# Threat Model Project

**Owner**: Razan Faris,Wafaa Alawadhi,Retaj Baaqeel,Ruba Alotabi
**Reviewer**:
**Contributors**:
**Date Generated**: Tue Oct 29 2024

# Executive Summary

## High level system description

The system represents a document delivery and management workflow within a trust boundary. It involves interactions between external entities (like Print Services, Banking, Email Providers, and PDS Users) and internal processes such as scheduling, document generation, and personal data storage. Key components include:

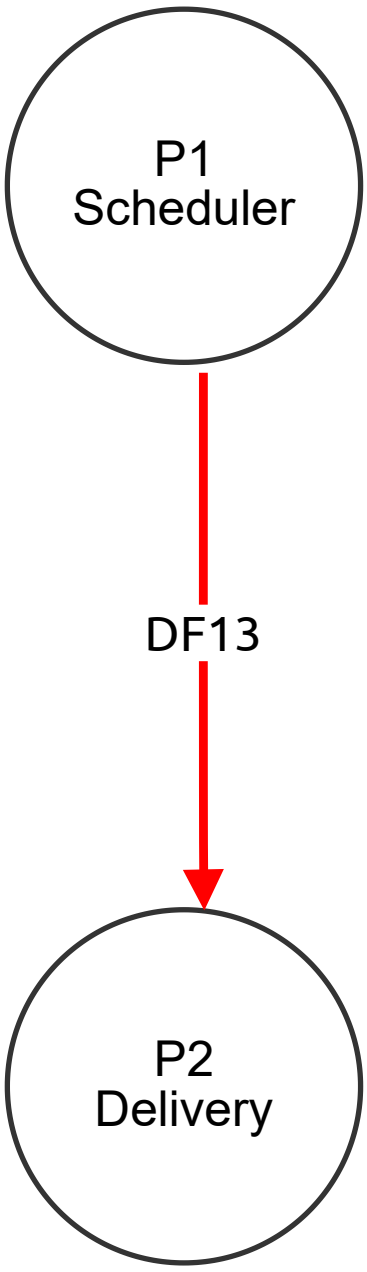
- P2 Delivery: Manages the flow of documents and communication with external services.
- P1 Scheduler: Coordinates tasks and communicates with other internal processes.
- P3 PDS: Stores user data and documents.
- P4 Document Generator: Creates documents for further processing.

Data flows indicate how information moves between these processes and external entities, ensuring delivery, scheduling, and storage of documents and user data.

## Summary

| | |
|---|---|
| **Total Threats** | 40 |
| **Total Mitigated** | 0 |
| **Not Mitigated** | 40 |
| **Open / High Priority** | 16 |
| **Open / Medium Priority** | 23 |
| **Open / Low Priority** | 1 |
| **Open / Unknown Priority** | 0 |

# New LINDDUN diagram



# New LINDDUN diagram

## P1
## Scheduler (Process)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

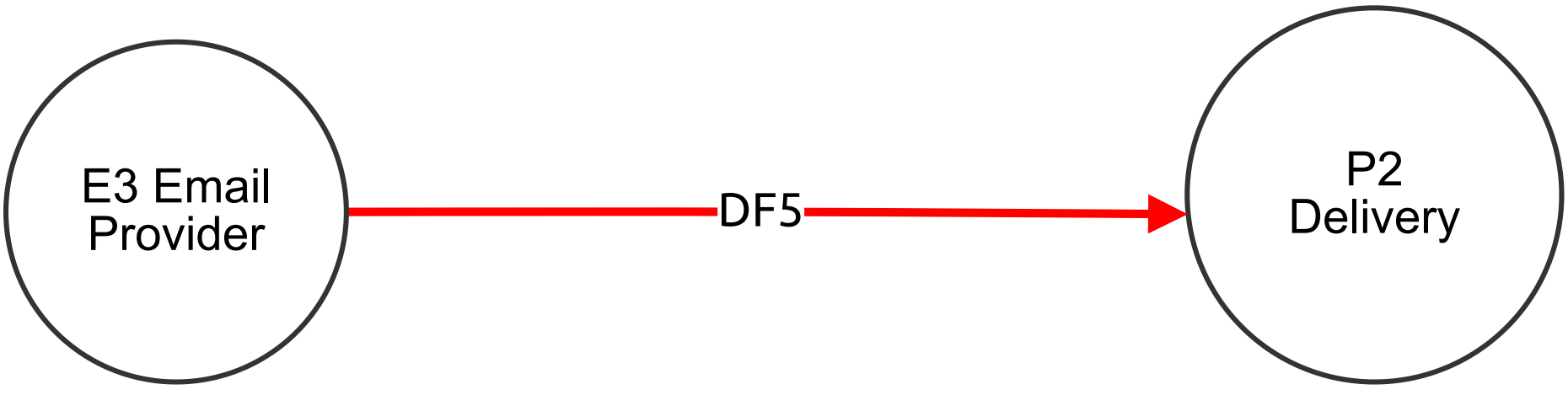
## P2
## Delivery (Process)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## DF13 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 9 | DF13,Detectability | Detectability | Low | Open | 3 | 1. At the source (P1 - Scheduler): P1 may unintentionally reveal that a user is part of the scheduling system through observed communications (D.1). For example, simply being part of the system and communicating with it could reveal a user's involvement, which might be sensitive depending on the context.<br>2. In the data flow itself (DF13): The flow of scheduling data could expose unintended side effects, such as logs or traces of communication that could be used to infer the actions of a user (D.2). This could reveal when a user interacts with the system or schedules specific actions.<br>3. At the destination (P2 - Delivery): System responses from P2 might inadvertently leak information, such as by confirming a user's account exists or providing specific error messages (D.3). These responses can give an observer clues about the user's identity or activities. | 1. At the source (P1 - Scheduler):<br>• Obfuscate User Involvement (D.1): To mitigate the risk of revealing user participation through observed communications, implement encryption protocols for all communication with the scheduling system. Additionally, use anonymous identifiers to prevent linking specific users to the system. Ensure that communications are indistinguishable from general network traffic to reduce the chance of detection.<br>2. In the data flow (DF13):<br>• Minimize Communication Traces (D.2): To prevent detection through logs or side effects, limit the amount of logging related to user actions and ensure logs are anonymized. Clear temporary files or residual data that could reveal user interactions. Use secure communication protocols like TLS to obscure user activity from external observers.<br>3. At the destination (P2 - Delivery):<br>• Reduce Information Leaked in System Responses (D.3): Avoid providing overly detailed error messages or responses that could reveal sensitive information, such as confirming user existence or specific actions. Implement generic error handling (e.g., "Invalid request") that does not provide clues about the user or system status. Additionally, use rate-limiting to prevent attackers from repeatedly querying the system for informa |

# New LINDDUN diagram



# New LINDDUN diagram

## P2
## Delivery (Process)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

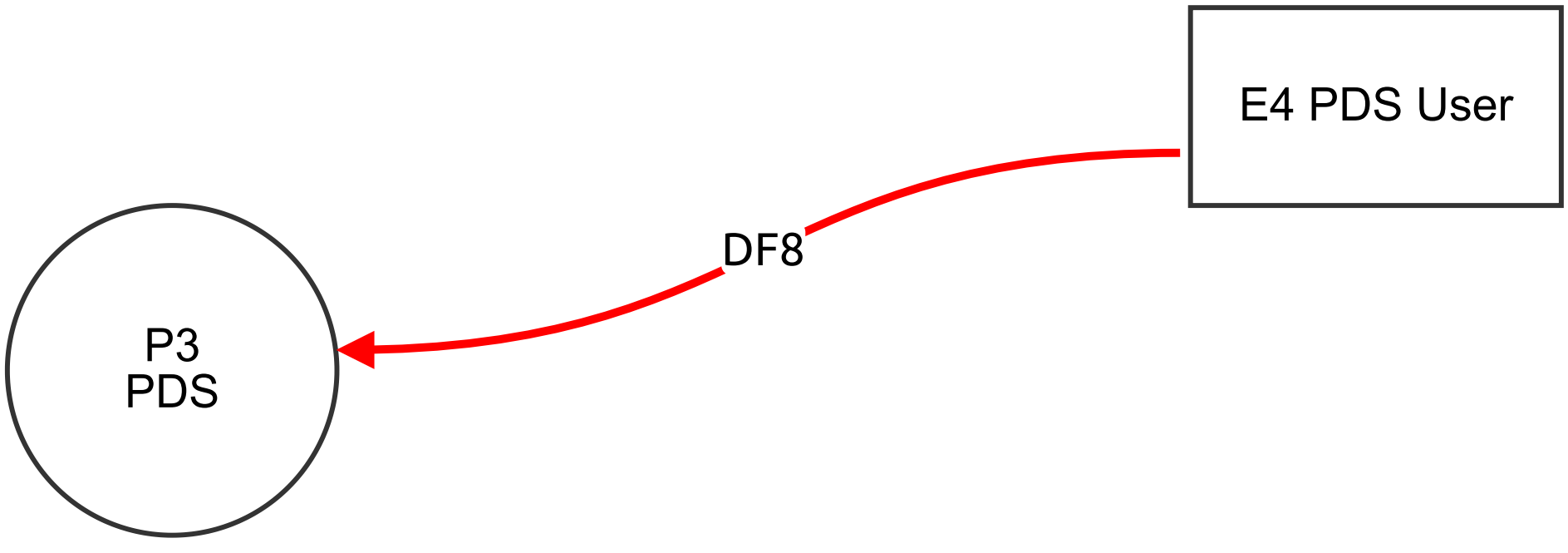
## DF5 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 49 | DF5,Disclosure of information | Disclosure of information | Medium | Open | 5 | 1. At the source (E3 - Email Provider), there is a risk that user data may be shared with unnecessary third parties, which can lead to excessive exposure (DD.4.1.1). This means that data, which should only be used for email processing, might be accessible to more parties than required, increasing the potential for unauthorized use.<br>2. In the data flow itself (DF5), there is a concern that it could carry unnecessary metadata such as timestamps or sender/recipient details, which are not essential for the delivery process (DD.1.3). This extra information may be exposed during transmission, potentially putting users' sensitive information at risk.<br>3. At the destination (P2 - Delivery), data may be retained for longer than necessary, violating data retention principles and increasing the likelihood of unauthorized access (DD.3.4). Without clear policies for data deletion after its use, stored information becomes vulnerable to attacks or misuse over time. | 1. At the source (E3 - Email Provider): To prevent unnecessary data sharing with third parties, implement strict access control policies. Only essential parties should have access to user data. Regular audits and data-sharing reviews can help ensure that data is shared only when absolutely necessary, reducing the risk of excessive exposure.<br>2. In the data flow (DF5): To mitigate the risk of metadata exposure, remove or anonymize unnecessary metadata (such as timestamps or sender/recipient details) from the data flow. Additionally, ensure that any sensitive data that must be transmitted is encrypted, both in transit and at rest, to prevent unauthorized interception.<br>3. At the destination (P2 - Delivery): Enforce data retention policies that limit how long data is stored. Implement automated mechanisms that securely delete or archive data once it is no longer needed for processing. Regularly review data retention practices to ensure compliance and prevent the accumulation of unnecessary data, reducing the risk of unauthorized access. |

## E3 Email
## Provider (Process)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

# New LINDDUN diagram



# New LINDDUN diagram

## P3

## PDS (Process)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

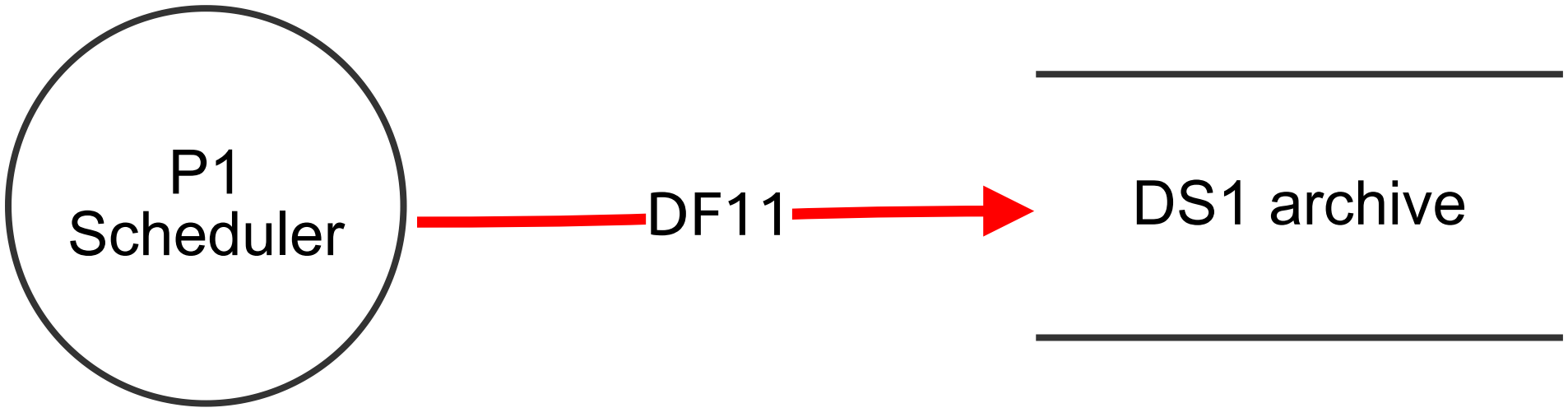
## DF8 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 56 | DF8, Non-Compliance | Non-compliance | Medium | Open | | In analyzing DF8, several non-compliance risks have been identified. Starting with the source, E4 may process more personal data than necessary, which breaches the data minimization principle by including details that aren't essential for document processing (Nc.1.1.2). Moving to the data flow itself, DF8 could retain data in transit longer than required, potentially violating storage limitation principles if no clear policy is in place for timely data deletion (Nc.1.1.4). At the destination, P3 (Document Service) may lack well-defined data management policies, including clear roles and responsibilities for handling personal data, leading to improper data management practices (Nc.2). | 1. Enforce Data Minimization Policies (E4 - Source): Review and limit the types of data processed by E4 to only what is necessary for document processing. Implement strict data collection guidelines and routinely audit data usage to ensure compliance with the data minimization principle.<br>2. Establish Data Retention Policies (DF8 - Data Flow): Define clear policies for data retention and timely deletion in transit. Implement automated mechanisms to delete or archive data after a specified period, ensuring data is not held longer than needed.<br>3. Define Data Management Roles and Responsibilities (P3 - Destination): Develop and document data management policies for P3 (Document Service). Assign specific roles and responsibilities for handling and managing personal data, ensuring accountability and adherence to best practices in data protection. |

## E4 PDS User (Actor)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

# New LINDDUN diagram



# New LINDDUN diagram

## P1
## Scheduler (Process)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

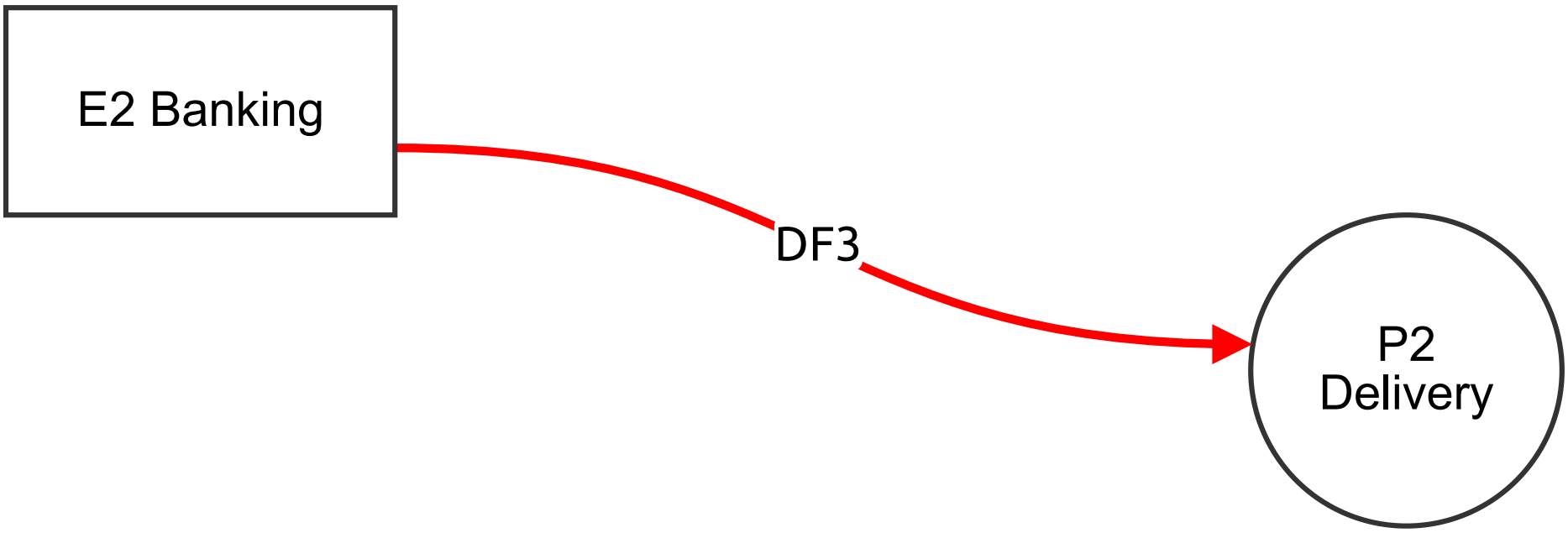
## DF11 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 57 | DF11 Non-repudiation | Non-repudiation | Medium | Open | 3 | here the document inside the schedular have some attribute that specify if the<br>document should be sent to delivery based on the time, date or to be stored in the<br>archive, also maybe this document is sensitive and we can’t send it now so we store<br>it and wait tell the right time, or user appear, then the archive the documents are<br>stored based on sensitivity.<br>Source (P1 Scheduler):<br>• here the attacker can access the scheduler and reschedule things, and then he can<br>deny what he did. This compromises the attribution of actions (Nr.2).<br>Data Flow (DF11):<br>• If the data flow is not encrypted then the attacker can observe the tasks and request<br>send between the schedular and the archive (Nr.1.1, Nr.1.3).<br>Destination (DS1 Archive):<br>• the attacker(employ from inside the organization) can manipulate the archive logs<br>with will result in Nr.1.1, Nr.1.3 and simply he can deny that he did this | Use robust logging to make sure no one can alter the data, even if the attacker has<br>linked info about something, altering will be difficult to do, also to reduce the risk at<br>transmission use digital signatures to ensure the integrity of the metadata during<br>transmission and storage. |

## DS1 archive (Store)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

# New LINDDUN diagram



# New LINDDUN diagram

## P2
## Delivery (Process)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## DF3 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 58 | DF3, Linkability | Linkability | Medium | Open | 1 | After the bank sends the invoices, the delivery process will receive it and then the<br>bank will return a delivery status contains the id of the particular document, this<br>allow the delivery to keep track of the current document.<br>Source (E2 Banking):<br>• Linking Threat: here we could consider The document ID itself as the threat, if not<br>properly anonymized or handled, could act as a unique identifier L.1.1 (Unique<br>identifier):linking the invoice to a specific user.<br>Data Flow (DF3):<br>• Linking Threat: L.1.1 (Unique identifier): The document ID in transit is vulnerable to<br>interception, potentially revealing a link between the invoice and the user. This data<br>centric threat relies on the ID being transmitted. L.2.1.1 (Quasi-identifier combining<br>data of a single individual): The combination of document ID and the delivery status<br>(e.g., timestamps, success/failure indicators) could be used as a quasi-identifier.<br>Destination (P2 Delivery):<br>• Linking Threat: if the delivery service stores this information insecurely. L.2.1.1<br>(Quasi-identifier combining data of a single individual): The document ID, combined<br>with other data held by the delivery service (e.g., delivery address, delivery method),<br>could create a quasi-identifier. L.2.2.1 (Profiling an individual): Repeated use of the<br>service by the same user, tracked via the document ID, could lead to profiling based<br>on delivery frequency or document types. The action-based threat depends on how<br>P2 uses the received data. | Try applying noise on the data to make it harder to be identified, and use strict ACL<br>based on the least privileged principal, additionally you can conduct regular audit to<br>check on the system. |

## E2 Banking (Actor)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

New LINDDUN diagram

DS2 PDS Docs

DF20

P3
PDS

# New LINDDUN diagram

## P3

## PDS (Process)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

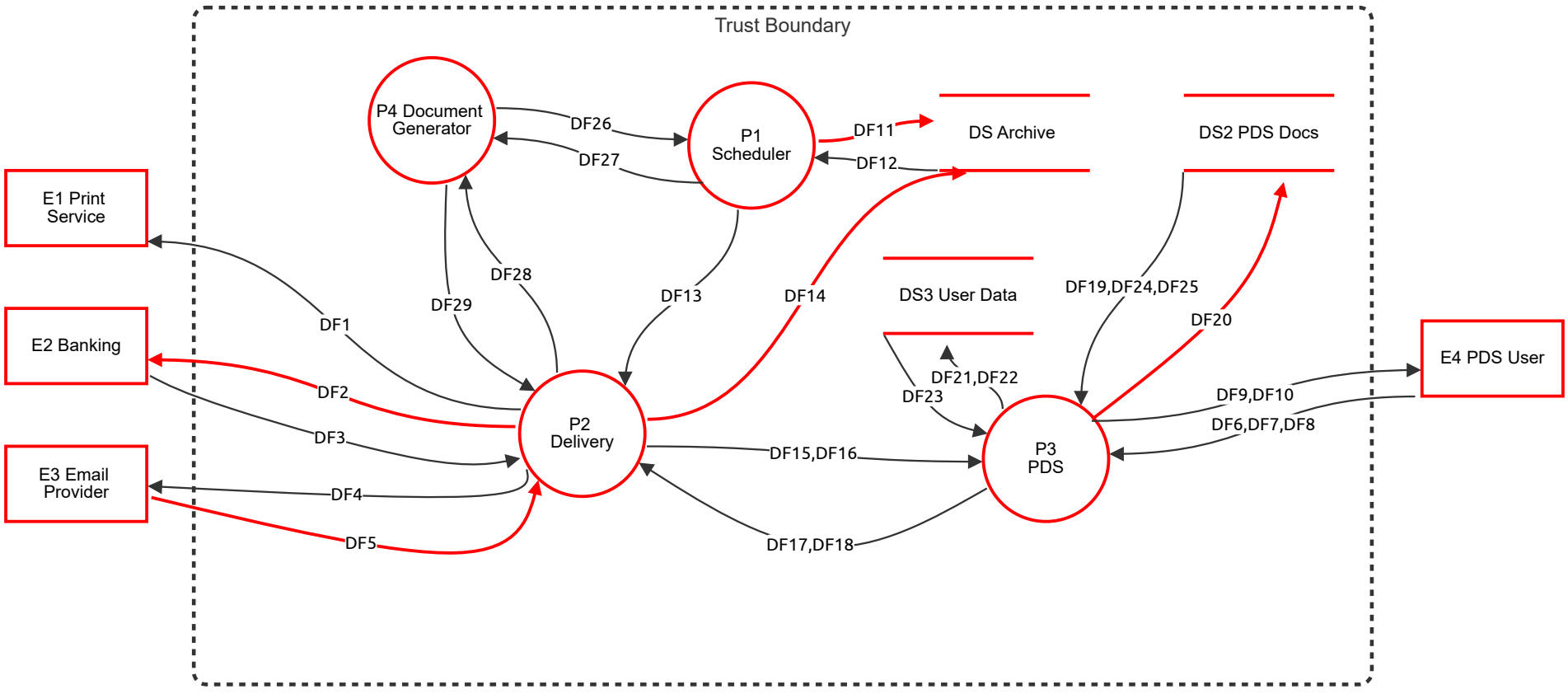
## DF20 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 59 | DF20,Identifiability | Identifiability | Medium | Open | | this flow begin with the user requesting a document, then the p3 process make sure<br>the user is authenticated, if he is then p3 will request DS2 data store to check the<br>document.<br>Source (P3 PDS):<br>• The P3 PDS processes data that is directly can identify users like there ID I.1.1<br>(Processing of identified data), not just that but if the loges combined with the ID<br>then this is a I.2.1.2 (Quasi-identifier).<br>Data Flow (P3 PDS to DS2 PDS Docs):<br>• If the data flow path is nit encrypted then user ID may be exposed and this lead us to<br>I.1.1 (Processing of identified data), also the meta data associated with the<br>document can be corrupted reviling information about the user I.1.2 (Identified<br>information in metadata).<br>Destination (DS2 PDS Docs):<br>• The document stored can contain information that directly reveal user identity I.2.2<br>(Revealing attributes), | Make sure to use strong authentication, and use encryption to secure the<br>communications between the proccess and the data store, |

## DS2 PDS Docs (Store)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

# New STRIDE diagram



# New STRIDE diagram

## P2
## Delivery (Process)

The delivery process is responsible for handling data transfer between di erent elements in the system. It manages the routing and delivery of data to various endpoints, ensuring data reaches the correct location.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 23 | STRIDE | Spoofing | High | Open | 7 | A threat actor could impersonate the delivery to execute unauthorized actions or modify delivery processes, leading to potential delays, data exposure, or unauthorized access to sensitive information in transit. | Implement SSL/TLS and PKI for secure data encryption and authentication during data transit.<br>Strengthen Access Control using MFA and session management to prevent unauthorized access and session hijacking. |
| 24 | STRIDE | Tampering | Medium | Open | 6 | A threat actor could intercept and alter data during the delivery process, leading to the delivery of incorrect information, modified document content, or insertion of malicious data. | Implement SSL/TLS and PKI for secure data encryption and authentication during data transit.<br>Strengthen Access Control using MFA and session management to prevent unauthorized access and session hijacking. |
| 25 | STRIDE | Information disclosure | High | Open | 8 | Sensitive data may be exposed or accessed by unauthorized individuals during the delivery process due to intercepted transmissions, insufficient access controls, or inadequate data handling practices. | Encrypt Data and Apply DLP to monitor for unauthorized sharing.<br>Use Secure Transmission Channels for safer data handling.<br>Apply Data Masking to protect sensitive information. |
| 61 | STRIDE | Denial of service | High | Open | 7 | Overwhelming the P2 Delivery component with a flood of requests, which disrupts document delivery. This attack could be executed by using automated scripts or botnets that send a high volume of requests to the delivery system, eventually causing it to become | Implement rate limiting on the delivery system to control the number of requests from each user or IP address.<br>Use web application firewalls (WAF) to filter and monitor incoming traffic for unusual patterns. |
| 65 | STRIDE | Elevation of privilege | High | Open | 7 | Privilege Escalation in the P2 Delivery System. An attacker could exploit vulnerabilities in the delivery system to gain unauthorized access or manipulate delivery processes, potentially by injecting malicious code. | Implement input validation and sanitization to prevent malicious code injection.<br>Monitor and log access attempts to detect and respond to unauthorized activities.<br>Use multi-factor authentication (MFA) for access to sensitive components within the delivery system. |

## P1
## Scheduler (Process)

The scheduler orchestrates tasks, managing timing and sequence for processes within the system. It’s responsible for scheduling operations and sending commands to other processes to initiate activities.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 20 | STRIDE | Spoofing | Medium | Open | 6 | A threat actor could impersonate the scheduler to execute unauthorized tasks or modify task schedules, disrupting operations. This could lead to delays, data exposure, or unauthorized control over the process flow. | Implement DNSSEC to prevent scheduler spoofing over the network.<br>Set up a Certificate Authority (CA) to verify devices accessing the scheduler.<br>Use IPSec or SSL/TLS to secure all scheduler communications. |

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 21 | STRIDE | Tampering | Medium | Open | 5 | A threat actor might alter scheduled tasks, affecting workflow timing or critical data, which can disrupt operations, cause delays, or compromise data integrity. | Enable audit logs to track and detect any tampering attempts.<br>Use digital signatures and hashes to protect scheduled tasks from unauthorized changes.<br>Apply ACLs to control who can modify scheduling settings, reducing tampering risks. |
| 22 | STRIDE | Information disclosure | High | Open | 8 | Unauthorized access to scheduling data could expose critical process details, such as schedules and task timings, which could be used by attackers to disrupt operations or plan further attacks. | Encrypt scheduling data both in transit and at rest to prevent unauthorized access.<br>Enable audit logs to track access and changes to scheduling data for compliance and monitoring.<br>Apply role-based access controls to limit data access to authorized users only. |

# P4 Document Generator (Process)

The document generator is responsible for creating and managing documents within the system. It may generate reports, summaries, or other documents based on system data.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 42 | STRIDE | Spoofing | Medium | Open | 5 | A threat actor could impersonate the document generator to create fake documents or initiate unauthorized document generation, leading to the spread of false information, access to sensitive documents, and misuse of resources. | Implement PKI and CA for entity verification on document generator<br>Apply DNSSEC to avoid DNS spoofing if generator is network-exposed<br>Limit document generation permissions by using RBAC |
| 43 | STRIDE | Tampering | Medium | Open | 6 | A threat actor may alter the content of generated documents, resulting in misinformation or falsified records. This compromises document integrity and could lead to legal or operational issues. | Sign generated documents to ensure authenticity and detect tampering<br>Enable logging and hashing to verify data integrity during document generation<br>Use digital signatures or watermarks to confirm document authenticity |
| 44 | STRIDE | Information disclosure | High | Open | 8 | Sensitive information within generated documents may be unintentionally exposed due to insufficient security controls, risking privacy breaches and data leaks. | Use PKI and CA to verify entities accessing the document generator<br>Apply DNSSEC to prevent DNS spoofing if network-accessible<br>Mask sensitive document content and restrict generator access to authorized users<br>Encrypt sensitive data and keep logs for auditing<br>Redact highly sensitive content to prevent unauthorized exposure |
| 63 | STRIDE | Repudiation | Medium | Open | 5 | An employee denying involvement in a specific document generation or delivery action, creating accountability issues. | Implement logging and auditing to record user actions, including timestamps and user IDs, ensuring traceability.<br>Use digital signatures or cryptographic methods to authenticate document actions, making it difficult for users to deny their actions.<br>Establish policies and training on accountability to reinforce the consequences of repudiation. |
| 70 | STRIDE | Denial of service | Medium | Open | 5 | A flood of document requests could overwhelm the generator, delaying document creation. | Implement Throttling for document requests.<br>Use Load Balancing.<br>Enable DDoS Protection Tools. |
| 71 | STRIDE | Elevation of privilege | High | Open | 7 | Unauthorized access to the document generator would allow threat actors to create or alter Official documents. | Enforce MFA for accessing the generator.<br>Apply RBAC for document management.<br>Conduct Regular Access Audits. |

# P3
# PDS (Process)

The PDS process manages sensitive personal data and is designed to ensure data privacy and security. It maintains user data confidentiality, integrity, and access control.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 38 | STRIDE | Spoofing | Medium | Open | 5 | A threat actor could impersonate a PDS (Personal Data Security) user to gain unauthorized access to sensitive data. This could lead to data theft, unauthorized modifications, or privacy breaches. | Here's the information without colons and in a simpler format:<br><br>Implement Authentication by using Kerberos or SSH keys to authenticate users and systems accessing PDS<br>Encrypt Transfers with SSL or SSH to secure data transfers within PDS |
| 39 | STRIDE | Tampering | Medium | Open | 6 | A threat actor could alter personal data within the PDS, potentially corrupting information or changing records. This tampering could result in data integrity loss, leading to inaccurate information or poor decision-making. | Ensure Data Integrity using hashing and digital signatures to detect unauthorized changes<br>Set Access Control with ACLs to restrict data modification rights<br>Enable Logging to monitor data modifications and detect tampering in real-time |
| 40 | STRIDE | Information disclosure | High | Open | 7 | Sensitive personal data within the PDS may be exposed to unauthorized users, risking privacy breaches and compliance violations. This could occur due to weak access controls, accidental exposure, or deliberate extraction by malicious actors. | Encrypt Data to secure all sensitive data within PDS<br>Restrict Access with role-based control to limit data exposure<br>Implement DLP and Logging to prevent unauthorized sharing and log access to sensitive data |

# E1 Print Service (Actor)

External service that manages print jobs, receiving data from the system to create physical documents. It requires secure access to prevent unauthorized document printing.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 15 | STRIDE | Spoofing | Medium | Open | 6 | A threat actor could impersonate the print service to intercept or redirect print jobs, capturing sensitive documents. This would grant unauthorized access to confidential information, potentially leading to further exploitation. | Enable SSL/TLS and PKI to secure connections and authenticate devices with trusted certificates<br>Implement Certificate Authority to verify and authorize devices accessing the print service<br>Enable DNSSEC to prevent DNS spoofing for network-accessible print services<br>Implement Certificate Authority (CA) to verify and authorize devices accessing the print service |

# E2 Banking (Actor)

External banking service for nancial transactions or data exchanges related to payment processing, user accounts, or other banking functions.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 17 | STRIDE | Spoofing | High | Open | 8 | A threat actor could impersonate the banking service, tricking users into sharing sensitive information such as account credentials or transaction data. This spoofing attack could lead to unauthorized access to user accounts or financial loss. | Enable Multi-Factor Authentication (MFA) to add an extra layer of security for user access, combining password entry with verification via a mobile app or SMS code to prevent unauthorized access.<br>Use SSL/TLS and DNSSEC to protect connections and prevent redirection to fake sites.<br>Apply PKI to authenticate users and devices securely. |

# E3 Email Provider (Actor)

Email service provider used for sending system-generated emails or noti cations. It handles external communication and may relay sensitive information to users.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 18 | STRIDE | Spoofing | High | Open | 7 | A threat actor could impersonate the email provider to gain unauthorized access to sensitive data, potentially resulting in data theft, unauthorized modifications, or privacy breaches | Use SPF, DKIM, and DMARC to verify email authenticity.<br>Apply SSL/TLS to secure email access and prevent credential theft.<br>Use SSH Host Keys for secure server authentication. |
| 60 | STRIDE | Repudiation | Medium | Open | 5 | A threat actor could use spoofed email addresses or compromised accounts to send malicious emails while hiding their identity. They may deny involvement, claiming the emails originated elsewhere, complicating accountability and tracing. | Implement comprehensive logging of all email actions, including timestamps, sender and recipient details, and email content.<br>Use digital signatures for outgoing emails to authenticate the sender and ensure the integrity of the message.<br>Establish clear policies on user accountability and conduct regular training to inform users about the importance of secure practices and the consequences of repudiation. |

# E4 PDS User (Actor)

Represents individuals or users who interact with the Personal Data Security (PDS) system, accessing or modifying personal data according to their permissions.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 19 | STRIDE | Spoofing | Medium | Open | 5 | A threat actor could impersonate a PDS user to gain unauthorized access to sensitive data, potentially leading to data theft or unauthorized modifications. | Enable Multi-Factor Authentication (MFA) to add an extra layer of security for user access, combining password entry with verification via a mobile app or SMS code to prevent unauthorized access.<br>Implement Session Timeouts to prevent hijacking risks.<br>Monitor Logins to identify and stop impersonation attempts. |
| 73 | STRIDE | Repudiation | Medium | Open | 5 | A PDS user could deny actions within the system, such as accessing or modifying sensitive data, creating accountability issues. | Log User Actions to keep a record of who does what in the system.<br>Use Digital Signatures to verify actions and make it hard to deny involvement.<br>Provide Training on user responsibility and consequences of repudiation |

# DS Archive  (Store)

This is a storage area for archived data, preserving historical records that may not need frequent access. It is used for long-term storage and may contain data for compliance, analysis, or audit purposes.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 26 | STRIDE | Tampering | Medium | Open | 6 | A threat actor may alter archived data, corrupting historical records and potentially leading to incorrect insights or decisions. Tampering with archived data can compromise its reliability and impact audits or regulatory compliance. | Implement digital signatures and hashing to verify data integrity.<br>Enable ACLs and version control to restrict modifications and maintain history.<br>Implement audit logs to record access and changes. |
| 27 | STRIDE | Information disclosure | Medium | Open | 6 | Unauthorized access to archived data could expose sensitive historical information, potentially resulting in data leaks or compliance violations. This threat is critical if the archived data contains personal or confidential information. | Enable encryption for archived data to prevent unauthorized access.<br>Implement regular access control audits to maintain updated permissions.<br>Enable DLP and data masking to prevent accidental or unauthorized data disclosure. |

# DS2 PDS Docs (Store)

Stores documents related to personal data security, such as policies, user data access logs, or compliance records.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 28 | STRIDE | Tampering | High | Open | 7 | Unauthorized changes to PDS (Personal Data Security) documents could corrupt critical information, leading to inaccurate records. This could impact business decisions, violate data integrity policies, and affect regulatory compliance. | Implement digital signatures to verify document authenticity and detect tampering.<br>Enable ACLs to restrict editing permissions to trusted users.<br>Implement audit trails and version control to monitor changes and allow reversion of unauthorized modifications. |
| 29 | STRIDE | Information disclosure | Medium | Open | 6 | PDS documents contain sensitive personal or organizational information that may be exposed without proper access controls. Unauthorized disclosure could lead to privacy breaches, reputational damage, and compliance issues. | Implement encryption for PDS documents at rest and in transit to prevent unauthorized access.<br>Enable DLP tools to monitor and prevent data leaks.<br>Regularly review access controls to ensure only authorized personnel can access sensitive documents. |

# DF1 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

# DF3 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

# DF4 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## DF6,DF7,DF8 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## DF9,DF10 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## DF12 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## DF13 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## DF17,DF18 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## DF19,DF24,DF25 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## DF21,DF22 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## DF23 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## DF26 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## DF27 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## DF28 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## DF29 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## DF11 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 62 | STRIDE | Denial of service | High | Open | 8 | A threat actor could target the DF11 system connection with network attacks to disrupt communication between system components, effectively halting data flow. | Use strong encryption protocols to secure the connection and prevent data interception. Monitor network traffic for unusual activity and implement intrusion detection systems (IDS) for early detection of attacks. |

## DF15,DF16 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

## DF2 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 75 | STRIDE | Tampering | High | Open | 8 | A threat actor could intercept and alter transaction data between the Delivery process (P2) and the Banking service (E2), leading to unauthorized modifications that affect payment amounts or account details | Use end-to-end encryption (such as TLS) to secure data in transit, along with digital signatures to verify data integrity at the receiving end. |

## DF14 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 76 | STRIDE | Denial of service | Medium | Open | 6 | A threat actor could flood the communication channel between the Scheduler (P1) and Delivery (P2) with an excessive number of requests, disrupting the scheduling of deliveries and causing delays. | Implement rate limiting, Web Application Firewall (WAF), and load balancing. |

## DF20 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 77 | STRIDE | Tampering | High | Open | 8 | A threat actor could intercept and alter document data being transferred from the PDS (P3) to the PDS Docs (DS2), leading to inaccurate or falsified records. | Implement hashing and digital signatures for integrity verification. |

## DF5 (Data Flow)

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 78 | STRIDE | Information disclosure | Medium | Open | 6 | Sensitive data sent from the Delivery process (P2) to the Email Provider (E3) may be exposed if intercepted, potentially leaking private information. | Implement TLS for secure communication and Data Loss Prevention (DLP) on the email provider. |

## DS3 User Data (Store)

Holds sensitive user information within the system, including personal data necessary for system operations. It is critical for maintaining user privacy.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 30 | STRIDE | Tampering | High | Open | 8 | A threat actor could modify user data, leading to unauthorized changes that compromise data integrity and damage user trust. Such alterations could result in inaccurate records, affecting decision-making, compliance, and overall user experience. | Enable digital signatures and hashing to protect data integrity.<br>Implement RBAC to limit write permissions to specific roles.<br>Enable real-time logging to monitor and address any unauthorized changes. |
| 33 | STRIDE | Information disclosure | High | Open | 9 | Unauthorized access to user data could expose personal information, leading to privacy violations, reputational damage, and legal repercussions. This is a critical threat, as user data often contains sensitive information, making it a prime target for attackers. | Implement encryption for all user data, both in storage and during transfers.<br>Apply data masking and DLP to protect sensitive fields and control data sharing.<br>Enable regular access audits to keep permissions updated and aligned with access needs. |