# 1. Overview

## Content:

This document outlines the design and architecture of the Blue Prism Robotic Process Automation (RPA) solution to be developed. It covers key components including:

### Case Management:

Implementation of workflows in Blue Prism to manage case processes and track progress using Blue Prism's case management capabilities. The use of Blue Prism's robotic solutions enables monitoring and management of automation through its platform.

### Business Rules:

Utilization of Blue Prism to automate business processes and enforce rules through business logic implemented via Blue Prism's decision-making capabilities, including calculations, expressions, and decision stages. Blue Prism's visual process design environment allows for efficient workflow design and logic implementation.

### User Interface:

Blue Prism RPA focuses on automation while providing capabilities to interact with user interfaces through Blue Prism's Application Modeller and UI Automation tools. This enables the automation of backend processes that enhance user interactions across various applications integrated within the Blue Prism ecosystem.

### Integration:

Connecting various data sources and services using Blue Prism’s connectors and integration capabilities. This ensures seamless data flow across applications and services through integrations with APIs, external databases, and other enterprise systems.

### Security:

Implementation of role-based access control and data security measures within Blue Prism, ensuring that only authorized users can execute robotic workflows and access sensitive data. Blue Prism’s platform provides robust access management features to safeguard automation processes.

### Deployment:

Strategies for deploying automated workflows using Blue Prism's deployment tools, along with managing the application lifecycle through best practices for maintaining and updating RPA projects within the Blue Prism ecosystem. This includes version control and environment management to ensure smooth transitions during updates.

# 2. User Authentication

# Blue Prism Design: User Authentication

## 1. Login

Authentication Method:

Users will authenticate using their enterprise LDAP credentials integrated with Azure Active Directory (AAD) for seamless authentication. This will be achieved by creating a Blue Prism process that interacts with the Azure AD API to validate user credentials.

### Implementation Steps:

## 1. HTTP Request Action:

* Use the HTTP Request action in Blue Prism to configure a request to the Azure AD API for user authentication.
* Pass the user credentials securely (using parameters) for validation.

## 2. Response Handling:

* Use a Decision stage to evaluate the API response and determine if the authentication was successful.
* Depending on the response, either proceed to the next step or prompt an error message.

## 2. Password Policy

Requirements:

* Minimum length: 8 characters
* Must include:
* At least one uppercase letter
* At least one lowercase letter
* At least one digit
* At least one special character

### Implementation Steps:

## 1. Define Password Validation Logic:

* Use a Calculation stage to define regex patterns for password validation.
* Create a Process to capture and process registration data, utilizing Data Items to hold the input values.

## 2. Enforce Password Policy:

* Implement a Decision stage to check the password against the policy before proceeding with user registration.

## 3. Multi-Factor Authentication (MFA)

Verification Method:

A One-Time Password (OTP) will be sent via email or SMS for additional verification.

### Implementation Steps:

## 1. Configure Azure MFA:

* Set up Azure Multi-Factor Authentication settings in Azure AD as required.

## 2. Send OTP:

* Use the Send Email action to send the OTP via email.
* For SMS notifications, integrate with a third-party service like Twilio by using a suitable API within a Business Object.

## 3. OTP Generation Workflow:

* Create a Process that generates the OTP (using a Calculation stage) and triggers the sending mechanism.

## 4. Session Timeout

Configuration:

Implement a session timeout of 15 minutes after inactivity.

### Implementation Steps:

## 1. Monitor User Activity:

* Use a Timer stage to track user activity within the application.

## 2. Log User Activity:

* Implement a Logging mechanism (e.g., write to a database or log file) to monitor user interactions.

## 3. Session Timeout Trigger:

* If no activity is detected for 15 minutes, use an Action stage to invoke a workflow that logs out the user or updates their session status appropriately.

## 5. Account Lockout

Policy:

User accounts will be locked after 5 failed login attempts.

### Implementation Steps:

## 1. Track Login Attempts:

* Create a Data Item (e.g., Counter) to keep track of the number of failed login attempts.

## 2. Log Failed Attempts:

* Use a Database action to log each failed attempt.

## 3. Implement Lockout Logic:

* Use a Decision stage to check if the count reaches 5.
* If the threshold is met, execute an Action stage to lock the account (e.g., update the user status in the database or send a notification to an admin using the Send Email action).

This Blue Prism design replicates the user authentication functionalities originally defined in the Pega RPA design.