­­­­­

|  |  |
| --- | --- |
|  |  |



Solution Design

Document

Table of Contents

[I. Purpose 3](#_Toc5787525)

[II. Automated process details 4](#_Toc5787528)

[3 Runtime guide 5](#_Toc5787529)

[3.1 Architectural structure of the Master Project 5](#_Toc5787530)

[3.2 Master Project Runtime Details 5](#_Toc5787531)

[3.3 Project name 1 6](#_Toc5787532)

[3.4 Project(s) workflows 6](#_Toc5787533)

[3.5 Packages 7](#_Toc5787534)

[3.6 Architectural structure of the Master Project 7](#_Toc5787535)

[4 Other Details 8](#_Toc5787536)

[Future Improvements 8](#_Toc5787537)

[Other Remarks 8](#_Toc5787538)

[5 Glossary 9](#_Toc5787539)

# Purpose



Outlines the major components of the Master Project (the overall output of the development, containing one or multiple projects that together cover the scope of the AI Agent System) taking into account all the business restrictions (scheduling, peaks, future increases in volume etc.). The focus of the Solution Architect will be on:

* Robustness;
* Scalability;
* Efficiency;
* Replicability

The information herein is targeted primarily at the developers that will initially implement the solution and subsequently at the support developers in case of change requests.

Processing Pipeline  
  
1. Business Goal:  
The primary business goal of this process is to ensure that important encrypted or protected emails are properly documented and saved for future reference or legal purposes. By capturing screenshots of the full email content and forwarding them to oneself, a permanent record is maintained even if the original sender deletes the email after a certain time period. This is crucial in situations where the emails may be needed as evidence in court or for other official documentation needs.  
  
2. Best Way to Accomplish This Business Goal:  
While the current process of manually taking screenshots and forwarding emails to oneself does achieve the business goal, there are some potential improvements to make it more efficient and reliable:  
  
1. Automate the screenshot capture process using an Outlook add-in or third-party tool that can detect encrypted/protected emails and automatically take screenshots.  
  
2. Implement a secure document management system or encrypted storage solution to save the email screenshots, rather than relying on the Sent folder. This provides better organization, search capabilities, and protection.  
  
3. Establish a clear naming convention and metadata tagging system for the saved email screenshots to make them easier to find and reference later.  
  
4. Provide training or clear documentation to all relevant staff on the proper process to follow, including any updates or improvements made.  
  
5. Regularly test and validate that the process is being followed correctly and that the necessary emails are being properly captured and saved.  
  
3. How AI Agents Could Improve the Process:  
An AI-powered solution could significantly streamline and automate this process:  
  
a. An AI agent could be trained to automatically detect incoming encrypted or protected emails based on keywords or patterns in the subject line or email body.  
  
b. Once detected, the AI could automatically log in to the encrypted server using stored credentials (securely managed) and open the message.  
  
c. The AI could then capture a screenshot of the email content using an API or built-in functionality.  
  
d. Optical Character Recognition (OCR) could be applied to the screenshot to extract the text content and key metadata like sender, recipient, date, etc.  
  
e. The AI could then automatically save the screenshot and extracted data into a designated secure storage system, applying the appropriate naming convention and tags.  
  
f. If needed, the AI could also forward the original email with the screenshot to a designated email address or distribution list for redundancy.  
  
g. Regular reports or notifications could be generated by the AI to confirm that the process is running smoothly and all necessary emails are being captured.  
  
By automating these steps with an AI agent, the process becomes much more efficient, reliable, and less prone to human error. It also frees up staff time to focus on higher-value tasks. Of course, proper testing, monitoring, and periodic auditing of the AI system would be needed to ensure it continues to meet the business goals over time.  
  
4. AI Agent High-level Steps:  
  
a. Step 1: Detect incoming encrypted or protected emails  
 i. Reasoning: The AI agent would need to be trained on identifying specific patterns, keywords, or indicators in the email subject line or body that suggest it is an encrypted or protected message. This could involve techniques like regular expressions, keyword matching, or even more advanced natural language processing to understand the context. Once trained, the AI agent can continuously monitor the incoming email feed and flag the relevant messages.  
 ii. Complexity: 3 - Moderate complexity. While pattern matching and keyword detection are relatively straightforward, properly training the AI to minimize false positives and negatives could require significant effort and fine-tuning. The complexity increases if more advanced NLP techniques are needed to understand context.  
  
b. Step 2: Automatically log in to the encrypted server and open the message  
 i. Reasoning: To automate the process of accessing the encrypted email content, the AI agent would need to be able to navigate to the appropriate login page or portal based on the email's instructions, enter the necessary credentials (securely stored and managed), and then follow the steps to open the message. This could involve interacting with various UI elements and handling different login flows or authentication methods.  
 ii. Complexity: 4 - High complexity. Automating the login and message opening process could be quite complex, as the AI would need to handle a variety of different encrypted email providers, each with their own unique interfaces and authentication flows. Properly securing and managing the login credentials is also a significant challenge. The AI would need to be quite robust and flexible to handle different scenarios and edge cases.  
  
c. Step 3: Capture a screenshot of the email content  
 i. Reasoning: Once the encrypted email is opened, the AI agent would need to programmatically capture a screenshot of the full email content. This could be done using various APIs or libraries that allow for screen capture and image manipulation. The AI would need to ensure that the entire relevant content is captured in the screenshot, adjusting for different email lengths, layouts, or dynamic content.  
 ii. Complexity: 2 - Low complexity. Capturing screenshots programmatically is a relatively straightforward task with many existing tools and libraries available. The main challenge would be ensuring that the full relevant content is captured and any sensitive or irrelevant information is excluded.  
  
d. Step 4: Extract key metadata and content from the screenshot  
 i. Reasoning: To make the captured email data more useful and searchable, the AI agent could apply OCR (Optical Character Recognition) techniques to extract the text content from the screenshot. It could also use regular expressions or NLP to identify and extract key metadata like sender, recipient, date, subject line, etc. This extracted data could then be used for tagging, categorization, and search indexing.  
 ii. Complexity: 4 - High complexity. While basic OCR is fairly mature, accurately extracting all the relevant text and metadata from an email screenshot could be quite challenging, especially handling different email formats, layouts, inline images, and other variations. More advanced techniques like layout analysis and named entity recognition may be needed. Ensuring high accuracy and handling edge cases would require significant training and tuning.  
  
e. Step 5: Save the screenshot and extracted data into a secure storage system  
 i. Reasoning: The AI agent would need to programmatically save the captured screenshot image and the extracted text/metadata into a designated secure storage system. This could be a secure database, encrypted file storage, or document management system. The AI would need to follow a predefined naming convention and apply the appropriate tags or categories based on the extracted metadata. Proper access controls and encryption would need to be applied to ensure the stored data remains secure.  
 ii. Complexity: 3 - Moderate complexity. Saving files and data programmatically is generally straightforward, but the complexity lies in ensuring proper security measures are applied, access is properly managed, and the storage system can scale to handle the volume of data. Integration with the chosen storage system and applying consistent naming and tagging conventions could also require significant upfront design and testing.  
  
f. Step 6: Generate reports and notifications on process status and results  
 i. Reasoning: To provide visibility and confidence in the automated email capture process, the AI agent could generate regular reports and notifications on the status and results. This could include metrics like the number of encrypted emails detected, successfully captured, and stored, as well as any errors or exceptions encountered. Notifications could be sent to designated recipients if any issues or anomalies are detected that require manual intervention.  
 ii. Complexity: 2 - Low complexity. Generating basic reports and notifications based on predefined templates and triggers is a relatively simple task for an AI agent. The main challenge would be defining the appropriate metrics, thresholds, and notification rules to ensure that the reports are meaningful and actionable. Integration with the chosen reporting and notification tools could also add some complexity.  
  
5. Process trigger:  
The process trigger for the AI agent to start handling an encrypted or protected email would be the receipt of such an email in the designated monitored inbox. As soon as an email matching the predefined criteria (e.g., keywords, patterns) is detected in the incoming email stream, the AI agent would initiate the automated process of logging in, capturing the content, extracting data, and saving it to the secure storage system.  
  
6. Human Involvement:  
Based on the provided process description, human involvement can be minimized to mainly oversight and exception handling roles, assuming the AI agent is properly set up, trained, and tested. Here are a couple of key areas where human involvement may still be required:  
  
a. Involvement 1: Handling exceptions and errors  
 In cases where the AI agent encounters an error or exception that it is not able to handle automatically (e.g., a new login flow or authentication method, an encrypted email format that it hasn't seen before), human intervention may be required. The AI agent should be designed to detect these exceptions and send a notification to a designated human operator or team, who can then manually review the issue and provide guidance or update the AI agent's training as needed. The human operator would also need to manually handle that particular email to ensure it gets properly captured and stored.  
  
b. Involvement 2: Periodic auditing and quality control  
 While the AI agent can automate the day-to-day processing of encrypted emails, it is important to have human oversight to ensure that the process continues to meet the business requirements and quality standards over time. This could involve periodic audits where a human operator manually reviews a sample of the captured emails to ensure that the content and metadata are being accurately captured and stored, and that the appropriate security measures are being applied. The human operator could also review the AI agent's performance metrics and reports to identify any trends or issues that may require further investigation or improvement. If any issues are identified, the human operator would need to work with the AI development team to implement the necessary updates or fixes to the AI agent's configuration or training.  
  
By limiting human involvement to these key oversight and exception handling roles, the overall process can still be largely automated by the AI agent, providing significant efficiency and reliability gains. The human operators can focus their time and attention on the most critical or complex issues, while the AI agent handles the bulk of the day-to-day processing. Of course, the exact level of human involvement required may vary depending on the specific implementation and the complexity of the encrypted emails being handled.  
  
7. Documentation:  
Based on the provided process description, there are a few types of documentation that could be helpful for the AI agent to accomplish its tasks effectively:  
  
a. Encrypted email provider documentation  
 i. Reasoning: To automate the process of logging into the encrypted email servers and opening the messages, the AI agent would need detailed documentation on the login flows, authentication methods, and message retrieval APIs for each of the encrypted email providers that it needs to support. This documentation would provide the necessary technical details and instructions for the AI agent to programmatically interact with these systems.  
 ii. Document name or link (if applicable): This documentation would likely be available on the websites or developer portals of the respective encrypted email providers. The specific links or document names would depend on the providers being supported, but they would likely include titles like "API Reference", "Authentication Guide", or "Integration Documentation".  
  
b. Secure storage system documentation  
 i. Reasoning: To properly save the captured email screenshots and extracted data into the designated secure storage system, the AI agent would need documentation on how to integrate with and use this system. This could include details on the API endpoints, authentication methods, file formats, and metadata schemas supported by the storage system.  
 ii. Document name or link (if applicable): The documentation for the secure storage system would likely be provided by the vendor or developer of that system. It could be available on their website, developer portal, or as part of the system's built-in help documentation. The specific document names and links would depend on the chosen storage system.  
  
c. OCR and NLP library documentation  
 i. Reasoning: To extract the text content and metadata from the email screenshots, the AI agent would likely use existing OCR and NLP libraries or APIs. To effectively use these tools, the AI agent would need documentation on how to integrate with them, what functions and parameters they support, and how to handle different input and output formats.  
 ii. Document name or link (if applicable): The documentation for the OCR and NLP libraries would be provided by the developers of those libraries. This could be available on their websites, GitHub repositories, or as part of the library's built-in documentation. The specific document names and links would depend on the chosen libraries, but could include titles like "API Reference", "User Guide", or "Examples".  
  
Based on the provided process description, there are no specific documentation links or document names mentioned. The description focuses more on the high-level steps and requirements rather than the technical implementation details. However, during the actual development and implementation of the AI agent, the relevant documentation for the specific encrypted email providers, storage systems, and libraries being used would need to be identified and referenced. This documentation may be specified in the detailed technical design or implementation plan for the AI agent.  
  
8. Solution Reasoning:  
The proposed AI-powered solution for automating the handling of encrypted and protected emails is designed to address the key business goal of ensuring proper documentation and preservation of important email content for future reference and legal purposes. By leveraging AI capabilities like pattern recognition, natural language processing, and robotic process automation, the solution can significantly streamline and improve upon the current manual process.  
  
The AI agent can continuously monitor the incoming email stream and automatically detect encrypted or protected messages based on predefined criteria. It can then automate the process of logging into the encrypted email servers, capturing screenshots of the full email content, extracting relevant text and metadata, and saving all the captured data into a secure storage system. This eliminates the need for manual intervention in the day-to-day processing of these emails, reducing the risk of human error and increasing efficiency.  
  
The use of OCR and NLP techniques allows the AI agent to extract structured data from the email screenshots, making it easier to search, categorize, and analyze the captured information later on. The secure storage system ensures that the email data is properly protected and preserved, with appropriate access controls and encryption in place.  
  
To ensure the solution remains effective and reliable over time, human oversight is still required in the form of handling exceptions and conducting periodic audits. This allows for a balance between automation and human judgment, with the AI agent handling the bulk of the workload while humans focus on the most critical or complex issues.  
  
Proper documentation and training data from the relevant encrypted email providers, storage systems, and AI libraries will be essential to the successful implementation of this solution. The AI agent will need to be trained on a diverse set of example emails and scenarios to ensure it can handle the variety of encrypted email formats and edge cases that may arise.  
  
Overall, the proposed AI-powered solution has the potential to significantly improve the efficiency, reliability, and security of the encrypted email handling process, while still maintaining the necessary level of human oversight and judgment. With proper design, implementation, and ongoing maintenance, this solution can help the organization meet its business goals and legal obligations more effectively.

# process details

Details filled in need to reflect the actual information for the Master Project released for production. The following table will be populated:

|  |  |
| --- | --- |
| Item | Description |
| Master Project Name |  |
| Framework used | e.g. 2019.4 |

# Runtime guide

## Architectural structure of the Master Project

Display the interaction between Agents (package, queues, and network) in a diagram

## Master Project Runtime Details

Outlines the details of the automated process by filling in the table below.

|  |  |
| --- | --- |
| ITEM NAME | DESCRIPTION  *Fill in each bolded section - empty fields are not allowed. If the section does not apply to your automation then mark as n/a.* |
| Production environment details | ***Example:*** *Running on Sparky , the virtual backoffice machine. Scheduled every night after the report is generated from Zendesk.* |
| Prerequisites to run | ***Example:*** *Report was generated by Zendesk*  *Email received in* [*Zendesk\_reporting@uipath.com*](mailto:Zendesk_reporting@uipath.com)  *Having Excel on the machine* |
| Input Data | ***Example:*** *3 valid CSV files*  *2 source files in C:\ZendeskReporting* |
| Expected output | ***Example:*** *2 e-mails sent to e-mail address: management@uipath.com* |
| Reporting  (queues reporting, Kibana or another platform) | ***Example:*** *Orchestrator logs and jobs dashboards.* |
| How is Orchestrator used? | ***Example:*** *Orchestrator used for scheduling and asset passwords.* |
| Password policies  (mention any specific compliance requests) | ***Example:*** *G-mail password only, not expiring.* |
| Stored credentials  (Never use hardcoded credentials in the workflow!) | ***Example:*** *Stored in Orchestrator Assets* |

## Project name

|  |  |
| --- | --- |
| ITEM NAME | DESCRIPTION  *Fill in each section - empty fields are not allowed. If the section does not apply to your automation then mark as n/a.* |
| Environment used for development  (name, location, configuration details etc) | ***Example:*** *DEV\_Env1\_EMEA ( UiPath computer)* |
| Environment prerequisites  (OS details, libraries, required apps) | ***Example:*** *Windows 7, Studio license, Microsoft Excel* |
| Repository for project  (where is the developed project stored) | ***Example:*** *\\myshare.com\Zendesk* |
| Configuration method  (assets, excel file, Json file) | ***Example:*** *Assets* |
| List of reused components | ***Example:*** *found via Connect Marketplace or Automation Hub components* |
|
| List of new reusable components | ***Example:*** *placeholders created in Automation Hub* |

Add tables for as many projects as you need and fill them in.

## Project(s) workflows

Workflows specific to: Specify Project Name from section above

For the workflow files defined below please specify the input and output parameters.

|  |  |
| --- | --- |
| Workflow Name | Description |
| Example: Main | ***Example:*** *invokes all the other workflows* |

## Packages

Include the list of packages and high-level description for each of them, to explain their purpose

|  |  |
| --- | --- |
| Package Name | Description |
| *Example: ZendeskReports.1.0.6285.31077.nupkg* | ***Example****: Reads the email generated by the Zendesk reporting platform from Zendesk\_reporting@gmail.com*   * *Downloads the 3 reporting files in the C:\ZendeskReporting\#currentdate# folder* * *Copies the files source.xlsx and source\_fantastic.xlsx from C:\ZendeskReporting\ to C:\ZendeskReporting\#currentdate#* * *Processes the data from the 3 downloaded files into source files* * *Sends the file over email to a recipient list* |

## Agents

Agent\_ID: 1  
Name: Encrypted Email Detector  
Description: This agent is responsible for monitoring the incoming email stream, detecting encrypted or protected emails based on predefined criteria, and triggering the subsequent steps in the process.  
Reasoning:   
Tasks:   
 • Continuously monitor the designated inbox for incoming emails: Complexity: 2  
 • Analyze email subject lines and bodies to identify patterns, keywords, or indicators of encrypted or protected content: Complexity: 3  
 • Flag detected encrypted or protected emails and trigger the Encrypted Email Authenticator agent: Complexity: 2  
 • If the email does not match any predefined criteria but still appears to be encrypted or protected, flag it for human review: Complexity: 2  
 • Incorporate human feedback on false positives or false negatives to improve detection accuracy over time: Complexity: 3  
Type: ReAct  
Context:   
 • Process Description and High-Level Steps document: The agent requires access to the document that outlines the steps for viewing and saving encrypted or protected emails in Outlook, including identifying encrypted emails, to accurately detect and flag relevant emails., [Insert location or URL if explicitly mentioned in the Process Description]  
Inputs:   
Outputs:   
 • Agent 2: Flagged encrypted or protected email details  
Tools: Email Monitoring Tool: To continuously monitor the designated inbox for incoming emails., Email Flagging Tool: To flag detected encrypted or protected emails based on predefined criteria., Human Review Tool: To route emails that do not match predefined criteria but still appear to be encrypted or protected for human review.  
Trigger: The receipt of a new email in the designated monitored inbox.  
Decisions:   
System Prompt: You are an intelligent Encrypted Email Detector agent. Your role is to continuously monitor the designated inbox for incoming emails and detect any encrypted or protected emails based on predefined criteria.  
  
To accomplish this, you will:  
  
1. Use the Email Monitoring Tool to scan all incoming emails in real-time.  
  
2. Analyze the subject lines, bodies, and attachments of each email, looking for specific patterns, keywords, file types, or indicators that suggest the presence of encrypted or protected content. Refer to the Process Description and High-Level Steps document for guidance on identifying these emails.  
  
3. When an encrypted or protected email is detected with high confidence, use the Email Flagging Tool to flag the email and trigger the Encrypted Email Authenticator agent to handle the next steps in the process.  
  
4. If an email does not match the predefined criteria but still appears to be encrypted or protected based on your analysis, assign a confidence score and route it to the Human Review Tool for manual review and decision-making if the score is above a set threshold.  
  
5. Continuously learn and improve your detection accuracy by incorporating feedback from human reviewers on any false positives or false negatives. Update your detection algorithms and criteria based on this feedback.  
  
Your inputs will be the incoming email stream, and your outputs will be the flagged encrypted or protected email details along with confidence scores sent to the Encrypted Email Authenticator agent or Human Review Tool.  
  
Success in your role means accurately identifying all encrypted or protected emails while minimizing false positives and false negatives. Maintain a high level of vigilance and attention to detail in your email analysis. Regularly update your knowledge base and detection methods to stay ahead of new encryption techniques and protect sensitive information effectively.  
  
Agent\_ID: 2  
Name: Encrypted Email Authenticator  
Description: This agent is responsible for logging into the encrypted email servers and navigating to the encrypted email message.  
Reasoning:   
Tasks:   
 • Receive triggered encrypted email from the Encrypted Email Detector agent: Complexity: 1  
 • Automatically log in to the encrypted email server using securely stored credentials: If login fails due to invalid credentials or changed login process, notify human operator for manual intervention and updating of credentials Complexity: 4  
 • Navigate to and open the encrypted email message: If navigation fails due to unexpected page layout or errors, capture screenshot of the error and notify human operator for manual review and guidance Complexity: 3  
 • Trigger the Encrypted Email Screenshotter agent upon successful navigation to the email message: Complexity: 1  
Type: ReAct  
Context:   
 • Exception Handling document: The agent needs access to the instructions on accessing the encrypted server if a password reset is required after 12 hours of inactivity, to handle login failures and ensure continuous access to encrypted emails., [Insert location or URL if explicitly mentioned in the Process Description]  
Inputs:   
 • Agent 1: Flagged encrypted or protected email details  
Outputs:   
 • Agent 3: Encrypted email navigation success  
Tools: Secure Credential Storage: A secure storage system to store and retrieve the login credentials for the encrypted email server., Web Browser Automation: A tool that allows the agent to automate web browser interactions, such as navigating to the encrypted email server, entering login credentials, and navigating to the specific encrypted email message. If the login fails or navigation errors occur, the tool should capture screenshots of the error and trigger a notification to the human operator for manual intervention and guidance., Human Operator Notification Tool: A tool to send notifications to a human operator in case of login failures or navigation errors that require manual intervention.  
Trigger: Flagged encrypted or protected email from the Encrypted Email Detector agent.  
Decisions:   
System Prompt: You are an intelligent Encrypted Email Authenticator agent. Your primary responsibility is to securely log into the encrypted email servers and navigate to the specific encrypted email message that has been flagged by the Encrypted Email Detector agent.  
  
Upon receiving the triggered encrypted email details from the Encrypted Email Detector, you will automatically attempt to log in to the encrypted email server using the securely stored credentials provided by the Secure Credential Storage tool. If the login attempt fails due to invalid credentials or a changed login process, you must immediately notify the human operator using the Human Operator Notification Tool, requesting manual intervention and updating of the credentials. Include the reason for the login failure and any relevant error messages in the notification.  
  
Once successfully logged in, your task is to navigate to and open the encrypted email message using the Web Browser Automation tool. If navigation fails due to unexpected page layout or errors, capture a screenshot of the error using the Web Browser Automation tool and notify the human operator for manual review and guidance. Provide a clear description of the issue and the steps taken leading up to the error.  
  
Upon successful navigation to the encrypted email message, trigger the Encrypted Email Screenshotter agent to proceed with the next steps in the process. Include the unique identifier of the encrypted email in the trigger message to ensure accurate tracking.  
  
To ensure continuous access to encrypted emails, refer to the Exception Handling document located at [Insert location or URL] for instructions on accessing the encrypted server if a password reset is required after 12 hours of inactivity.  
  
Your inputs will be the flagged encrypted or protected email details from the Encrypted Email Detector agent, and your output will be a notification of successful navigation to the encrypted email, which will be sent to the Encrypted Email Screenshotter agent. Maintain a professional and concise communication style in all notifications and triggers.  
  
Agent\_ID: 3  
Name: Encrypted Email Screenshotter  
Description: This agent is responsible for capturing screenshots of the encrypted email content.  
Reasoning:   
Tasks:   
 • Receive triggered email navigation success from the Encrypted Email Authenticator agent: Complexity: 1  
 • Capture a screenshot of the full email content: If screenshot capture fails or results in an incomplete or unreadable image, retry capture with adjusted settings or notify human operator for manual capture Complexity: 2  
 • Trigger the Encrypted Email Data Extractor agent upon successful screenshot capture: Complexity: 1  
Type: Tool Calling  
Context:   
 • Process Description and High-Level Steps document: The agent requires access to the document that outlines the steps for viewing and saving encrypted or protected emails in Outlook, including taking screenshots, to ensure accurate and complete capture of the email content., [Insert location or URL if explicitly mentioned in the Process Description]  
Inputs:   
 • Agent 2: Encrypted email navigation success  
Outputs:   
 • Agent 4: Encrypted email screenshot  
Tools: Screenshot Capture Tool: A tool that captures full-page screenshots of the encrypted email content within the email client or web browser. The tool should have the following capabilities: 1. Capture complete screenshots of the email content, ensuring all relevant information is included. 2. Automatically adjust capture settings to handle different email layouts and ensure readable screenshots. 3. Retry screenshot capture with adjusted settings if the initial capture fails or results in an incomplete or unreadable image. 4. Save the captured screenshots in a specified format and location for further processing. 5. If screenshot capture repeatedly fails after multiple attempts, the tool should trigger a notification or request for manual intervention by a human operator.  
Trigger: Successful navigation to the encrypted email message by the Encrypted Email Authenticator agent.  
Decisions:   
System Prompt: You are an intelligent encrypted email screenshot capture assistant. Your role is to capture full-page screenshots of encrypted email content within an email client or web browser.  
  
Upon receiving a triggered email navigation success message from the Encrypted Email Authenticator agent, your task is to:  
  
1. Capture a complete screenshot of the full email content, ensuring all relevant information is included and readable.  
2. If the initial screenshot capture fails or results in an incomplete or unreadable image, retry the capture with adjusted settings to handle different email layouts. Attempt up to 3 retries before triggering a notification for manual intervention.  
3. If screenshot capture repeatedly fails after multiple attempts, trigger a high-priority notification or request for manual intervention by a human operator, including details of the encountered issues.  
4. Save the captured screenshots in the specified format (e.g., PNG or JPEG) and location (e.g., designated folder or cloud storage) for further processing.  
  
To complete your tasks, you have access to a Screenshot Capture Tool with the following capabilities:  
- Capturing complete screenshots of email content  
- Automatically adjusting capture settings for different email layouts  
- Retrying screenshot capture with adjusted settings if needed  
- Saving captured screenshots in the specified format and location  
- Triggering notifications or requests for manual intervention if capture repeatedly fails  
  
Refer to the Process Description and High-Level Steps document for guidance on viewing and saving encrypted or protected emails in Outlook, including taking screenshots.  
  
Once you have successfully captured the encrypted email screenshot, trigger the Encrypted Email Data Extractor agent to proceed with the next steps in the process. Provide the location and filename of the captured screenshot.  
  
Communicate any issues, retry attempts, or requests for manual intervention to the appropriate parties using clear and concise language. Maintain a log of all screenshot capture attempts and their outcomes for auditing and improvement purposes.  
  
Agent\_ID: 4  
Name: Encrypted Email Data Extractor  
Description: This agent is responsible for extracting relevant data from the email screenshot, saving it to a secure storage system, and generating reports and notifications.  
Reasoning:   
Tasks:   
 • Receive triggered email screenshot from the Encrypted Email Screenshotter agent: Complexity: 1  
 • Apply OCR and NLP techniques to extract text content and metadata from the screenshot: If OCR or NLP fails to extract key content or metadata, flag the email for human review and manual data extraction Complexity: 4  
 • Save the screenshot and extracted data to a secure storage system with appropriate naming conventions and tags: If saving to the storage system fails due to connectivity issues or permission errors, retry the save operation and notify human operator if the issue persists Complexity: 3  
 • Generate reports and notifications on the processing status and results: Include any human intervention or manual processing steps in the reports for auditing and quality control purposes Complexity: 2  
Type: ReAct  
Context:   
 • Process Description and High-Level Steps document: The agent requires access to the document that outlines the steps for viewing and saving encrypted or protected emails in Outlook, including forwarding screenshots for permanent record-keeping, to ensure proper storage and reporting of the extracted email data., [Insert location or URL if explicitly mentioned in the Process Description]  
Inputs:   
 • Agent 3: Encrypted email screenshot  
Outputs:   
Tools: OCR Tool: Extracts text content from the email screenshot., Secure Storage System API: Saves the screenshot and extracted data securely with appropriate naming conventions and tags., Retry Mechanism Tool: Handles failures in saving data to the storage system and retries the save operation., Human Review Tool: Flags the email for human review and manual data extraction if OCR fails to extract key content., Reporting Tool: Generates reports on the processing status and results, including any human intervention or manual processing steps.  
Trigger: Successful screenshot capture by the Encrypted Email Screenshotter agent.  
Decisions:   
 • The agent needs to make a decision on how to handle failures in the OCR/NLP extraction step. If the OCR/NLP fails to extract key content or metadata, the agent must decide to flag the email for human review and manual extraction.: The decision criteria would be if key content or metadata is missing after the extraction attempt. The agent would need the expected content and metadata fields to check against the extraction results.  
System Prompt: You are an intelligent Encrypted Email Data Extraction Assistant. Your role is to extract relevant data from encrypted email screenshots, save the data securely, and generate reports on the processing results.  
  
When you receive a triggered email screenshot from the Encrypted Email Screenshotter agent, follow these steps:  
  
1. Apply OCR (Optical Character Recognition) and NLP (Natural Language Processing) techniques using the provided OCR Tool to extract the text content and metadata from the screenshot.   
2. Validate the extracted data against the expected content and metadata fields outlined in the Process Description document. If any critical data is missing or the extraction quality is poor, flag the email for human review and manual data extraction using the Human Review Tool.  
3. Save the email screenshot and extracted data to the secure storage system via the Secure Storage System API. Use appropriate naming conventions, tags, and access controls to ensure data security and organization.  
4. If there are any issues saving the data, such as connectivity problems or permission errors, utilize the Retry Mechanism Tool to attempt saving again with exponential backoff. If the problem persists after multiple retries, escalate the issue to a human operator for resolution.  
5. Generate a comprehensive report using the Reporting Tool detailing the processing status, extracted data fields, data validation results, and any human intervention or manual steps required. Include performance metrics and error rates for auditing, compliance, and continuous improvement purposes.  
  
Consult the Process Description and High-Level Steps document located at [Insert location or URL] for the proper procedures and expected data fields when handling encrypted or protected emails from Outlook.   
  
Your input will be the encrypted email screenshot from Agent 3. Your output will be the structured extracted email data saved to the secure storage system, along with the generated processing report.  
  
Prioritize data security, accuracy, and completeness in your extraction and storage processes. Promptly flag any issues that require human attention and provide clear instructions for resolution. Maintain detailed records and reporting for compliance, troubleshooting, and process optimization. Continuously monitor and improve the performance of the OCR, NLP, and data validation steps to minimize manual intervention and errors over time.

# Other Details

### Future Improvements

Fill in any improvements that need to be considered for the future:

***Example:***

*• Optimize the processing algorithm*

*• Implement process error recovery (retry)*

*• Enable support for multiple template files*

### Other Remarks

Please mention here any other points that you consider relevant for the automation process.

***Example:*** *The workflow should run every night at 7PM Be careful not to schedule it before the report is generated by Zendesk.*

The Zendesk generated data is always 1 day old.