoka Transact will provision users just-in-time when receiving a SAML Response from Azure AD.

The following basic application roles must be configured in Azure AD and provided in the SAML Response. This allows Avoka to confirm the user has been authenticated and also allows Avoka to restrict the user to the features/functions available to that role in the Avoka Workspace or Analytics applications. There are additional roles that are part of the Journey Manager Server that users may be mapped to if they are part of IT and or Support:

- Processing Staff
- Work Spaces Staff
- Helpdesk Staff
- Manager

Note: Okta was not operationalized at the time of writing of this solution. The IAM team has recommended the adoption of the native Journey Manager authentication and authorization capabilities. The IAM team is responsible for the

migration of this configuration to Okta as per the prioritizations set by the IAM program. It is anticipated this migration will be relatively straightforward given the adoption of a standards based protocol.

2.6.6.1. Vendor Azure Okta Configuration Reference

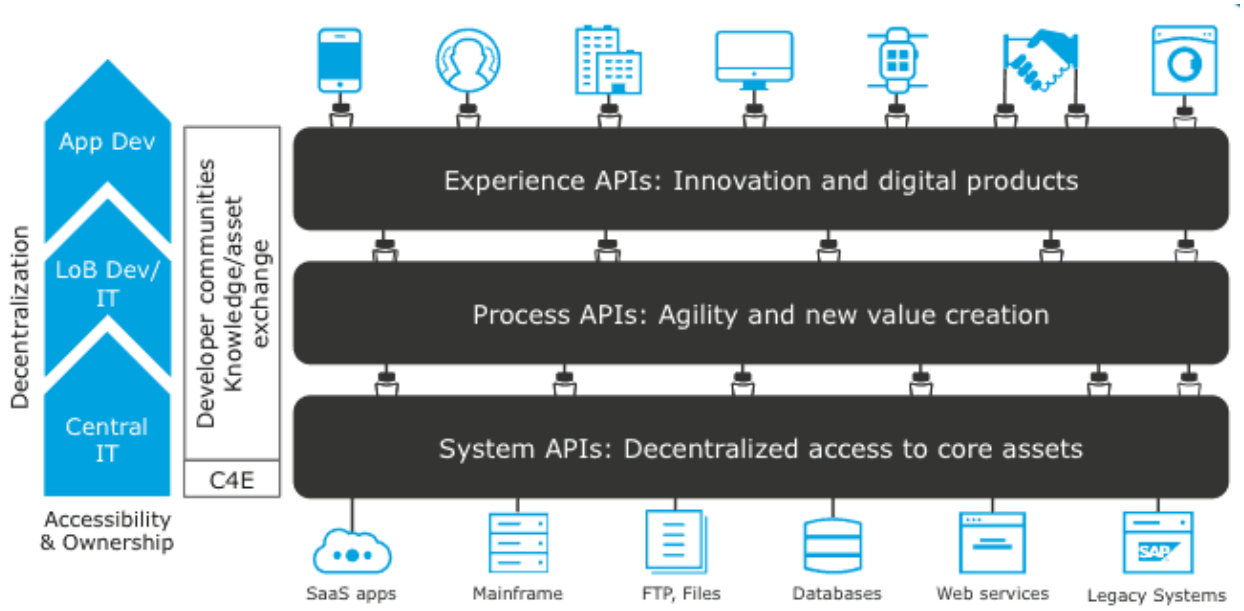
CWB_SSO Okta Example.docx

2.7. Integration Architecture

At the centre of the CWB integration architecture is the Mule API Gateway. CWB will follow a methodical way fo connecting data to applications, leading to reusable and purposeful APIs. The resulting 3 tiers of APIs will allow for reuse across the enterprise and a means of adapting APIs to the specific needs of a consuming application. This also avoids the common pitfalls of point-to-point integration.

The common pattern in the CWB Digital Program will be to build System APIs for all of the systems of record and Experience APIs for each consuming application. Process APIs will be developed where a more coarse grained API can be identified that is commonly reusable across the enterprise that also generally includes orchestration across multiple System APIs.

Although many third parties are involved in the onboarding project, some of this is hidden behind thirdstream, the fintech integration partner CWB has partnered with. Thirdstream has a number of existing partnerships and integrations available to support digital onboarding in the Canadian market.



The content in this section will primarily focus on non-standard integrations from CWB systems/applications to internal or external components. Fourth party integrations are excluded. For example, all partners beyond thirdstream are not shown here since CWB does not directly integrate with these parties, nor do we manage the partner relationship.

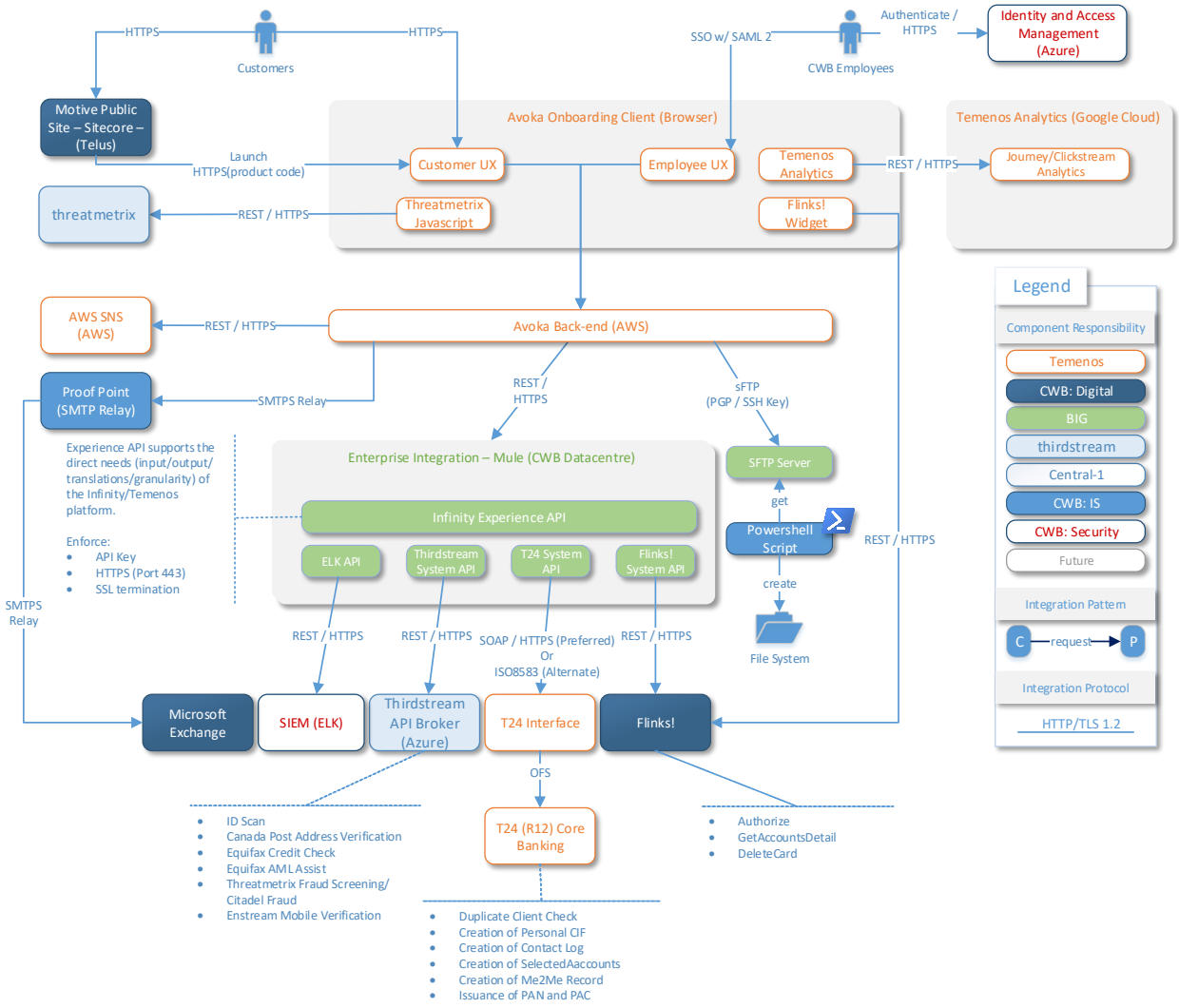
Several additional integrations are also included that are not initiated through Mule APIs. For example, Flinks is a fintech that supports the online banking login and retrieval of account information for many Canadian FIs. The integration with this partner is initiated through a UI widget, therefore, the integration is direct from browser to Flinks. Additional information is collected from Flinks subsequent to a validated authentication.

The Threatmetrix integration is similar, in that a javascript library is embedded in the browser. This javascript sends device information directly to threatmetrix without a Mule integration. Additional information is sent to and collected from threatmetrix subsequent to the submission of a form.

Journey Manager will collect all forms, and third party information in a PGP encrypted zip file. This file will be submitted to CWB's sftp server and stored in the CWB document management system (Filenet). This integration

does not take advantage of Mule, primarily to a general architectural pattern that prefers Mule for real-time integrations and sftp servers for batch file integrations.

2.7.1. Overview Diagram



2.7.2. API Security

API Connectivity between Avoka, the on-premise Mule runtime and thirdstream will implement the following security controls as approved by the CWB Security Team. Furthermore, where sensitive credentials are passed from Avoka to CWB, there will be an additional attribute level encryption applied. See Secure Handling of Credentials for further details.

Avoka (See #1)

- Whitelist CWB IP Addresses
- All communication with CWB is over via TLS 1.2

CWB (See #2, #3, #4)

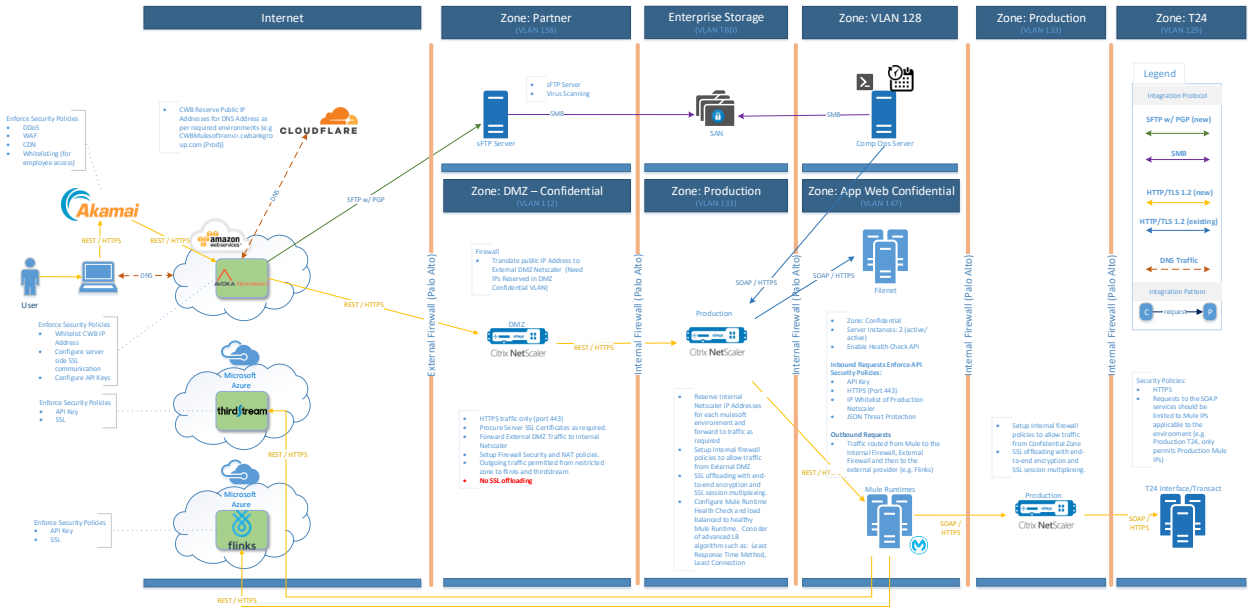
- Whitelist Avoka IPs
- Enforce API Key for each API call
- Enforce TLS 1.2 (server side only)
- SSL is terminated at Mule, thereby traversing all layers as encrypted traffic
- Where file exchanges are required, sFTP with PGP encryption will be utilized

Thirdstream (see #5, #6)

- Enforce API Key for each API call
- Enforce TLS 1.2 (server side only)
- CWB enforces Firewall policy to allow traffic to the thirdstream domain/endpoints from internal mulesoft runtimes

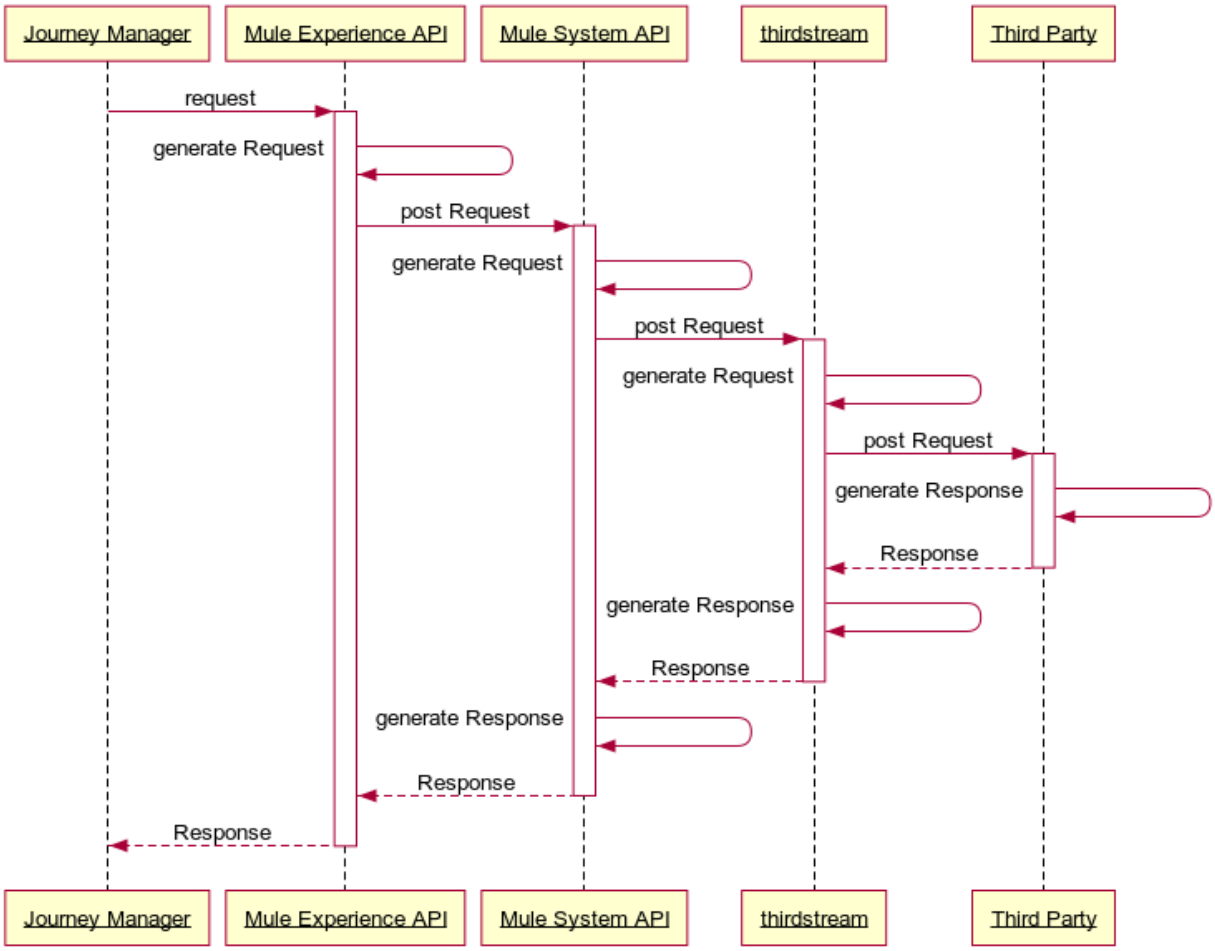
Flinks

- Enforce API Key for each API call
- Enforce TLS 1.2 (server side only)
- CWB enforces Firewall policy to allow traffic to the Flinks domain/endpoints from internal mulesoft runtimes



2.7.3. Third Party Integration Pattern

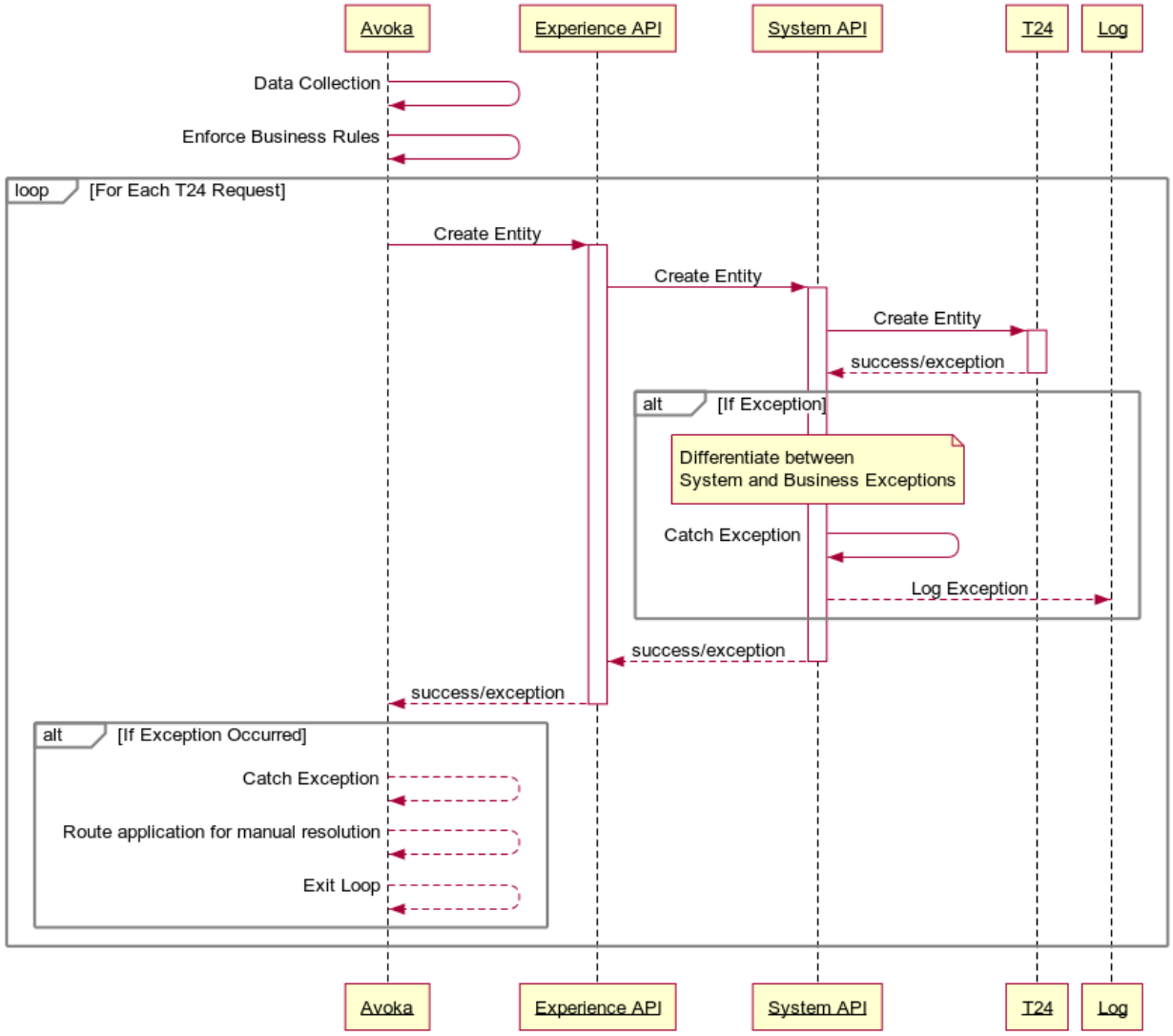
CWB has partnered with thirdstream - an Alberta based fintech with specialization in the account opening process and with digital integration to Canadian partners - to facilitate customer verification, address verification, fraud monitoring and funding. The typical pattern for integration will be as indicated in the sequence digram below. Exceptions will be permitted where necessary (see the section on Exceptions to Integration Patterns).



2.7.4. Error Handling

Multiple application tiers are part of any request from Avoka Journey Manager to provider systems (such as T24). The following decisions have been made and approach defined to provide the business with an accurate understanding of where errors have occurred and where manual intervention is required to complete the application process on behalf of the customer.

- Journey Manager will call the APIs to create the required T24 entities once the system has collected and validated all customer details,and determined the customer has met all business rules for automated customer/account creation
- Experience APIs hosted by Mule will remain “granular”, allowing the Journey Manager to orchestrate the API requests as per the business requirements.
- Errors raised by a provider system, or by Mule itself, whether technical or business oriented will be propagated up to Journey Manager with sufficient detail to determine the error code, and its classification (business or technical).
- Journey Manager will route these errors to the appropriate queue for alerting and manual intervention.
- Automated retries will generally not be implemented at any layer due to the lack of idempotency in the T24 core banking system and the potential to create duplicate records. If a scenario is identified where an exception clearly identifies a scenario where an automated retry can be attempted, then then an automated retry should be attempted.
- This topic will be reconsidered when discussing the new online banking solution.



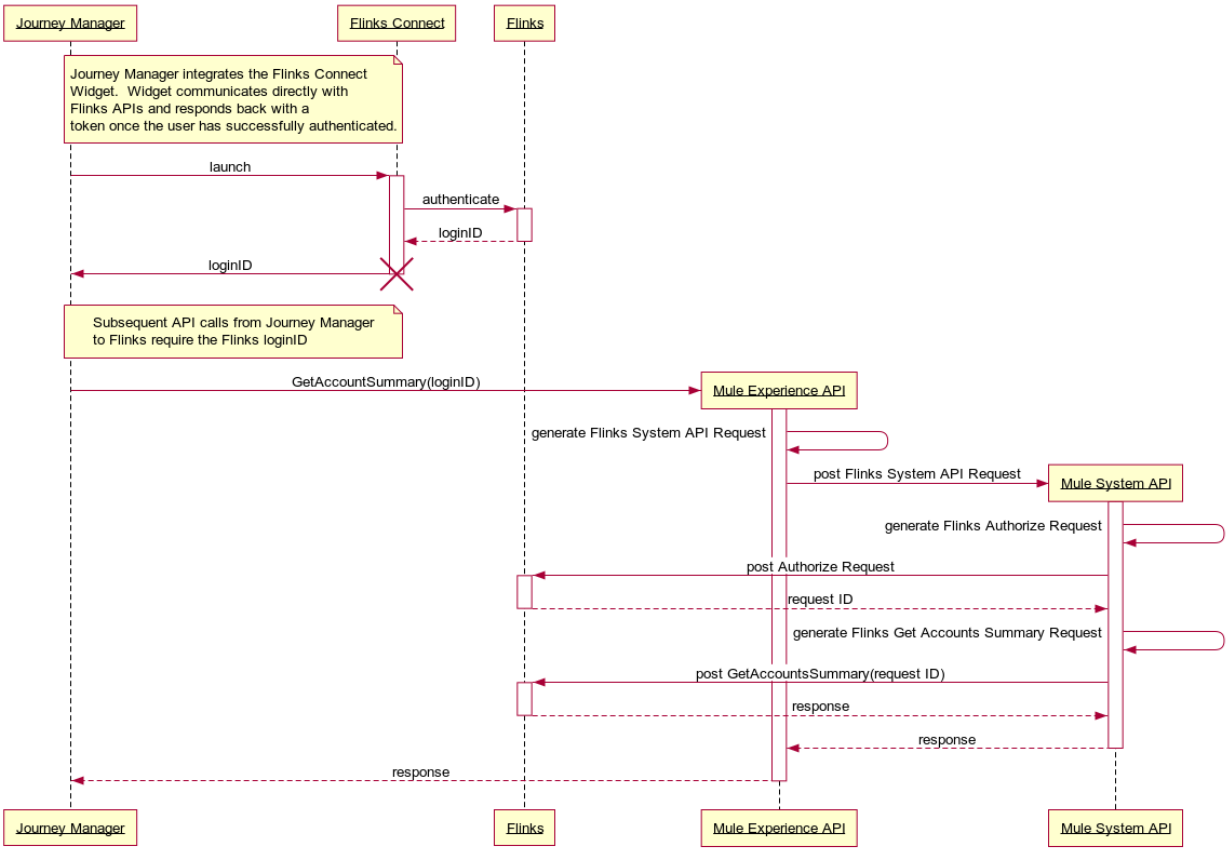
2.7.5. Key Integrations

2.7.5.1. Flinks Integration Pattern

Although Flinks is supported by thirdstream, the Third Party Integration Pattern will not be adhered to for the following reasons:

- CWB has set a principal that no non-CWB credentials shall be captured or processed directly by CWB applications/systems.
- An API integration model for Flinks requires the capture of non-CWB credentials (userid, password, multi-factor authentication) and the hand-off of these details from browser to various intermediary systems, such as: Journey Manager, Mule, thirdstream and then Flinks.

- Flinks Connect is a module that assists all customers in connecting their bank accounts in a secure and intuitive way. All the complicated capture of bank credentials, multi-factor authentication, edge cases and errors are handled —keeping credentials from ever hitting CWB servers.
- CWB has less development, maintenance and testing with respect to the the integration of Flinks and the addition of new financial institutions.
- Flinks Connect becomes a component of the Journey Manager application that needs to be added in a webview. No additional hosting or additional server is needed.



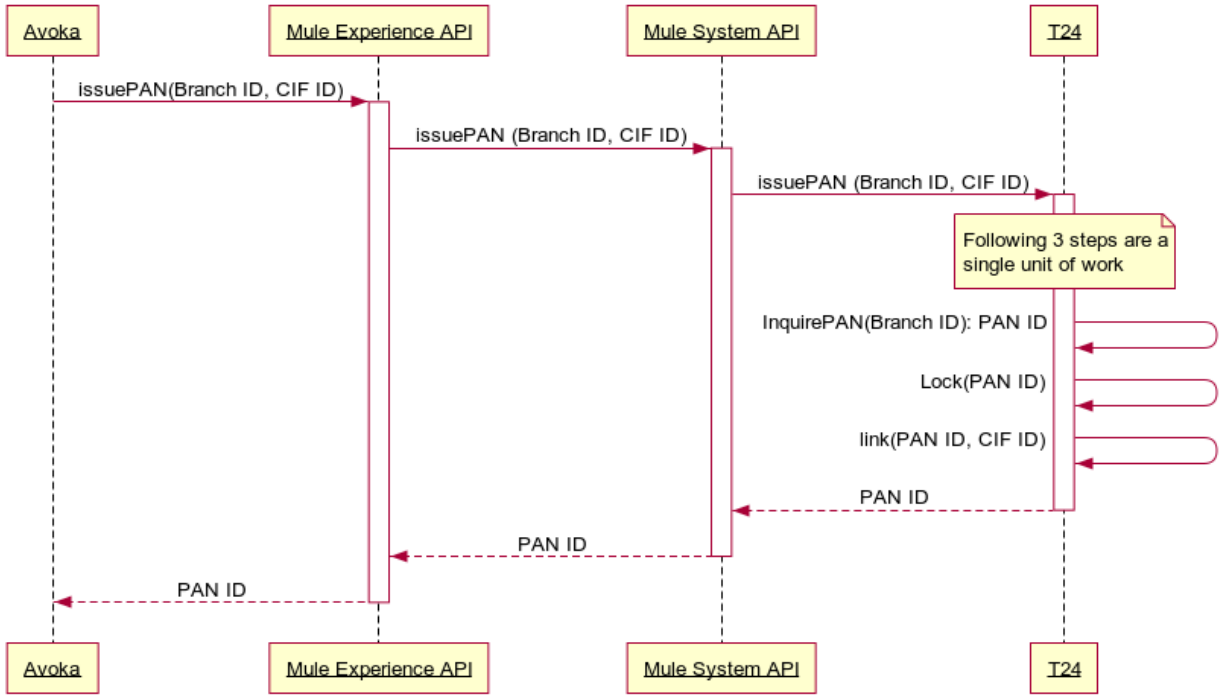
2.7.5.2. Threatmetrix Integration

Threatmetrix is a fraud prevention platform. Threatmetrix provides a javascript library and a session key that is embedded in the Avoka customer UX. Device data is collected by the javascript, directly transmitted to Threatmetrix servers and analyzed by Threatmetrix, resulting in a risk score. When requesting a fraud score, Avoka will call the Fraud Check API hosted by Mule passing along the session key utilized by the threatmetrix javascript, which in turn calls thirdstream and then threatmetrix to determine the resulting risk score. This risk score is used in decisioning logic.

2.7.5.3. PAN Issuance

PAN issuance will require T24 to handle the following steps in a single atomic unit of work:

- Determine the next available PAN ID from a Branch's inventory
- Lock the PAN
- Link the PAN to the Customer's CIF



2.7.5.4. Secure Handling of Credentials

The Digital Onboarding process captures customer credentials (PAC, secret question and secret answer), transmits these to Journey Manager which in turn calls the necessary CWB APIs to transmit the value for update in T24. This information is especially sensitive, since it can be used to access a customer's online banking account, expose PII and enable money movement. Therefore, the credentials will be encrypted in the browser upon entry by the user and decrypted by the Mule runtime before sending the value to the T24 Interface/T24 Transact servers over secured transport protocols.

RSA public key encryption will be utilized to encrypt/decrypt the credentials. Keypairs will be generated by CWB and the public keys distributed to the Journey Manager administrator to populate the Journey Manager Keystore. See Cipher Specifications for further details. The private keys will be stored in the Keystore of the Mule runtime components. CWB will generate two keypairs. This will facilitate a seamless rotation between keys in the event the active keypair must be substituted for another. This will allow inflight applications with an "old" keypair to co-exist with new applications with the "new" keypair. See Key Rotation for further details.

Before the encrypted credential is sent over the wire from the browser, it will be *wrapped* to include some additional meta-data to support the key rotation process. See Encrypted Payload for further details on this process.

1.7.4.4.1 Cipher Specifications

The following specifications were successfully applied in a proof of concept that encrypted data in the browser and decrypted it in a server side Java component. These same settings are acceptable for a production implementation and should be replicated in the Avoka and Mulesoft components.

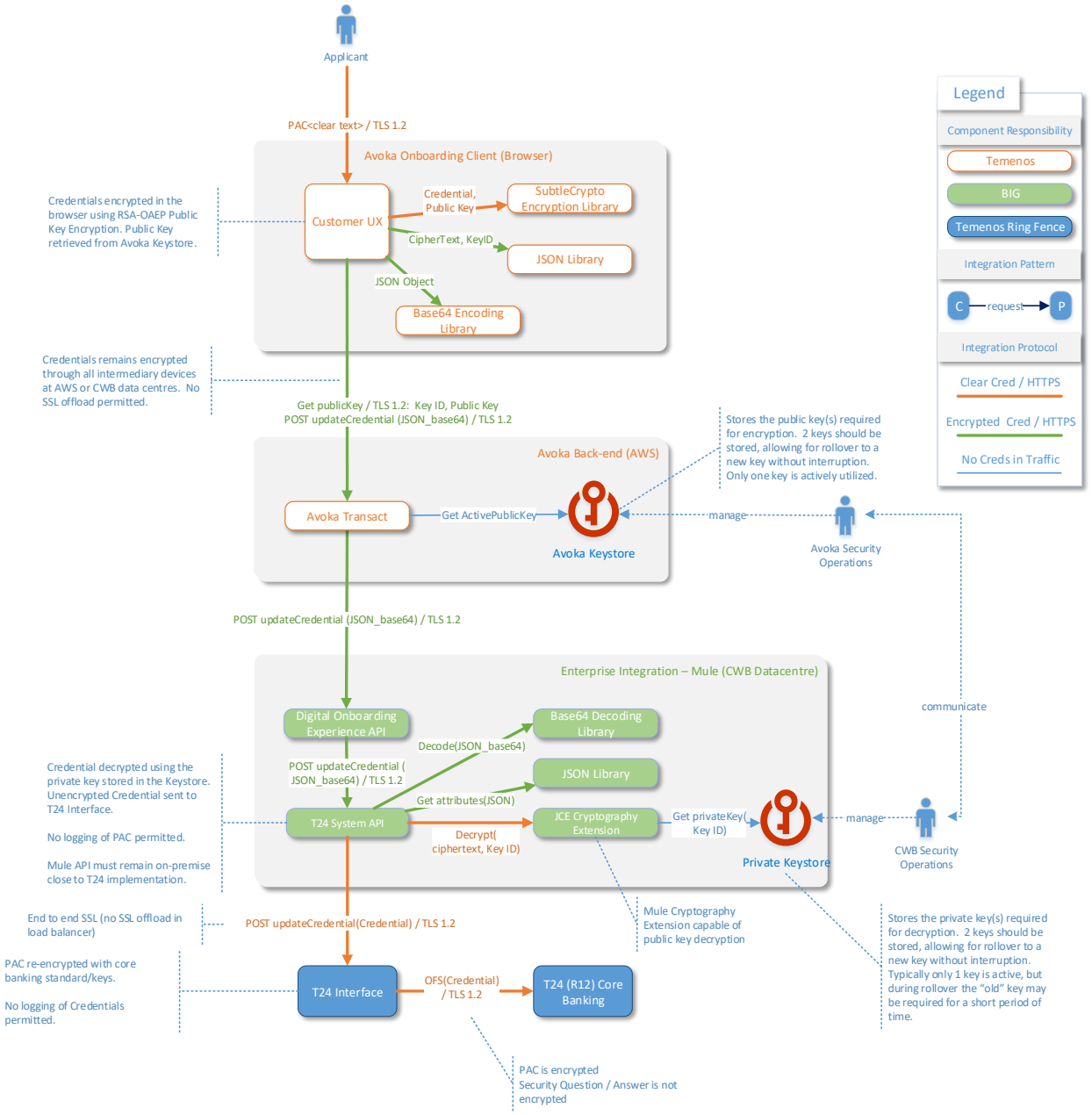
Javascript:

Encryption Algorithm:	RSA
Padding:	Optimal Asymmetric Encryption Padding (OAEP)
Modulus Length:	2048
Public Exponent:	65537
Hash function:	SHA-256

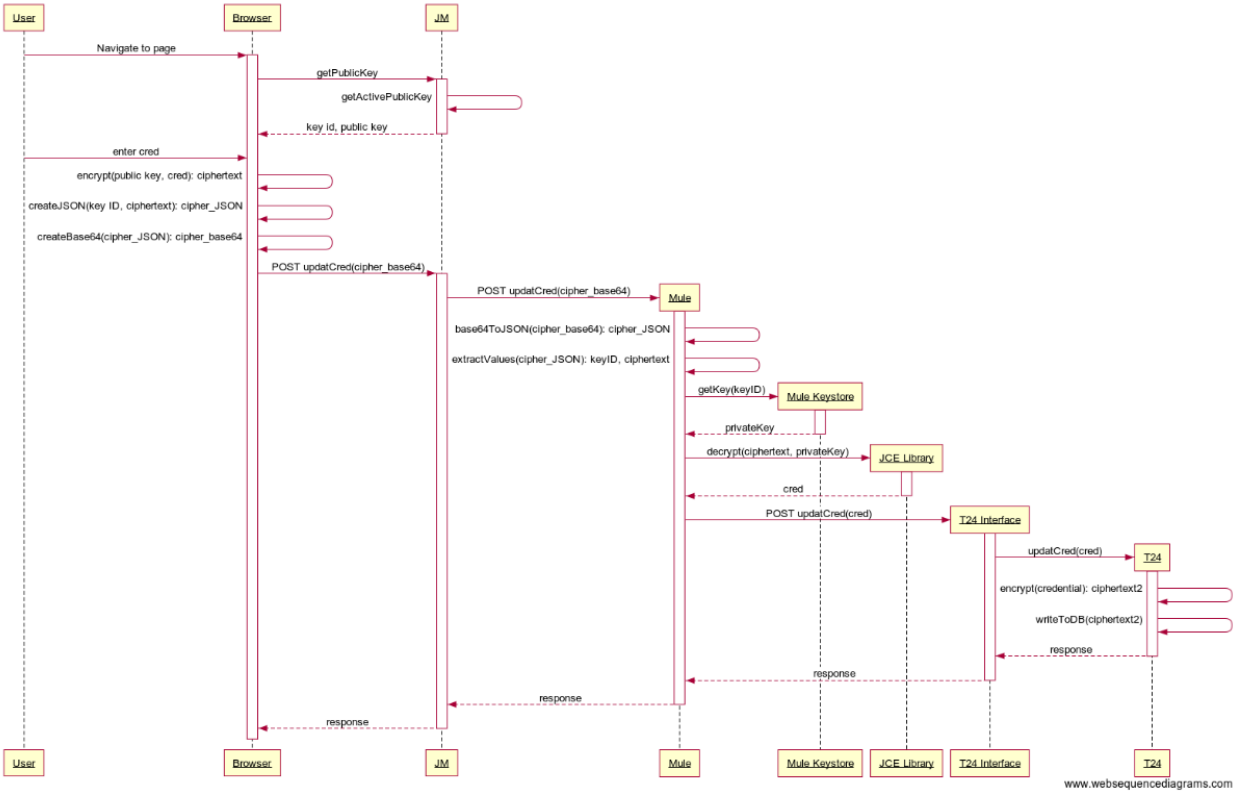
Java:

Cipher:	RSA/ECB/OAEPWITHSHA-256ANDMGF1PADDING
OAEP Message Digest Algorithm:	SHA-256
OAEP Mask Generation Function:	MGF1
OAEP Parameter Spec:	SHA-256
OAEP 'P' Encoding Value:	Default

1.7.4.4.2 Overview Diagram



1.7.4.4.3 Sequence Diagram



1.7.4.4.4 Sequence Steps

1. User navigates to a page with a credential (e.g. PAC, secret question, secret answer)
2. Browser application retrieves the currently active public key and associated keyID.
3. Browser encrypts the credential (aka ciphertext), utilizing the public key and the cryptographic library native to most modern browsers
4. Browser creates a JSON object, including the KeyID and the encrypted credential. (aka cipher_JSON)
5. Browser base64 encodes the JSON object (aka cipher_base64)
6. Browser submits the HTTP request and cipher_base64 string to Journey Manager
7. Journey Manager submits the HTTP request and cipher_base64 string to Mule
8. Mule decodes the cipher_base64 value, resulting in the cipher_JSON object
9. Mule extracts the KeyID and cipher text from the JSON object
10. Mule retrieves the private RSA Key based on the KeyID received
11. Mule decrypts the ciphertext utilizing the private RSA Key, resulting in the original credential

Note: the following steps are as per current design and utilize the native encryption scheme utilized by T24 today to safely encrypt the credential in the T24 database

12. Mule submits the credential to T24 Interface
13. T24 Interface submits the value to T24
14. T24 encrypts the value and stores it in the database

1.7.4.4.5 Key Rotation

Both the client (Journey Manager) and server (T24 Interface & HSM) will have separate key stores, each with two "key slots". The client (Journey Manager) keystore will store the public keys and the server (HSM) keystore will store the private keys.

To support the rotation of public key pairs, 2 "key slots" will be configured in both the client and server key stores. Only 1 key slot will be active in the client application at any one time, but the server must be able to decrypt with either of the 2 keys. This is to address the period of key rotation, where a new key is activated (and the old one deactivated). New applications will utilize the new key, but there may still be pending applications utilizing the old key that have not yet been submitted to the server. In both cases the server must be able to decrypt the encrypted value regardless of which key was utilized.

A Key rotation will be triggered when the Journey Manager application switches which "key slot" is active. The keyID will be communicated along with each encrypted value to provide the server a "hint" as to the key that is in use for the particular transaction.

Once it is confirmed that the old key is no longer in use, a new key pair should be generated by CWB Security Operations for the inactive slot, distributed to the appropriate key store administrators and updated in both the client and server key stores. Once these steps have been taken, the solution is prepared for a key rotation.

1.7.4.4.6 Encrypted Payload

The credentials captured in the browser will undergo the following transformation before sending the sensitive data over the wire.

- Encrypt the credential using RSA Public Key Encryption
- Create a JSON object with two values:
    - KeyID - the key id of the public key utilized to encrypt the credential
    - Value - the encrypted credential
    - e.g. **{ "kid":n, "value":"<encrypted credential>"}**
- Base64 encode the JSON object

1.7.4.4.7 Logging

Credentials should not be written to log files at any tier, inclusive of Avoka, Mule and T24 Interface/T24 Transact. If this occurs, the values should be encrypted, masked or hashed at rest. Elastic Search aggregated logging must not import any credentials in clear text format.

1.7.4.4.8 HSM

The Hardware Security Module (HSM) from FutureX will not be utilized to store or decrypt values as originally intended. The appliance currently in production cannot support asymmetric encryption routines and is therefore not a viable alternative for the time being.

1.7.4.4.9 Mule Security Constraints/Controls

- Mule must decrypt using standard Mule or Java components. No third party libraries are acceptable unless approved by the Security Team.
- Mule must implement secure storage of secrets, including public/private keypairs and keystore passwords
- The APIs affected, must remain in the on-premise Mule runtimes and not migrated to the cloud until credential storage is migrated to Okta.
- The Mule runtime must not log any of the sensitive credentials
- The Mule runtime must communicate with the T24 Interface Server over TLS
- Mule Runtime must be moved from the Restricted Network Zone to the Confidential Network Zone. This should be applied across all non-prod zones as well.
- Least Privilege access controls applied to Mule production servers

1.7.4.4.10 T24 Interface / T24 Transact Security Constraints/Controls

- The T24 Interface Server must not log any of the sensitive credentials
- The T24 Interface Server must communicate with T24 Transact (Core Banking) over TLS
- T24 must not log any of the sensitive credentials

1.7.4.4.11 POC Implementation Details

Javascript

```
window.RSAOAEP = {
        name: "RSA-OAEP",
        modulusLength: 2048,
        publicExponent: new Uint8Array([0x01, 0x00, 0x01]),
        hash: {name: "SHA-256"},
    }
```

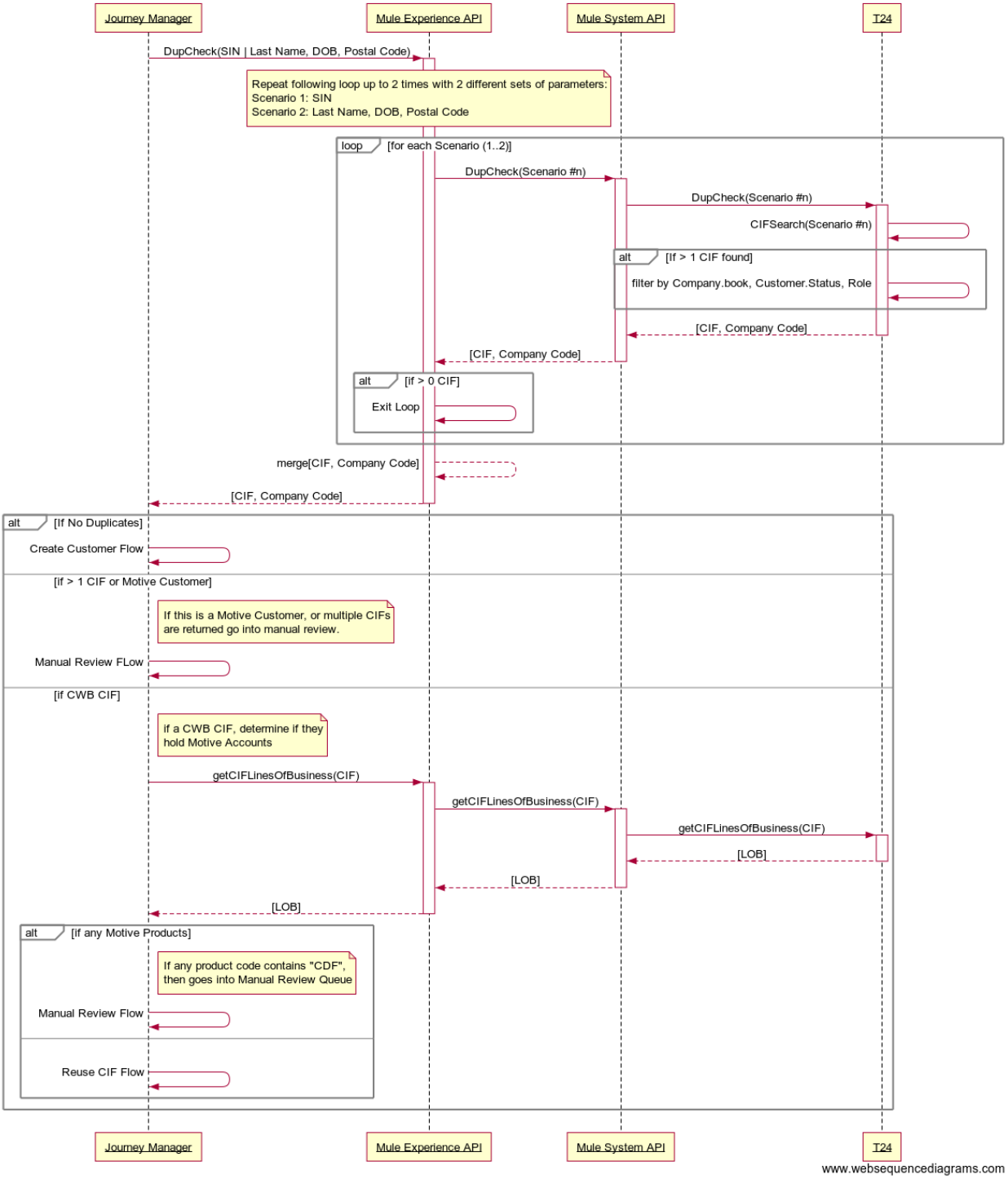
Java

```
cipher = Cipher.getInstance("RSA/ECB/OAEPWITHSHA-256ANDMGF1PADDING");
oaepParameterSpec = new OAEPParameterSpec("SHA-256", "MGF1",MGF1ParameterSpec.SHA256, PSource.PSpecified.DEFAULT);
Key key = this.decryptkeystore.getKey(keyAlias, "password").toCharArray());
cipher.init(Cipher.DECRYPT_MODE, <key>, oaepParameterSpec);
```

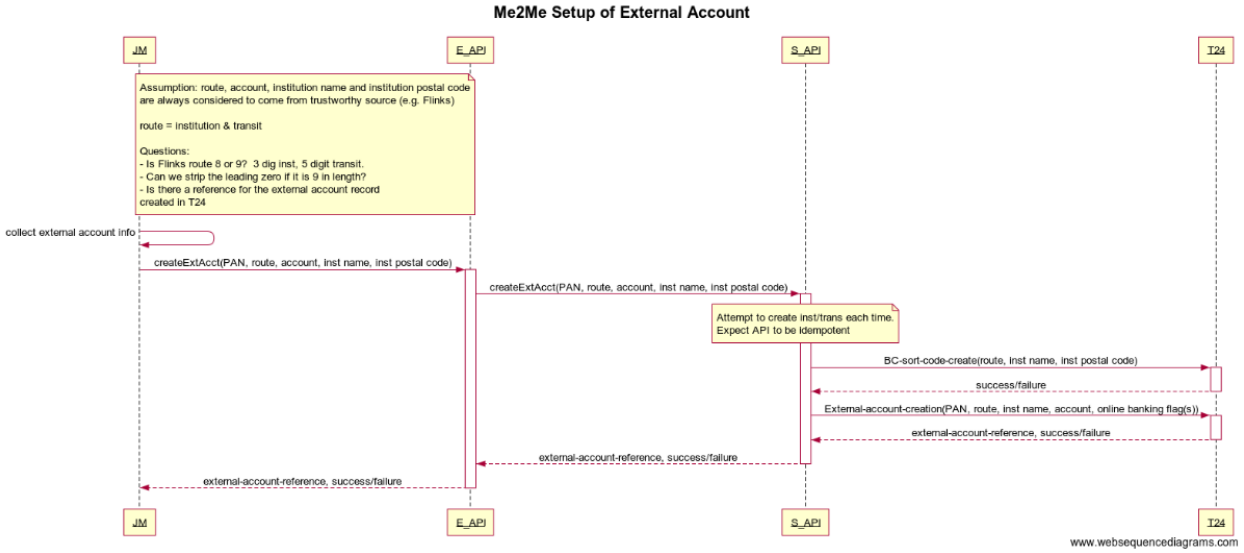
2.7.5.5. Image Compression

Mule will enable an integration with thirdstream to extract information from the AAMVA barcode on a Canadian Driver's Licence. Mule will take on the responsibility of image adjustments to meet the preferred resolution of the image to ensure optimal performance by the thirdstream service. Standard image files (jpeg, gif, png, tiff, etc.) will be supported; however, tiff images will not be optimized by the Mule service due to a gap in tiff image processing capability. The image will be passed as is to the thirdstream service. This may result in a less than optimal performance for tiff images; however, tiff images are very unlikely to be provided by most customers.

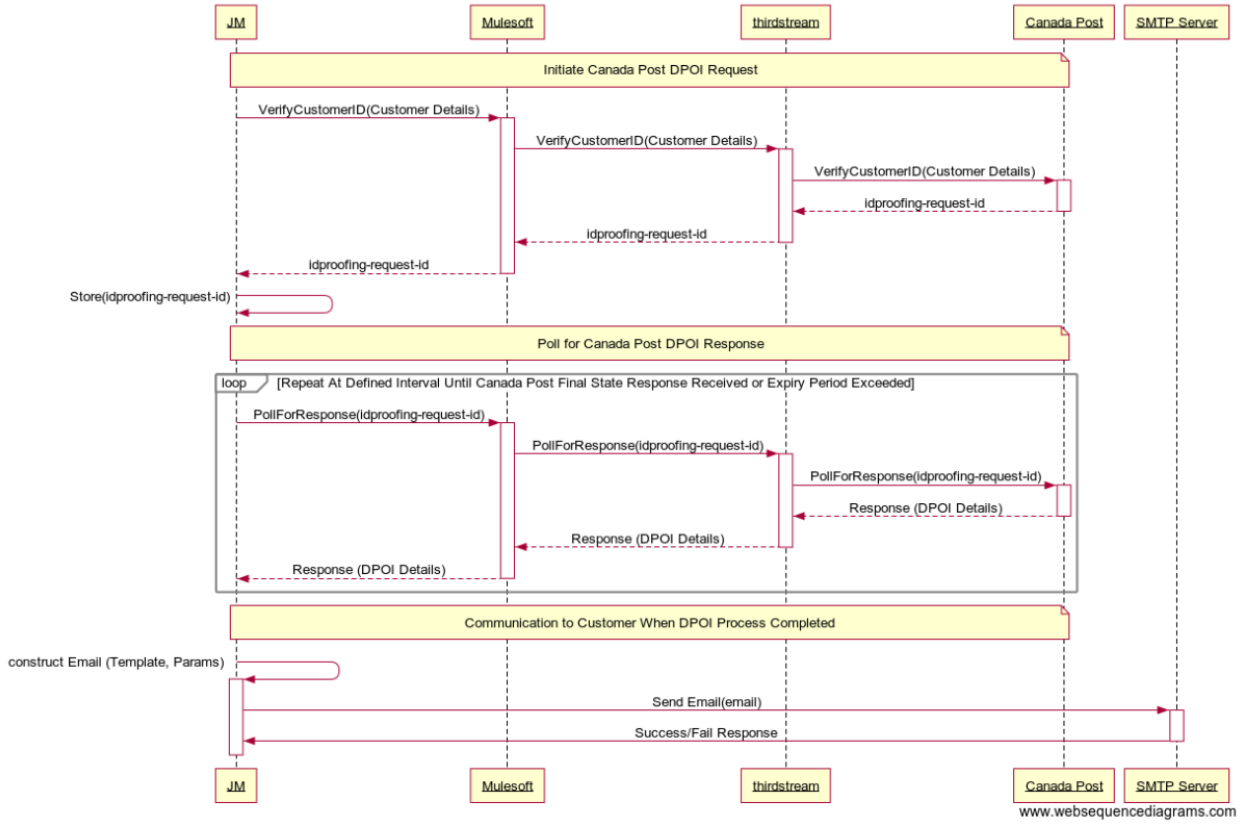
2.7.5.6. Customer Duplicate Check



2.7.5.7. Me2Me Setup



2.7.5.8. Canada Post DPOI



2.7.5.9. Okta Authentication and Single Sign-On

DCO will support use cases for existing customers to self-identify and authenticate against the CWB Customer Okta tenant. Authentication will allow DCO to optimize the application process, prepopulating the application with information already known about the customer. Customers will authenticate utilizing the Okta widget.

Authenticated User Flow - Consolidated

2.7.6. sFTP Integration

Journey Manager is an event based system, and will send a zipped and PGP encrypted package of documents once an onboarding application has reached a final state. These packages arrive at any time throughout the day and represent a single digital onboarding application. The following sections describe where the files will be stored on the sftp server, the file naming standard and the steps taken to upload these files to Filenet for the required retention period.

2.7.6.1. SFTP Server Root Path

The sftp server root path will allow for production and non-production environments. Each root path will be prefixed by the *system ID* provided to Temenos and the *line of business*. Different system IDs will be provided for non-production and production environments. For example, for applications processed through the Motive Journey Manager flow, this will be prefixed with *motive*.

Journey Manager Environment	SFTP Root Path
Development	${system ID}/${lob}/dev
SIT	${system ID}/$(lob)/sit
UAT	${system ID}/$(lob)/uat
PrePROD	${system ID}/$(lob)/preprod
PROD	${system ID}/$(lob)/prod

2.7.6.2. SFTP Server Folder

The delivery folder is based on *final status* of the application review process follows.

Final Application Status	Folder
Approved	/approved
Withdrawn	/withdrawn
Abandoned	/abandoned
Declined	/declined

E.g.

If an application is processed by the production motive journey flow and ultimately approved, it will be delivered to:

Temenos/motive/prod/approved.

If an application is processed to the uat motive journey flow and ultimately declined, it will be delivered to:

Temenos_tst/motive/uat/declined.

2.7.6.3. File Naming Standard

The **.ZIP file naming pattern** will include the primary CIF ID, Line of Business, Journey Manager Tracking Code and the Final Status as follows:

${CIF_ID}-${line of business}-${trackingCode}-${finalStatus}-dco.zip

Examples:

123456-Motive-3XRV7HA-Approved-dco.zip (Approved example)

Motive-3XRV7HA-Withdrawn-dco.zip (Withdrawn example)

Motive-3XRV7HA-Abandoned-dco.zip (Abandoned example)

2.7.6.4. File Contents

The contents of the delivery .ZIP file will include:

Folder	File(s)	Notes
/<form name>/	FormXml.xml	The form XML data
/<form name>/Emails/	<Email Name>Email.html	Each Email sent is added as an .HTML file
/<form name>/File-Attachments/	Attachment<File Name>	Each file attachment on the Txn
/<form name>/Txn-Properties/	<Property Name>	All Properties stored on the Txn that are not Email, Integrations, etc.
/<form name>/<Integration Name>-Integration/	<Property Name>	Each Property stored on the Txn that is specific to the Integration Services
/<form name>/	FormReceipt.pdf	Receipt PDF

2.7.6.5. Filenet Integration

The data in the production zip files is considered **confidential** and the contents of this file will be archived in Filenet. The Filenet folder location and associated metadata is detailed further below.

Computer Operations will develop a powershell script [1] to schedule the movement of files from the sftp server to a secure location on the Storage Area Network. The files must be removed from the sftp server when moved to the

[1] Generally the Computer Operations group utilizes a common server to run powershell scripts to facilitate the movement of files within the CWB network. This server is not in the Confidential Zone and for this reason is not ideal when dealing with confidential data. However, given that the DCO zip files will be moved

secure folder structure on the NAS. From there, the file will be decrypted, unzipped and stored in the the Filenet application. **A unique AD service account** will be requested and given authority to access/manage the files from the specified sftp folders and upload the files to the appropriate location(s) on the SAN and then on to Filenet.

Depending on the sftp folder structure and naming standards of the file, computer ops will upload the files into Filenet based on the following rules:

SFTP Source	Filenet Target	Filenet Meta-data	Description / Rules
{lob}/prod/approved e.g. lob = motive	{lob}/CIF_ID e.g. lob = motive	CIF_ID TrackingCode	These files represent approved applications in the production environment. These files will be received with the following naming standard: ${CIF_ID}-${line of business}-${trackingCode}-${finalStatus}-dco.zip The CIF_ID can be extracted from the filename when determining where to store the file in the Filenet structure. Filenet Meta-data will be set based on the naming standard of the file. In this case, both the CIF_ID and TrackingCode should be set as meta-data.
{lob}/prod/withdrawn	{lob}/withdrawn/${year file was received}	TrackingCode	These files represent applications that have been withdrawn by the user in the production environment. These files will be received with the following naming standard: ${line of business}-${trackingCode}-${finalStatus}-dco.zip The "*year file was received*" (i.e. YYYY) should be determined from the creation date of the file on the sftp server (or in the SAN folder – whichever is most expedient to implement). Filenet Meta-data will be set based on the naming standard of the file. In this case, the TrackingCode should be set as meta-data.
{lob}/prod/abandoned	{lob}/abandoned/${year file was received}	TrackingCode	These files represent applications that have been withdrawn by the user in the production environment. These files will be received with the following naming standard: ${line of business}-${trackingCode}-${finalStatus}-dco.zip The "*year file was received*" (i.e. YYYY) should be determined from the creation date of the file on the sftp server (or in the SAN folder – whichever is most expedient to implement). Filenet Meta-data will be set based on the naming standard of the file. In this case, the TrackingCode should be set as meta-data.

to a secure location on the SAN, remain in this location for decryption and unzipping and then stored in Filenet, this will be acceptable for the time being.

{lob}/prod/declined	{lob}/declined/${year file was received}	TrackingCode	These files represent applications that have been declined by CWB in the production environment. These files will be received with the following naming standard: ${line of business}-${trackingCode}-${finalStatus}-dco.zip The "*year file was received*" (i.e. YYYY) should be determined from the creation date of the file on the sftp server (or in the SAN folder – whichever is most expedient to implement). Filenet Meta-data will be set based on the naming standard of the file. In this case, the TrackingCode should be set as meta-data.

2.7.6.6. Filenet Access

Access to Filenet is determined through AD privileges and limited to a small group of individuals with the authority to view/download the file contents under this folder.

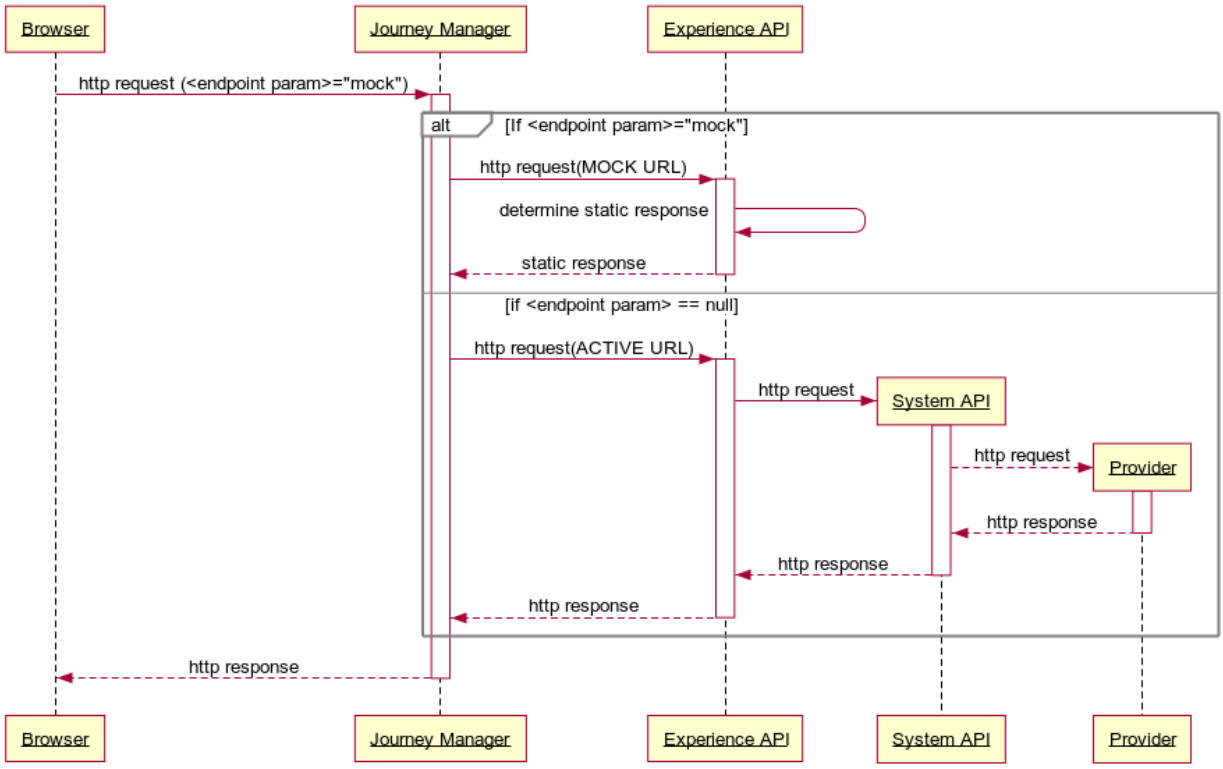
2.7.6.7. Filenet File Retention

Filenet will be configured to retain these files for 7 years.

2.7.7. Mock APIs for Testing

Mock APIs will be established to help the CWB Quality Assurance team test edge cases in pre-production environments that are otherwise difficult to test, given the wide variety of third parties involved in the end-to-end solution. A Mocking framework will be established, allowing a QA tester to direct requests to a specific API Mock endpoint when testing a scenario. Journey Manager will accept http parameters indicating which endpoint(s) should be redirected to a Mule hosted Mock endpoint. Mule will configure a variety of response types, which will be selected based on content in the original request. The Mock services will sit at the "Experience API" layer. The Mock services will load response files from a local folder on the Mule Runtime server. Group access will be provided to the folder which will permit an individual to load files for mock service testing.

At this time, Mock testing will be limited to the Partner QA Environment and the CWB SIT Environment. Journey Manager Mock parameters and Mule Mock services will not be deployed to the CWB UAT and Production environments.



2.7.8. Summary Integrations

2.7.8.1. File Based/Batch Integrations

Source	Target	Facilitated By	Status	Occurance	File Type	Protocol	Security
Avoka Platform (AWS)	CWB Datacentre	Computer Operations via Powershell Scripting	New	Event Driven	Zip File	sFTP	PGP Encryption

2.7.8.2. Real-time Widget/Javascript Integrations

Function	Provider	Type
Threatmetrix Device Details Collector	Threatmetrix	Javascript Library
Flinks Logon Widget	Flinks	Widget via iFrame
Journey Manager Analytics	Google Analytics	Javascript Library

2.7.8.3. Real-Time Integrations

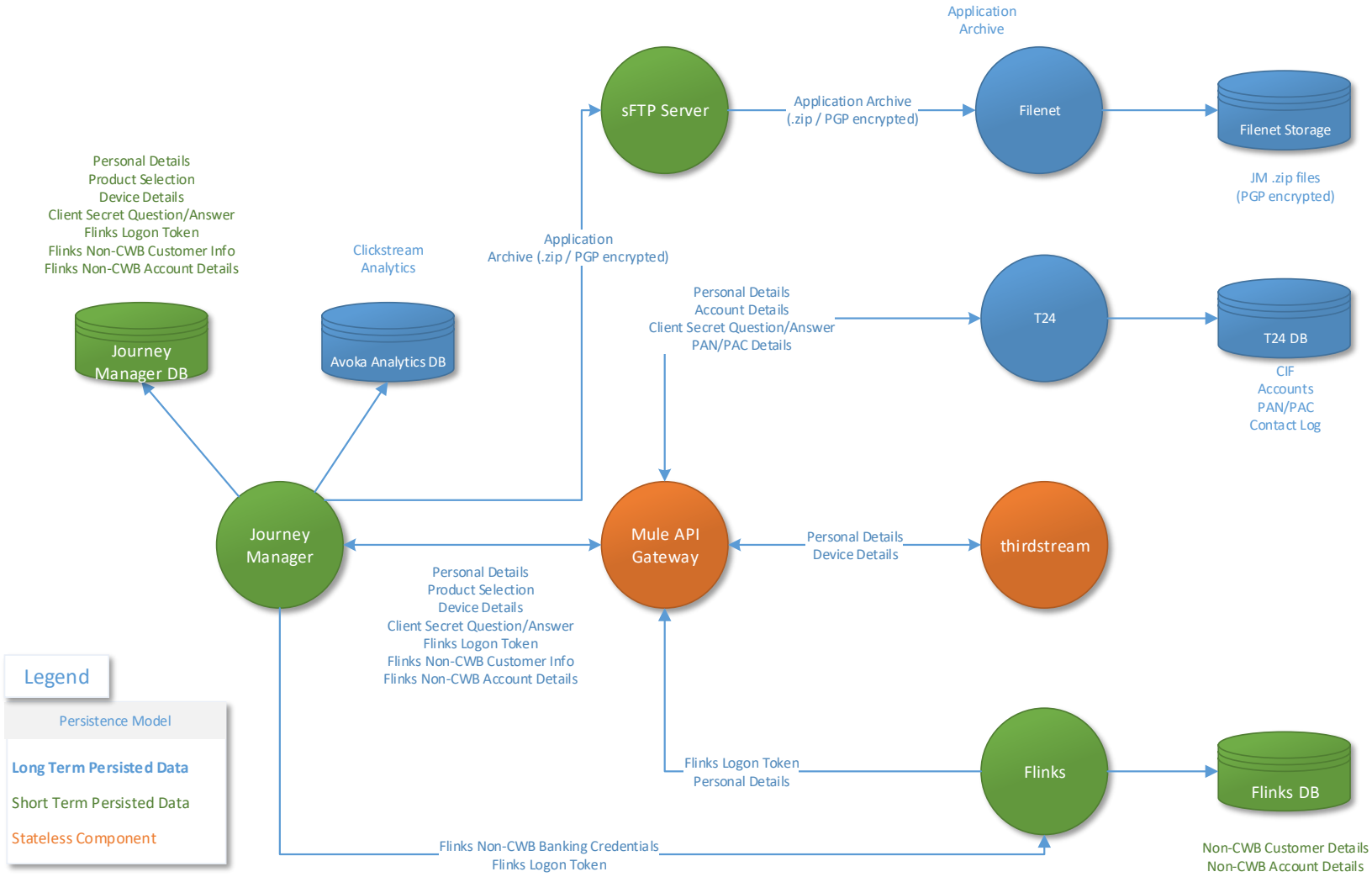
Function	Endpoint	MuleSoft	Flinks	Thirdstream	T24 (TWS / Transact)	Amazon (AWS)	Proof Point
Canada Address Post Verification	Mulesoft REST API	GET /addresses		/addresses			
	Mulesoft REST API	GET /addresses/{id}		/addresses/{id}			
ID Scan	Mulesoft REST API	POST /identitycards/readBarcodes		POST /identitycards/readBarcodes			
Equifax Credit Check	Mulesoft REST API	POST /personalCreditReports		POST /creditbureau/v2/reports/personalcredit			
Equifax AML Assist	Mulesoft REST API	POST /amlComplianceReports		POST /amlcompliance/reports			
Threatmetrix Fraud Screening / Citadel Fraud	Mulesoft REST API	POST /fraudAssessmentReports		POST /fraudAssessments			
Enstream Mobile Verification	Mulesoft REST API	TODO					
Flinks Login	Flinks URL		Logon Widget				

Get External Accounts	Mulesoft REST API	GET /externalFIAccounts	GET /authorize GET /GetAccountsSummary GET /GetAccountsDetail				
DeleteCard	Mulesoft REST API	Delete /DeleteCard	Delete /DeleteCard				
Duplicate CIF Check	Mulesoft REST API	GET /corebanking/customers			WebserviceforECWBCUSCCVCIF		
Create Customer	Mulesoft REST API	POST /corebanking/customers			Based on CUSTOMER,CWB.PERSONAL		
Create Contact Log	Mulesoft REST API	POST /corebanking/customers/{id}/securityQuestions			DigVersionforCRContactLog		
Issue PAN	Mulesoft REST API	POST /corebanking/customers/{id}/cards					
Update PAC	Mulesoft REST API	PUT /corebanking/customers/{id}/cards/{id}					
Create Account	Mulesoft REST API	POST /corebanking/customers/{id}/accounts					
Create M2M	Mulesoft REST API						
Fund M2M	Mulesoft REST API						
Send SMS	Amazon Web Services REST API					See Amazon SNS API	

Send Email	Proof Point SMTP Relay SMTPS						SMTPS

2.8. Information and Data Architecture

2.8.1. Diagram



2.8.2. Process

Data collected by the Avoka Journey Manager platform is stored for a relatively brief period of time, until the customer application reaches a final state. Once the final state has been achieved, the application is either complete, withdrawn or abandoned. Typical "happy path" processing will result in API calls from Avoka to Mule that create entities in T24, the system of record for customers, accounts, PAN/PAC, Contact Logs and funding.

All details, including those not previously sent to CWB systems will be collected in a zipped archive file and transmitted to CWB (via sFTP) for storage in Filenet. The file will be transmitted with PGP encryption and will remain in this state when stored in Filenet.

Flinks, a third party involved in the identity verification step of the onboarding process will persist/cache non-CWB data until CWB explicitely requests a deletion of this data. This will also occur once the onboarding application has reached a final state.

Fourth party systems (i.e. those integrated with through third parties) are not included in this illustration as there is insuffient information collected at this time to determine the persistence model followed.

2.8.3. Information Classification

As per Section 2.2 of the Information Classification Standard Document, the data handled by the onboarding process is considered classified as **Level 3: Confidential**. All necessary security controls for classified data will be followed when in transit or stored.

2.9. Technical Architecture

The Digital Onboarding technical architecture is comprised of 4 major areas.

Journey Manager

Temenos Journey Manager is the platform on which the CWB Digital Onboarding application is built. CWB has entered into a contract with Temenos to host and manage the non-prod and production environments for this application. At the time of writing, Journey Manager can only be hosted in AWS. Several deployment options have been discussed and one recommended by the Architecture and Security Teams. The details of this are provided in the sections below.

Mule

The Mule API Gateway will be the primary means of integrating with CWB internal and external partners. At the time of writing, the Mule runtimes will be hosted in the CWB data centre. An Architectural Decision was created to determine the deployment model for the Mule runtimes, but with the primary driver being project timelines. A hybrid architecture was approved, allowing Mule to be deployed on-premise and also in the cloud, with appropriate security controls in place. Details of this architecture are provided in the sections below.

External Providers

External providers such as thirdstream and flinks are provided as a SaaS model. Secure protocols, such as TLS 1.2 and API keys are utilized to connect to each of these partners. No further details of the technical architecture are described in this document.

Internal Providers

Internal providers such as T24 Connect, Filenet, SAS AML, Proofpoint and Microsoft Exchange all have established technical architectures. Additional environments have been established for T24 Connect to facilitate testing and SOAP API development, but no additional changes have occurred to the architecture of any other internal providers. No further details are provided in this document.

2.9.1. Environment Purpose/Definition

In partnership with Digital Onboarding implementation partners Avoka/Temenos, Bits and Glass and thirdstream, CWB application development, CWB Application Management Services and CWB Quality Assurance the following environments have been defined in support of the project SDLC and operational support activities:

2.9.1.1. Project Environments

jm-infinity-environments.xlsx

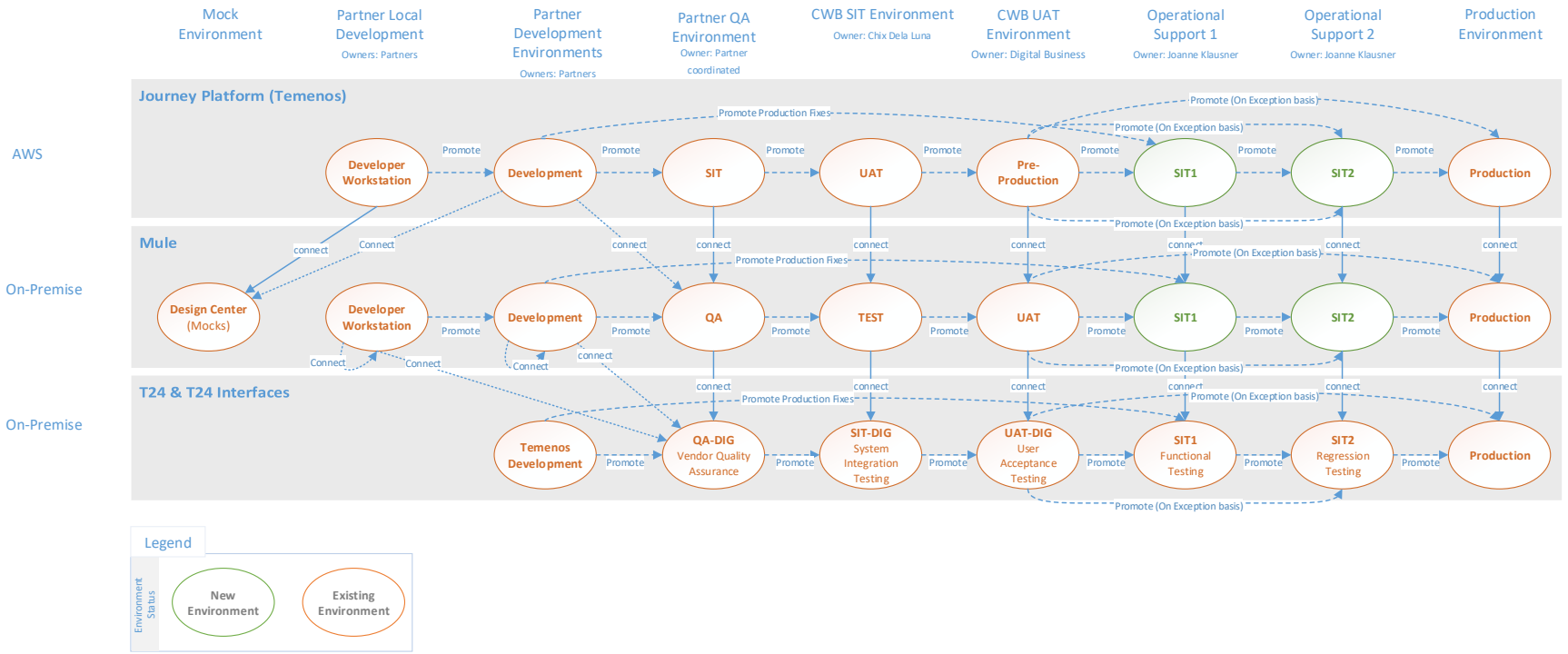
2.9.1.2. Operational Support Environments

- **CWB Operational Support 1 –** CWB coordinated **functional** testing of production defect fixes or minor production enhancement.
- **CWB Operational Support 2 –** CWB coordinated **regression** testing of production defect fixes or minor production enhancements.

2.9.1.3. Production Environment

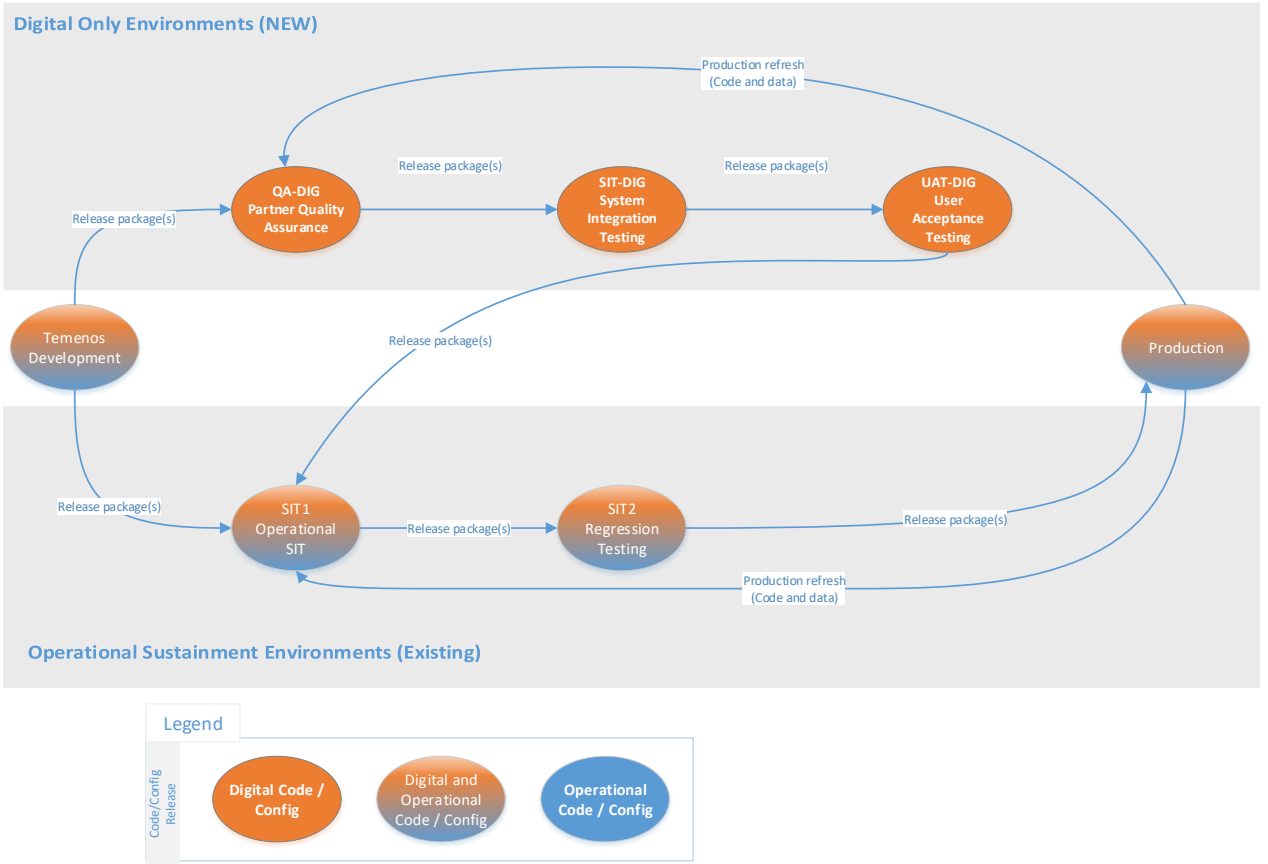
- **Production –** The customer facing production environment.

2.9.2. Project and Operational Support Environment Diagram

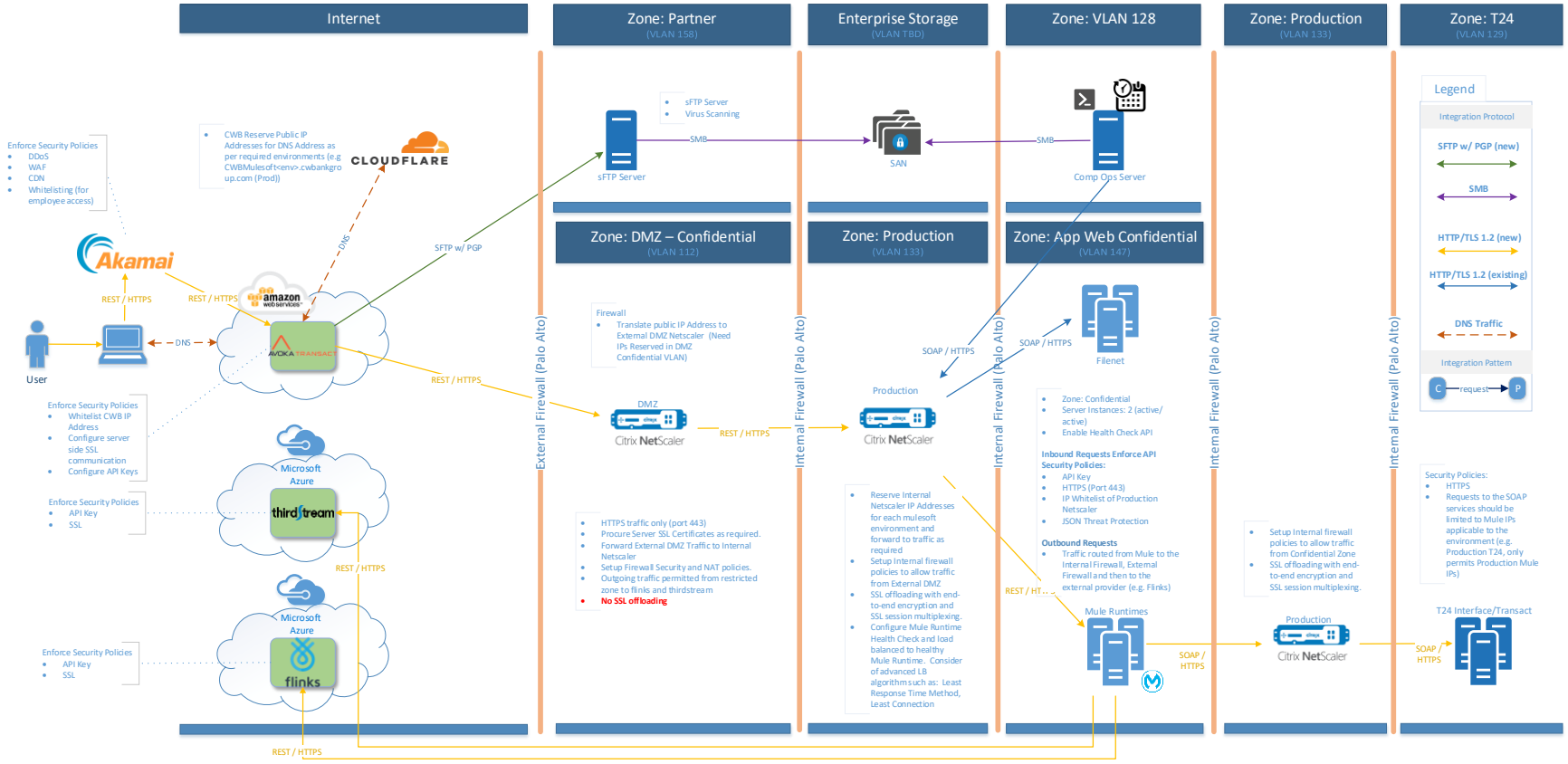


2.9.3. T24 Project and Operational Support Diagram

The Digital Onboarding program has introduced 3 new T24 environments. The purpose of these environments is to ensure the Digital Onboarding program and its related projects can independently develop and test features without contention with the activities occurring in the T24 operational environments. It will generally be true that any code developed in the onboarding program will also need to be tested in the operational environments to ensure all systems dependent on T24 are regression tested. This will commonly occur at the end of a series of digital onboarding sprints, when a significant release of digital onboarding enhancements are to be released. There may be some cases where code can be deployed from the digital environments directly into production, but it is not typically the rule.



2.9.4. Production Infrastructure Design



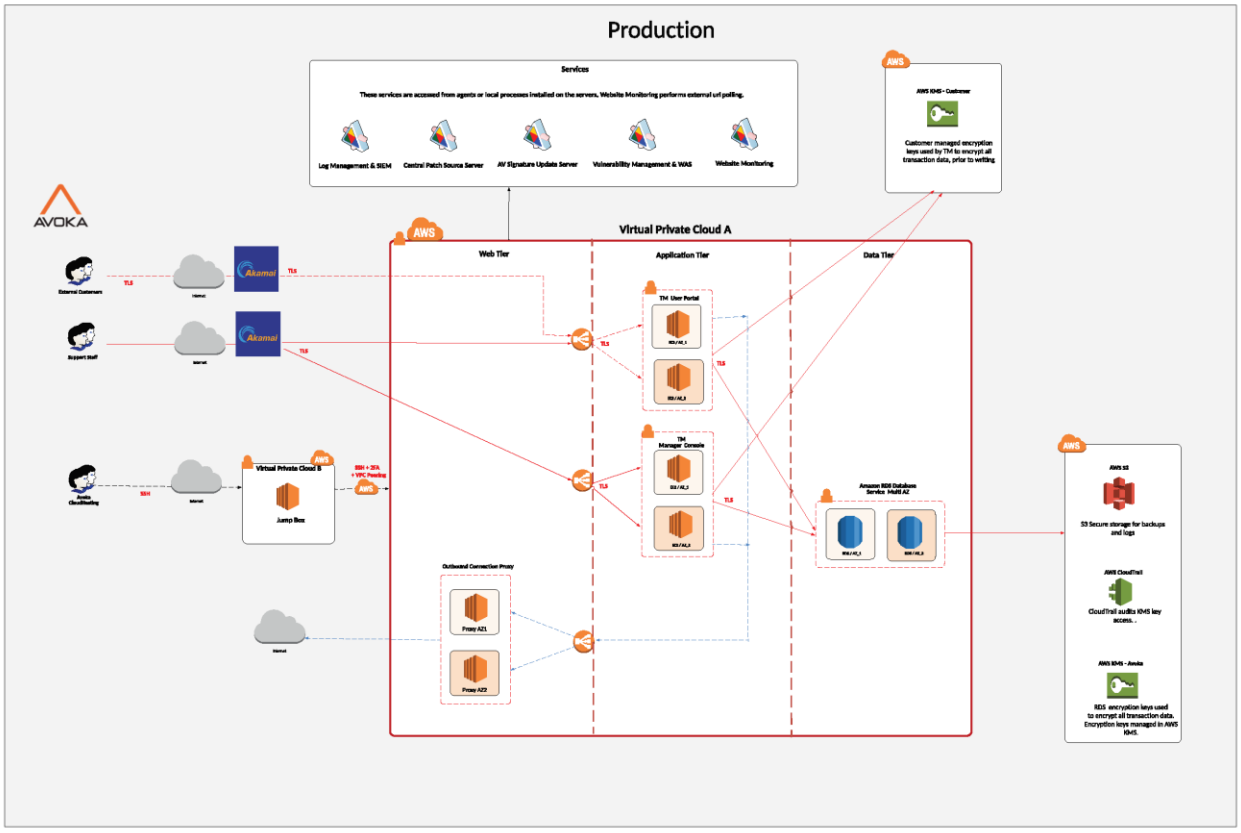
2.9.5. Journey Manager

CWB will enter into an agreement with Temenos to host and manage the Digital Onboarding application on behalf of CWB. Temenos recommends several different deployment alternatives and are also able to customize any deployment to meet specific client requirements. At this time, Temenos is only prepared to host the application in AWS. Future deployment options will include Azure; however, this deployment option is not considered here since the Temenos cloud hosting team is not yet able to certify it for general use.

The pros/cons of each option are articulated in detail by the the Architectural Decision – Digital Onboarding Production Hosting document. Architecture / Security Teams recommend the adoption of **Alternative 1: Virtual Data Centre (VDC)** with the following additional recommendations:

- Hosting must be limited to Canadian Datacentres
- Akamai will be adopted for WAF, CDN, IP Whitelisting (inbound), DoS, DDoS, Country Blocking, etc.
- AWS Key Management Services (KMS) to be isolated to an account only accessible to CWB. CWB will manage keys related to the digital onboarding solution.
- Separate application servers are required for internal customer support staff functions. Access must be restricted to CWB IPs and only authorized CWB personnel can access this endpoint with a MFA challenge.
- CWB will organize annual independent PEN testing
- Temenos Journey Manager to CWB network connectivity will continue utilizing SSL encrypted traffic over the internet with IP Whitelisting and API security controls.
- Temenos Journey Manager Security Audit Logs, Event Logs, System Health Events, Error Logs, etc. must be routed to CWB for integration into the SIEM and any other relevant system.
- *CWB should strive to integrate this with Okta as soon as possible. Enhanced API security controls leveraging Okta's API security capabilities will be leveraged once this component is available.*

The formal decision and guidance is found in the Architectural Decisions section of this document.



2.9.6. Directory and Identity Services

2.9.6.1. DNS

The Journey Manager front end domain will be hosted by AWS Route 53.

CWB APIs expose a domain and API endpoints to the Journey Manager platform. The CWB Cloudflare DNS is used for all public facing domains.

2.9.6.2. Active Directory

The employee facing component of Temenos Journey Manager (workspaces) will initially utilize the authentication capabilities of the Journey Manager Platform. Integration with Okta or Azure AD were discussed, but the Identity and Access Management team has agreed to delay integration with the

Employee IAM component until Okta has been operationalized. The IAM team is responsible for prioritizing applications for migration to Okta.

The customer facing application is unauthenticated since the purpose is to onboard new customers. The final step of the onboarding journey flow is the creation of customer credentials in T24. The customer repository will migrate to Okta in a future project.

2.9.6.3. User Accounts / Group Name

The Avoka Transaction Manager provides a roles and permissions based security authorization model for system administration functions. Organization administrative users can belong to multiple roles, which in turn contain a series of permissions that will enable these user to access components of the TM Management Console.

The Management Console permission sets are highly configurable with over 140 separate view, edit and remove permissions for key system functions.

Roles and permissions will be defined and configured in consultation with the CWBFG Identity and Access Management practice.

2.9.6.4. Service Accounts

Accounts/groups should be unique to each environment (DEV, TEST, PROD). Naming standard to be applied by the IO group.

Account Purpose	Active Directory Accounts	Password Managed
SFTP Batch Integration Script	TBD	Active Directory

2.9.7. Firewall Rules

2.9.7.1. Partner QA, CWB SIT, CWB UAT and Production

The rules should be applicable for Partner QA, CWB SIT, CWB UAT and Production environments.

Table 5 Firewall Ports

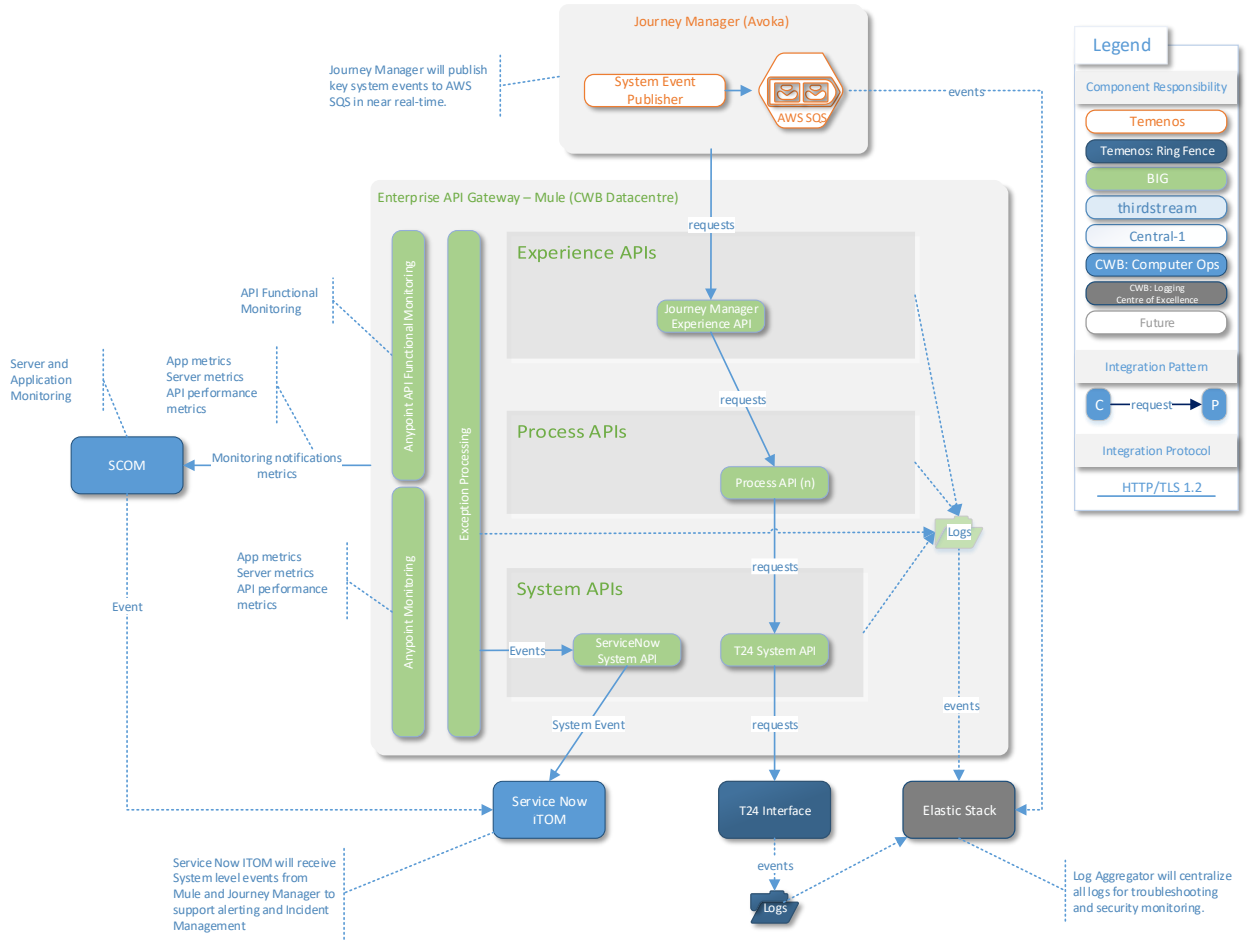
FIREWALL PORTS					
Source Address	**Source Ports**	**Destination Address**	**Destination Ports**	**Direction**	**Purpose**
Administration					
Inter nodes communication					
Temenos Journey Manager (aka Avoka Transact)	>1023	Citrix Load Balancer (External – DMZ Confidential)	HTTPS	Uni	Integration
Citrix Load Balancer (External)	>1023	Citrix Load Balancer (Internal - Production)	HTTPS	Uni	Integration
SFTP Server	>1023	Enterprise Storage (SAN)	SMB	Uni	Integration
Mule Runtime	>1023	Citrix Load Balancer (Internal)	HTTPS	Uni	Integration
Mule Runtime	>1023	Citrix Load Balancer (Internal)	4000-4002	Uni	Integration (ISO8583 Messaging Protocol)
Comp Ops Server	>1023	Citrix Load Balancer (Internal)	HTTPS	Uni	Integration
Comp Ops Server	>1023	Enterprise Storage (SAN)	SMB	Uni	Integration
Citrix Load Balancer (Internal)	>1023	Mule Runtime (App Web Confidential)	HTTPS	Uni	Integration
Citrix Load Balancer (Internal)	>1023	T24 SOAP Interface Server	HTTPS	Uni	Integration
Citrix Load Balancer (Internal)	>1023	ISO8583 Interface Server	4000-4002	Uni	Integration (ISO8583 Messaging Protocol)
Citrix Load Balancer (Internal)	>1023	Filenet	HTTPS	Uni	Integration
Services and Resources					
Internet					
Mule Runtime	>1023	Flinks	HTTPS	Uni	Integration
Mule Runtime	>1023	Thirdstream	HTTPS	Uni	Integration
Temenos Journey Manager (aka Avoka Transact)	>1023	SFTP Server	SFTPs	Uni	Integration
Security and Logging Services					
Mule Runtime Servers	>1023	Syslog Server Elastic	UDP/20514, TCP/1468	Uni	Syslog - Elastic
			TCP/6514	Uni	Secure Syslog
		nms.cwb.local	TCP/22	Uni	SFTP
Directory Services					

Mule Runtime Servers	>1023	dc1.cwb.local dc2.cwb.local d4-dc1.cwb.loca	AD	Uni	AD, Windows services
			NTP	Uni	Time service
		ica.cwb.local	TCP/9090	Uni	CA PKI
			OSCP	Uni	CRL, OSCP
			SCEP	Uni	CRL, OSCP
		dc1.cwb.local dc2.cwb.local d4-dc1.cwb.loca	DNS	Uni	DNS
		ntp.cwb.local	UDP/123	Uni	NTP
Email and Communication Services					
Temenos Journey Manager (aka Avoka Transact)		Proofpoint SMTP Relay	TCP/25		SMTPs
Monitoring					
SCOMM	>1023	Mule	scomm	Uni	Monitoring
Email and Communication Services					
Avoka Transact		Proofpoint	TCP/25	Uni	SMTPS Relay

3. System Management Design

3.1. Monitoring, Logging, Traceability and Incident Management

3.1.1. Overview Diagram



3.1.2. Logging & API Traceability

Journey Manager will produce two unique IDs to help with the end-to-end correlation of log records. These two IDs are described as follows:

- Tracking Code – Represents the unique Reference ID generated for each customer application.
- Request Correlation ID – Represents the unique UUID generated for each API request.

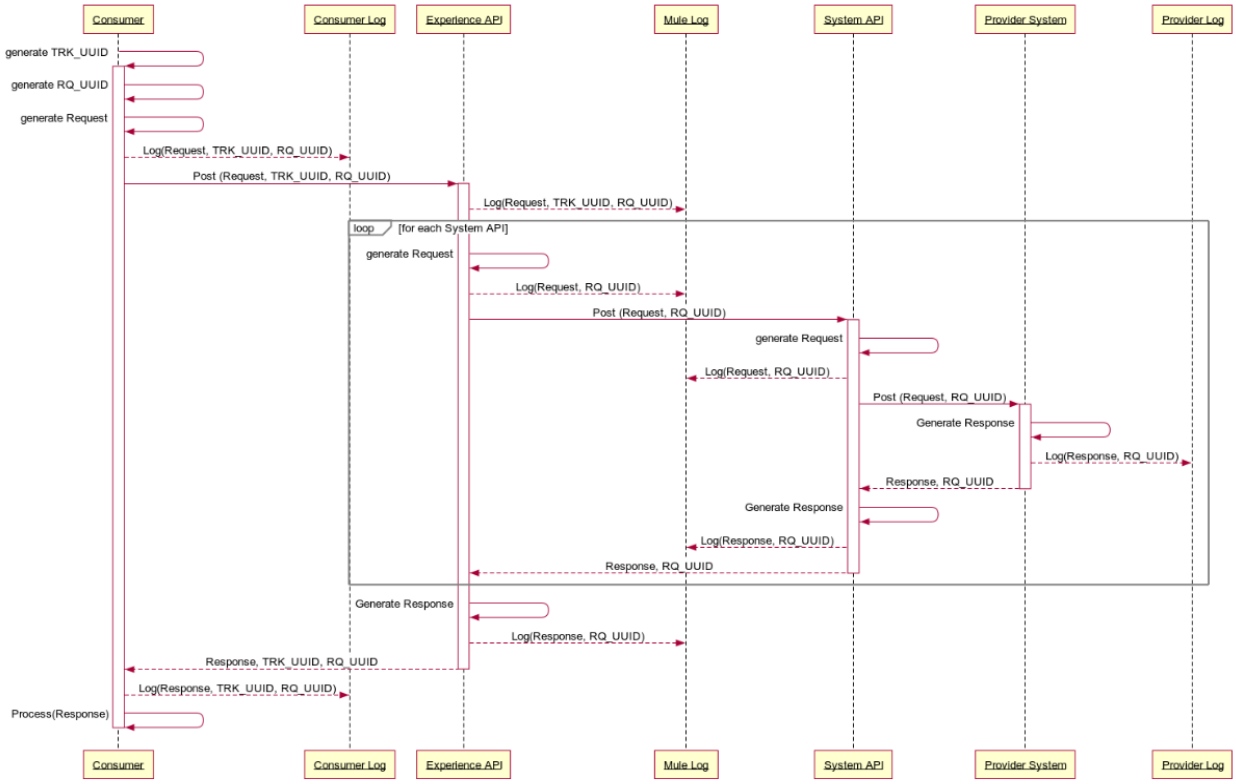
These two values will be submitted by Journey Manager as HTTP header values with each API request to Mule. Ideally the two values are written to the log as two separated values. If this isn't possible, then it is acceptable to combine them into one value. When doing so, the values must be separated by a pipe (vertical bar) delimiter (i.e. "|").

Mule will receive the Tracking Code and Request Correlation ID in the HTTP header and will log both values at the Experience API level. The Request Correlation ID will be passed to all downstream APIs (Process API, System API, Provider API) and included in logs at each level.

Mule will also send the Request Correlation ID with each T24 request (Provider API). The T24 Interface will log this value as part of the T24 Interface logs.

The Elastic Search Stack will aggregate all logs from Journey Manager, Mule and the T24 Interface and effectively stitch together the logs, presenting an end-to-end flow of log activity.

3.1.2.1. Sequence Diagram



3.1.2.2. Sequence Description

The following sequence describes the responsibilities of each component in logging the tracking and request correlation IDs and passing the value(s) on to the next downstream component.

1. Journey Manager generates a Tracking Code (TRK_UUID) for a new customer application
2. Journey Manager generates the necessary API requests
3. For each request
    a. Journey Manager generates a Request Correlation ID (RQ_UUID)
    b. Journey Manager logs the request meta-data, TRK_UUID and RQ_UUID
    c. Journey Manager submits the request along with the TRK_UUID and RQ_UUID to Mule
    d. Experience API logs the request meta-data, TRK_UUID and RQ_UUID
    e. Experience API repeats the following for each System API call
        i. Generate the System Request
        ii. Experience API logs the request meta-data and RQ_UUID
        iii. Experience API calls the System API with the RQ_UUID
        iv. System API generates the provider request
        v. System API logs the request meta-data and RQ_UUID
        vi. System API calls the provider API with the RQ_UUID
        vii. Provider API generates a response
        viii. Provider logs the response meta-data and RQ_UUID
        ix. Provider API returns the response to the System API
        x. System API receives the response

xi. System API generates a response
xii. System API logs the response meta-data and RQ_UUID
xiii. System API returns the response to the Experience API
xiv. Experience API receives the response

f. Experience API generates a response for Journey Manager
g. Experience API logs the response meta-data and RQ_UUID
h. Exerience API sends response to Journey Manager
i. Journey Manager receives the response
j. Journey Manager logs the response meta-data, TRK_UUID and RQ_UUID
k. Journey Manager processes the response

3.1.2.3. Mule Logging Guidance

Log errors, warnings, information and debug messages with standardized attributes, including relevant information (when, where, who, what) about the requests/responses in human readable AND machine parsable format. The following minimum information should be provided for troubleshooting purposes:

- HTTP Header Information (including TRK_UUID, RQ_UUID where possible)
- HTTP Query Parameters
- HTTP Response Code
- Log Date and Time (use a standard date and time format (ISO8601)
- Event Date and Time (use a standard date and time format (ISO8601)
- Application Identifier (e.g. Journey Manager – Motive)
- Application Version (e.g. 1.1.1)
- Environment (e.g. Production)
- Application Address (cluster/host name, or server IP address and port number)
- API/Resource Name
- Request Direction (Akova -> Mule | Mule -> Akova), a.k.a. Request or Response, remember we aren't logging at the HTTP layer just the message bodies
- Payload/Meta-data (See guidance on *Sensitive Information* below)

- Sensitive Information should not be logged. In some cases partial masking or hashing of data may be permissible to help with troubleshooting purposes, in which cases the word "masked" or "hashed" will be included in the list below. These exceptions should be discussed with Architecture and Security. Data not to include in logs include:
  - Application source code
  - Session identification values (hashed)
  - Access tokens
  - Sensitive personal data and some forms of personally identifiable information (PII)

- Authentication passwords
- Database connection strings
- Encryption keys and other master secrets
- Bank account or payment card holder data (masked)
- Data of a higher security classification than the logging system is allowed to store
- Commercially-sensitive information
- Information it is illegal to collect in the relevant jurisdictions
- Information a user has opted out of collection, or not consented to e.g. use of do not track, or where consent to collect has expired

3.1.3. Monitoring

3.1.3.1. Mule – Native Monitoring

As part of Anypoint Platform, Anypoint Monitoring provides visibility into integrations across the CWB app network. The monitoring tools provide feedback from Mule flows and components in the app network.

Operations and development teams will use the monitoring tools to diagnose issues and prescribe solutions to behavior that negatively impacts digital performance. The monitoring tools are designed to reduce the time to identify and resolve these issues through aggregated metrics, data visualization tools, alerts for issues, and a log aggregation system. Specifically, Anypoint Monitoring provides ways to:

- Aggregate and map metrics across dependent systems in real-time.
- Configure dashboards and alerts to reduce the mean time to identification of issues (MTTI).
- Store and search log data at scale.

3.1.3.2. Mule - API Functional Monitoring

The Mulesoft API Functional Monitoring solution enables developers and operators to perform consistent testing of the functional behavior and performance of CWB APIs, throughout the API lifecycle, in testing and production environments.

The solution helps you carry out the following tasks:

- White-box testing: This type of testing validates the behavior of individual APIs against the understanding of how their internals work. As part of this type of testing, you mock and simulate dependencies (for example, back-end systems and other APIs).
- Black-box testing: This type of testing validates the overall behavior of an API and its real/live dependencies as a whole, based purely on inputs and outputs (i.e. without knowing or altering the API internals - no simulation or mocking).
- Runtime monitoring: This type of monitoring ensures that deployed APIs are operating within expected performance in production environments. It makes use of behavioral test cases that use real inputs and expected outputs, and exercise dependencies, as in black-box testing.

CWB will leverage **Runtime monitoring** to validate the expected performance in a production environment. APIs monitored for this purpose must provide a set of *non-destructive data* that can be utilized to test the functionality of the API, but not impact downstream provider systems.

3.1.3.3. Mule – Alerting

The CWB Integration team will define and trigger alerts based on rules (or thresholds) and policies for CWB API resources. When these thresholds are crossed for a certain period of time, CWB will receive notification to take action.

All Mule generated alerts will be routed to the ServiceNow IT Operations Management module to enable centralized incident management. The Mulesoft ServiceNow connector will be leveraged to integrate with ServiceNow and create events upon which the SericeNow (based on configuration management) can update relevant dashboards, determine if an incident should be auto-generated or if a manual review is required before an incident is created.

3.1.3.4. Mule – SCOM Monitoring

Java Application Performance Monitoring (APM) in System Center - Operations Manager lets you monitor Java applications to get details about application performance and exception events that can help determine the root causes of problems. The System Center Management Pack for Java Application Performance Monitoring lets you monitor Java application performance and exception events by using Operations Manager Application Advisor. With Operations Manager Application Advisor, you can investigate method and resource timing for performance events, stack traces for exception events, Java-specific counters for events (such as Average Request Time, Requests Per Second, JVM Memory, and Class Loader), and run some of the standard Application Performance Monitoring reports.

3.1.3.5. Mule – ServiceNow Integration

The Event Management application is part of the IT Operations Management (ITOM) area, which also covers CMDB Discovery, Service Mapping and Orchestration. With the Event Management application CWB integrates multiple monitoring sources, and create ServiceNow events out of it.

SCOM will be integrated in this fashion to provide meaningful dashboards to operational staff and ensure there is a fulsome view of application and server health for the Mule runtime and Mule applications.

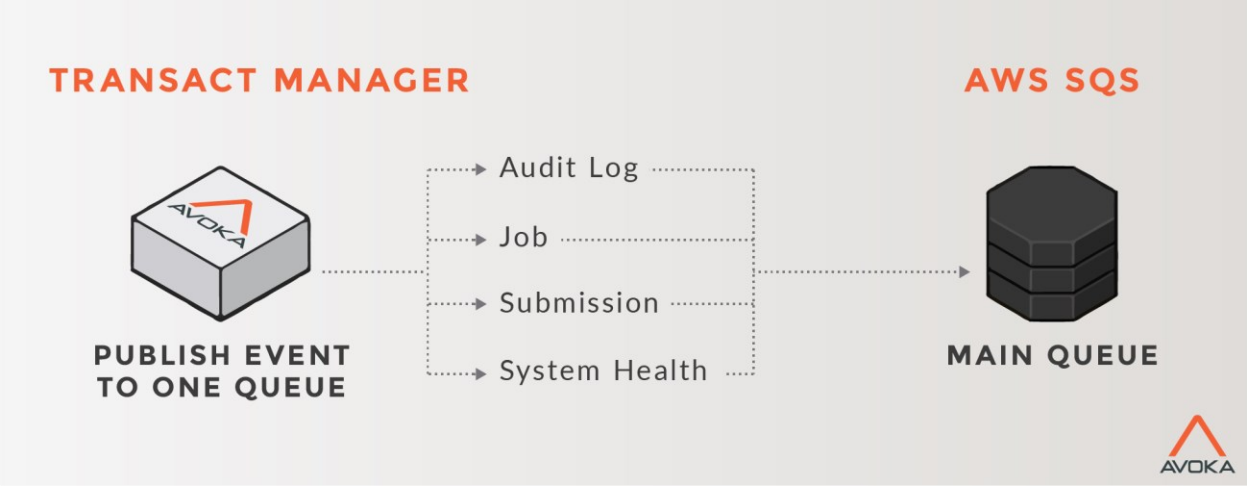
3.1.3.6. Mule - Health Check

A health check endpoint will be defined that can be used by systems to verify that a Mule runtime is operational and can accept new requests. Ideally, the health check will also provide additional details that can be leveraged by advanced load balancers to route requests to instances that are not only healthy, but are in the best position to accept the next request (e.g. combination of lowest: CPU utilization, memory utilization, response times, etc.)

3.2. Log Aggregator Integration

All logs will be aggregated by the Elastic Stack in near real-time. The Elastic Stack will be configured to read events from the AWS SQS queue (see SQS Input Plugin), Mule servers (see Filebeat) and T24 logs and indexed as required for both the Security Operations and Digital Technology Services Teams. The Digital Technology Services team will write queries to correlate and show the full relationship between Journey Manager, Mulesoft and T24 transaction logs. See the Logging & API Traceabilty section for further details on how transactions across systems are correlated.

The Journey Manager System Event Publisher will publish key system events to a **single** AWS SQS event queue, one for **production** and another for **all non-production** environments. The CWB Elastic instance will pop off events from this queue at a pace it can manage, parse the messages and store the content as required for indexing, searching and reporting.



Connectivity to SQS from the CWB Elastic Stack must be secured in transit via TLS 1.2 and encrypted at rest. Access to this data must also be restricted by role and limited to a small subset of CWB employees on a need to know basis. Special care must be taken to follow the CWB Data Protection Standard [2] to ensure sensitive customer data is handled according to this standard.

Event types supported by Journey Manager are summarized below (reference), along with the CWB party that derives the most value from consuming, indexing and searching the event.

Event Type	Interested Party	
	Security Operations	Digital Technology Services
Audit Logs	High value	Low value
Collaboration Job Events	Low value	Low value
Transaction Events	High value	Low value
System Health Events	Low value	High value
User Authentication Events	High value	High value

Event messages are published in JSON format as defined by the System Event Publisher specification.

3.3. Service Level

Refer to **APPENDIX E - Service Level Objectives Responsibility Matrix** for more details.

AVAILABILITY AND PERFORMANCE STANDARDS

[2] See Keylight GRC Platform

Network Area	Availability Target	Measurement Method	Avg. Network Resp. Time Target	Acceptable Resp. Time	Response Time
LAN	99.99%	Impacted user minutes	Under 5 ms	10 ms	Round-trip ping response
WAN	99.99%	Impacted user minutes	Under 100 ms	150 ms	Round-trip ping response

3.4. Service Priority

SLA-SLO MATRIX			
Priority	**Response Time**	**Resolution Time**	**Penalty**
Medium -2	15 min	24 hrs	NA

3.5. Systems Management

3.5.1. Application Management

The Mule systems are managed via the application servers' web interface. Journey Manager (From Temenos/Avoka) will be managed by Temenos/Accutive directly.

3.5.2. Infrastructure Management

Following infrastructure management systems are required to be setup and used to access and monitor the Mule and Avoka Journey Manager environments.

SERVICE MANAGEMENT TOOLS		
Process	**Yes/No**	**Tools**
System access management required?	Yes	
Events and/or fault management required?	Yes	
System performance monitoring required?	Yes	
Application performance monitoring required?	Yes	
Configuration management required?	Yes	
Asset management required?	Yes	
Identity and access management required?	Yes	

3.6. Service and Process Automation Capabilities

SERVICE AND PROCESS AUTOMATION CAPABILITIES				
Service Function / Process Name	**Purpose**	**Interface**	**Dependencies**	**Comments**
NA	NA	NA	NA	NA

3.7. Business Continuity

3.7.1. Backup and Restore

Refer to **APPENDIX E Service Level Objectives Responsibility Matrix** for more details.

3.7.2. Disaster Recovery

Refer to **APPENDIX E Service Level Objectives Responsibility Matrix** for more details.

3.7.3. Data Retention Policy

Refer to **APPENDIX E Service Level Objectives Responsibility Matrix** for more details.

4. Approvals

Name, Position	Name, Position
Date	Date

4.1. Prerequisites for Detailed Infrastructure Design

Project Name	
Project Manager	
ARB Oversight?	Yes / No
Was architecture engaged in Business Case or Project Charter development?	Yes / No
Architecture TRB Oversight?	Yes / No
Are all required licenses accounted for?	Yes / No

Document	Document name / location of document	Status	Provided (Y/N/NA)
Approved Business Case?			
Approved Functional & Nonfunctional Requirements Document			
High Level Solution Design			
Project Code			

5. Appendices

APPENDIX A. Infrastructure Servers

Infrastructure Services			
Servers	**Primary Site**	**DR Site**	
DNS Domain	cwb.local	cwb.local	
Primary Name server	dc1.cwb.local	-dc1.cwb.local	
Secondary Name server	dc2.cwb.local	-dc2.cwb.local	
Primary NTP server	ntp.cwb.local	ntp.cwb.local	
Secondary NTP server	dc2.cwb.local	-dc2.cwb.local	
Time Zone	Mountain Time (US & Canada)	Mountain Time (US & Canada)	
SFTP/FTP Server	nms.cwb.local	nms.cwb.local	
Root CA	ica.cwb.local	ica.cwb.local	
Domain Controllers	dc1.cwb.local dc2.cwb.local d4-dc1.cwb.local	dc1.cwb.local dc2.cwb.local d4-dc1.cwb.local	

APPENDIX B. Drive Mapping

See the Environments section for specifics of drive sizes for each application. The table below represents what is typical and can be used if not specifically overwridden in the environments section.

Drive Mapping				
Drive Letter	**Standard Size (GB)**	**dB Server**	**App Server**	**Web Server**
C:	60	OS	OS	OS
E:	80		App Software Data	App Software Data
G:	30	SQL Data		
F:	Depends upon dBs to be hosted	SQL logs		
H:	100			
I:	100	TempLog		
J:	100 (If Required)	TempLog2		
P:	**10**	**Paging**	**Paging**	Paging

APPENDIX D. Glossary

Term	Definition

APPENDIX E. Service Level Objectives Responsibility Matrix

Category ID	Service Level Agreement	SLA Type	DEV	TEST	PROD	Internal (IS) / External (Vendor)
IO	Retain regulatory reports generated by the Wired Application (STR, LCTR, EFT) in read only mode for 6 years.	Storage / Retention			X	Internal
IO	Testing before installation to detect malicious and Trojan code is mandatory ➔ Applicable to both SAS AML and Wired	Security	X		X	Internal
IO	Must be able to scale compute and storage resources to manage an additional 5% growth of records to be processed during the nightly batch and a one-time increase of 60% of records to be processed in the event of a CWBFG acquisition. ➔ Applicable to both SAS AML and Wired	Scalability		X	X	Internal
AMS IO	The test environment must have at least the last 2 years of historical data taken directly from production to permit for realistic testing of AML scenarios. The testing instance should take regular snapshots from production. ➔ Applicable to both SAS AML and Wired Application	Storage		X		Internal
AMS IS Vendor	Any licensing or intellectual property right terms must be documented and understood by CWB AMS, IS and the vendor ➔ Applicable to both SAS AML and Wired Application	Licensing	X	X	X	External
IO	The environment (inclusive of data and configuration) must be backed up on a daily basis as part of standard CWB practices – 5 pm daily. ➔ Applicable to both SAS AML and Wired Application	Backup	X	X	X	Internal
IO	Source: Cory Gould Currently, no timeframe has been committed and is best effort. For non-catastrophic events, recovery time is 4 hours. A catastrophic event is likely days. The business target is 72 hours in the event of a DR event. ➔ Applicable to both SAS AML and Wired Application	Recovery	X	X	X	Internal
IO	Infrastructure: Source: Neil Cory	Uptime	X	X	X	Internal

	Guaranteed uptime of 99.9% (PROD) Unscheduled downtimes of: Daily: 1m 24s Weekly: 10m 5s Monthly: 43m 48s Yearly: 8hy 45m 57s Non-production environments (DEV, TEST) uptime of 99.9% only during business hours 8x5 *Business requires: 6am x 11pm (DEV, TEST)					
IO	Application must be kept current with SAS AML and the Wired Application patches.	Maintenance - Patches	X	X	X	Internal
AMS DSS/IM	AMS Support Agreement: Please refer to CWB IS Standard Defect & Release Process	Issue Resolution	X	X	X	Internal

References

5.1. Infinity Reference Architecture

Infinity Reference Architecture - Nov 2

5.2. Temenos Cloud Deployment Options

VDC_Plus_20190704.pdf

VDC-KMS_20190725.pdf

Journey Manager VDC vs VDC+ - Feat

5.3. Temenos Journey Manager Platform

Online Platform References

5.4. Temenos Security Architecture

Avoka_Security_Architecture_1805.pdf