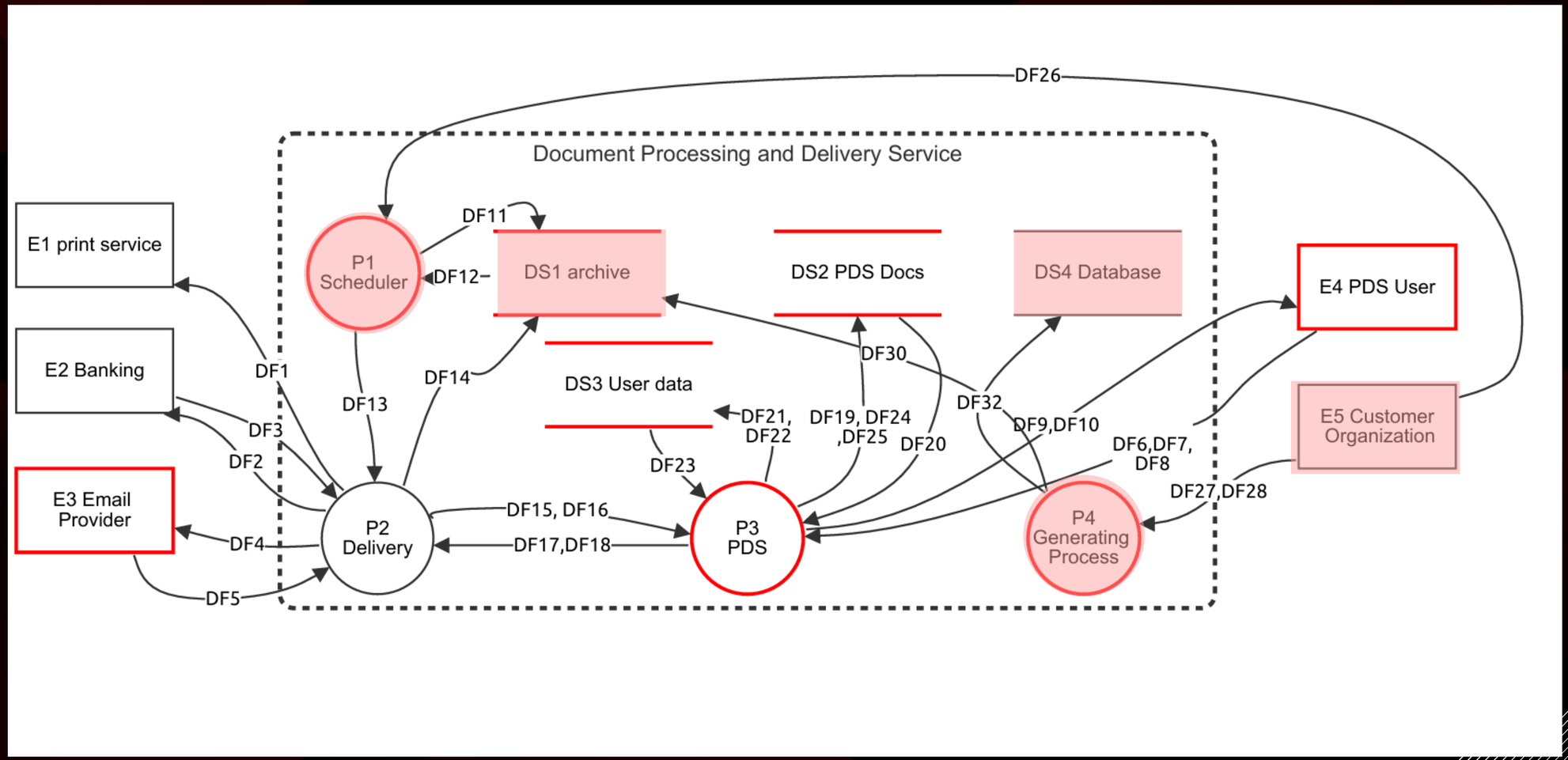
SEC2401_CYBER THREAT AND INCIDENT RESPONSE

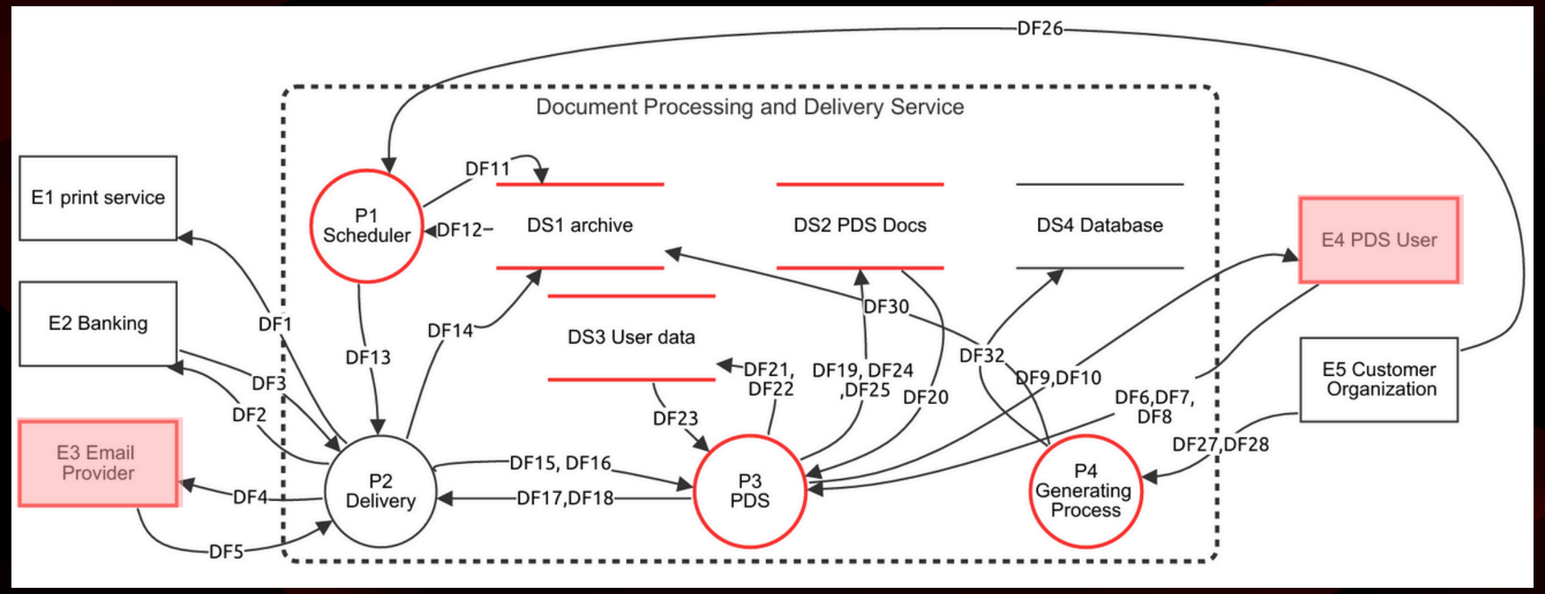
Document Processing Service

Presented to: Dr. Shaimaa Bajoudah

DOCUMENT PROCESSING AND DELIVERY SYSTEM *(DFD)*



STRIDE THREATS *(SPOOFING)*



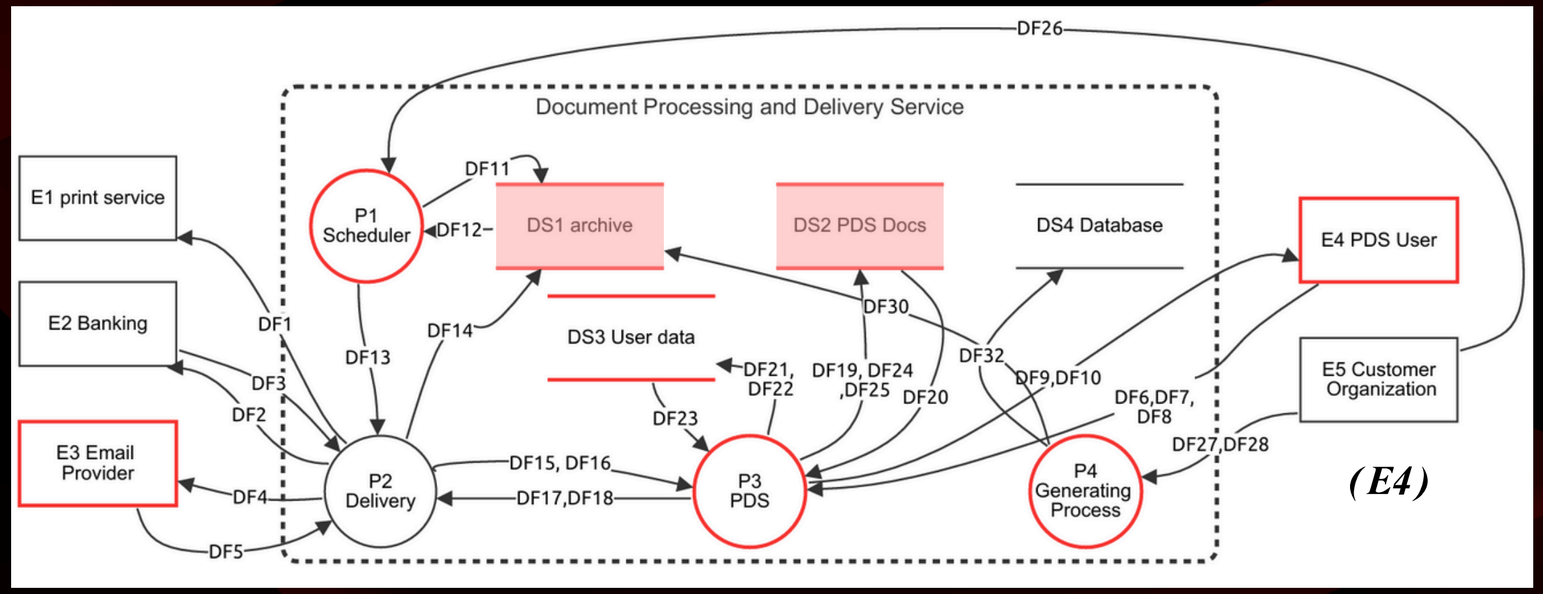
1. Impersonating the Email Provider *(E3)*

An attacker could send forged emails that look like they originated from the official email provider, especially if the domain lacks proper email authentication mechanisms.
This can trick the system or staff into sending sensitive documents to the attacker.

2. Spoofing the PDS User Identity *(E4)*

The PDS user interacts directly with the system to request documents and services. An attacker may impersonate a legitimate user by using stolen or weak credentials. If successful, the attacker gains unauthorized access to system functions and sensitive data while being treated as a trusted user.

STRIDE THREATS *(TAMPERING)*



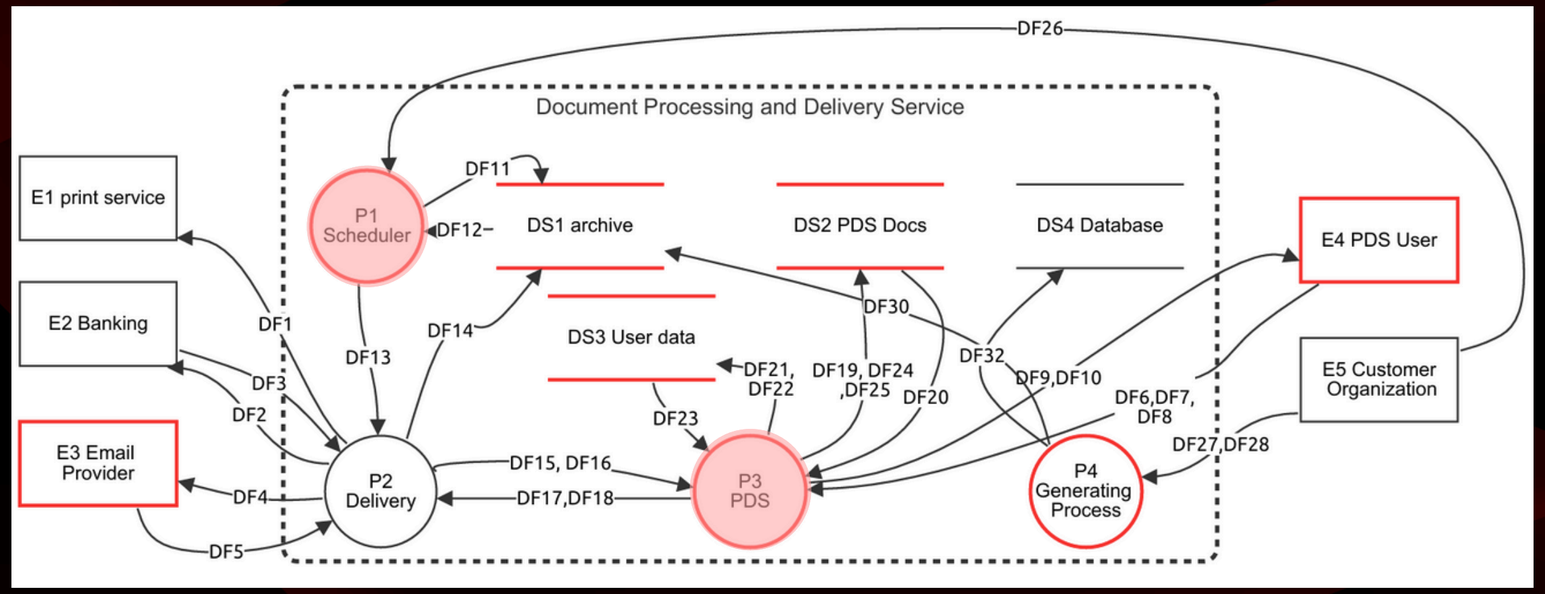
3. Unauthorized Modification of Archived Files *(DS1)*

The Archive stores final document files. If access is not properly controlled, unauthorized users may view confidential documents or modify archived files, which can compromise data integrity and confidentiality.

4. Editing PDS Documents Stored in the System *(DS2)*

PDS Docs stores user specific documents. An attacker may modify, delete, or replace documents, which can result in incorrect or misleading information being presented to users.

STRIDE THREATS *(REPUDIATION)*



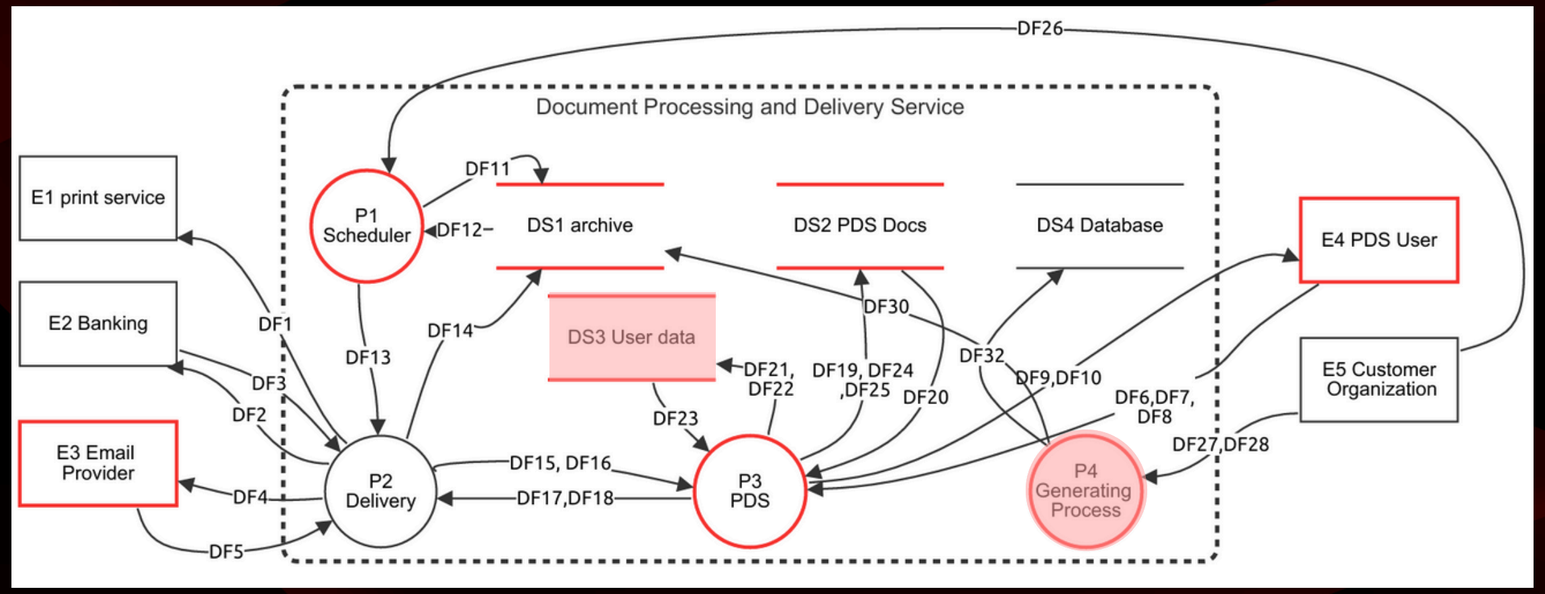
5. PDS User Denying Submitted Requests *(P3)*

A PDS user may deny having submitted a specific request if the system does not maintain veriable and tamper resistant records. In the absence of reliable evidence, the user can claim they never initiated the request that triggered document generation, delivery, or other system actions.

6. No Traceability for Scheduler Actions *(P1)*

If the Scheduler executes tasks without associating them with the user who triggered them, no one can be reliably held responsible. This makes it easy for someone to deny that they initiated a process that caused an error or system disruption.

STRIDE THREATS *(INFORMATION DISCLOSURE)*



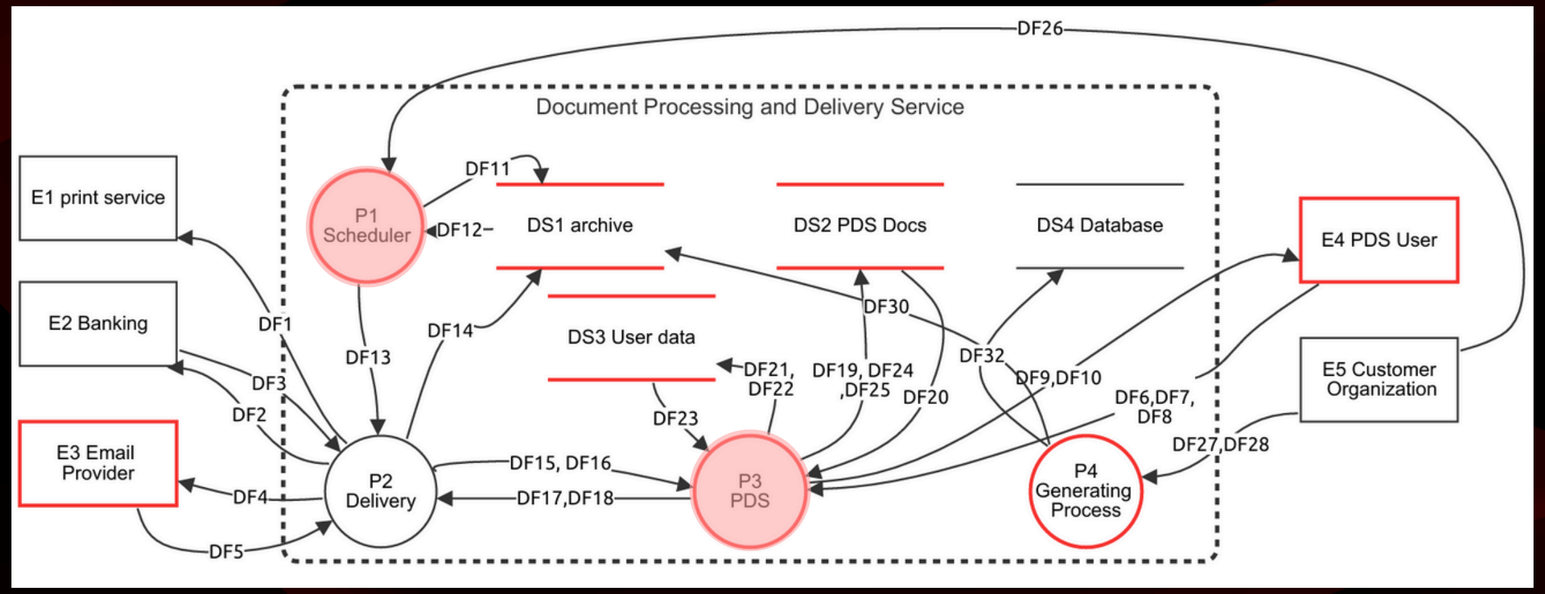
7. Data Leakage Through the Generating Process *(P4)*

The generating process handles sensitive data while creating documents. During this process, data may be temporarily stored in memory or in temporary files. If these are not properly protected, unauthorized access may occur, leading to data leakage.

8. Exposure of User Personal Data *(DS3)*

User Data contains sensitive user information and preferences. Unauthorized access may lead to data leakage, privacy violations, or misuse of personal data.

STRIDE THREATS *(DENIAL OF SERVICE)*



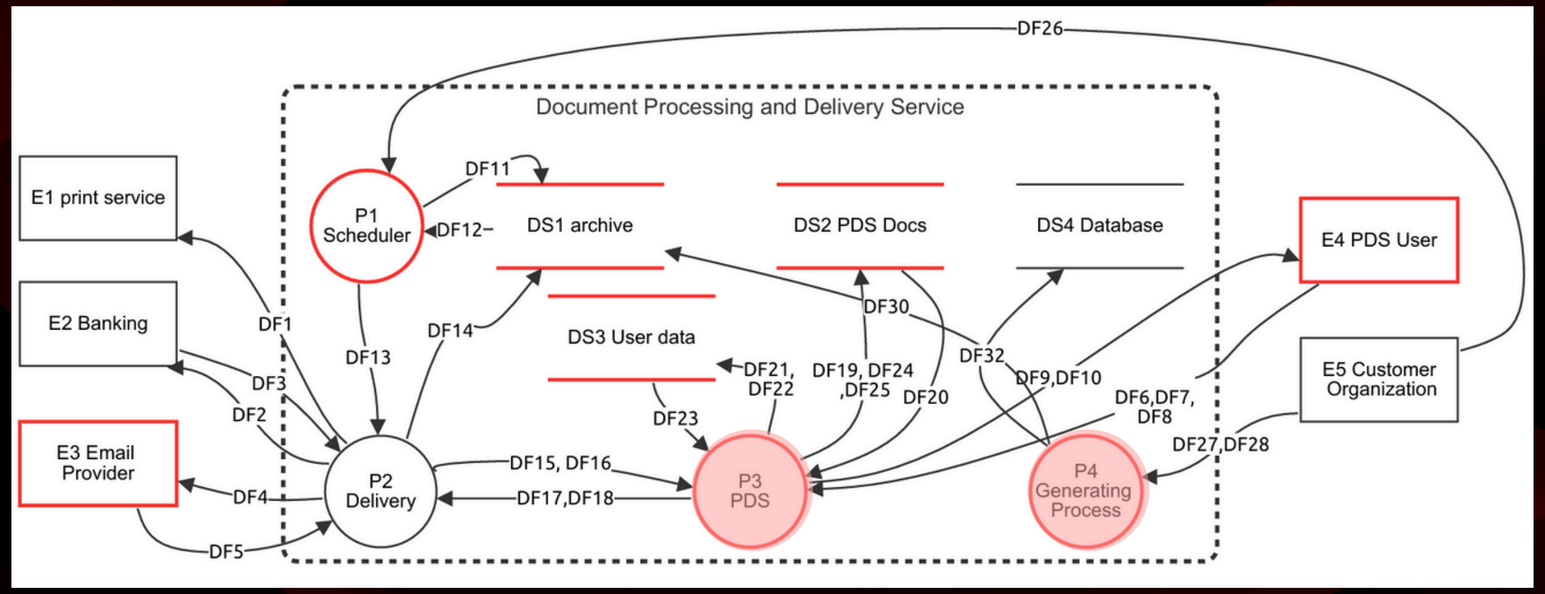
9. Flooding the Scheduler with Excessive Requests *(P1)*

An attacker may overwhelm the Scheduler by repeatedly sending request triggers, causing slowdowns or complete stalls in document handling. This is common when there is no rate limiting or queue protection.

10. PDS Process Overload Attack *(P3)*

An attacker may overwhelm the PDS (P3) process by sending a large number of document generation or delivery requests in a short period. This excessive load can cause the PDS process to become unresponsive, This prevents real users from completing normal operations.

STRIDE THREATS *(ELEVATION OF PRIVILEGE)*



11. Privilege Escalation in PDS Process *(P3)*

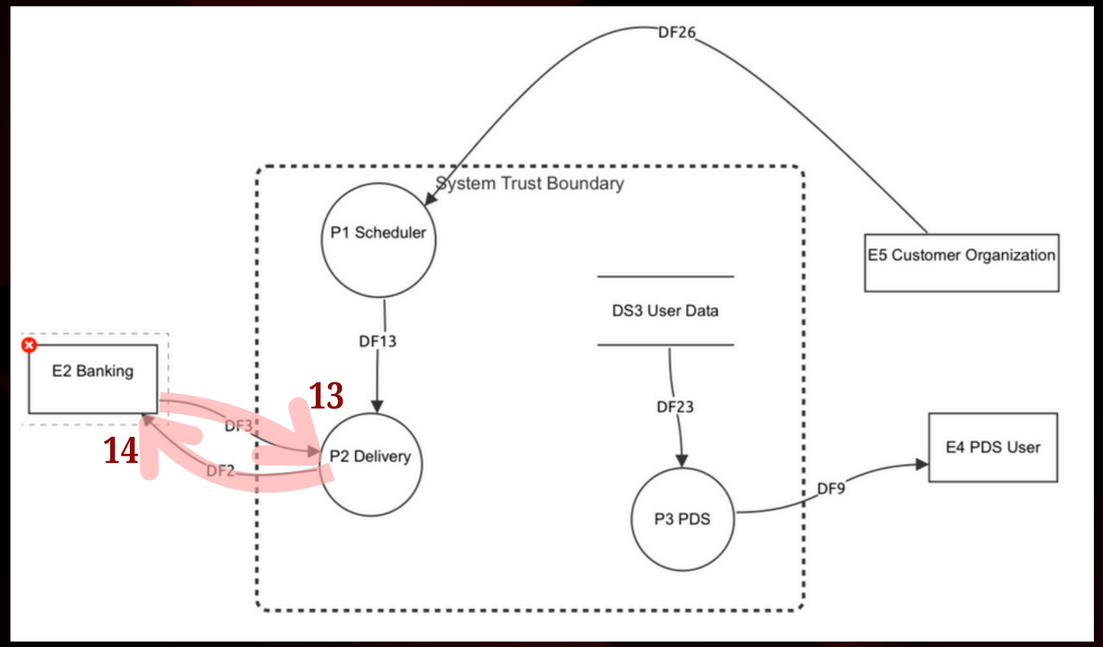
An attacker may exploit a vulnerability in the PDS (P3) process to gain higher privileges than intended. By abusing weak access controls or software flaws, the attacker could access restricted document data, perform unauthorized actions, or manipulate delivery and user data beyond their assigned role.

12. Privilege Escalation Inside the Generating Process *(P4)*

The generating process relies on templates and inputs to produce documents. If these inputs are not strictly validated, an attacker may exploit them to execute actions with higher privileges than intended, potentially affecting system integrity.

LINDDUN THREATS

LINKABILITY (L.2.2) & NON-REPUDIATION (NR.1.1)



13. Profiling of customers through payment activity *(DF3)*

In Data Flow DF3, payment-related metadata flows from the Banking service to the Delivery process. Although the payment content is not shared, repeated exposure of metadata such as timestamps and transaction identifiers can be linked with delivery records over time. This linkage may allow an attacker to profile customer behavior, payment frequency, or organizational activity patterns based on recurring payment and delivery interactions.

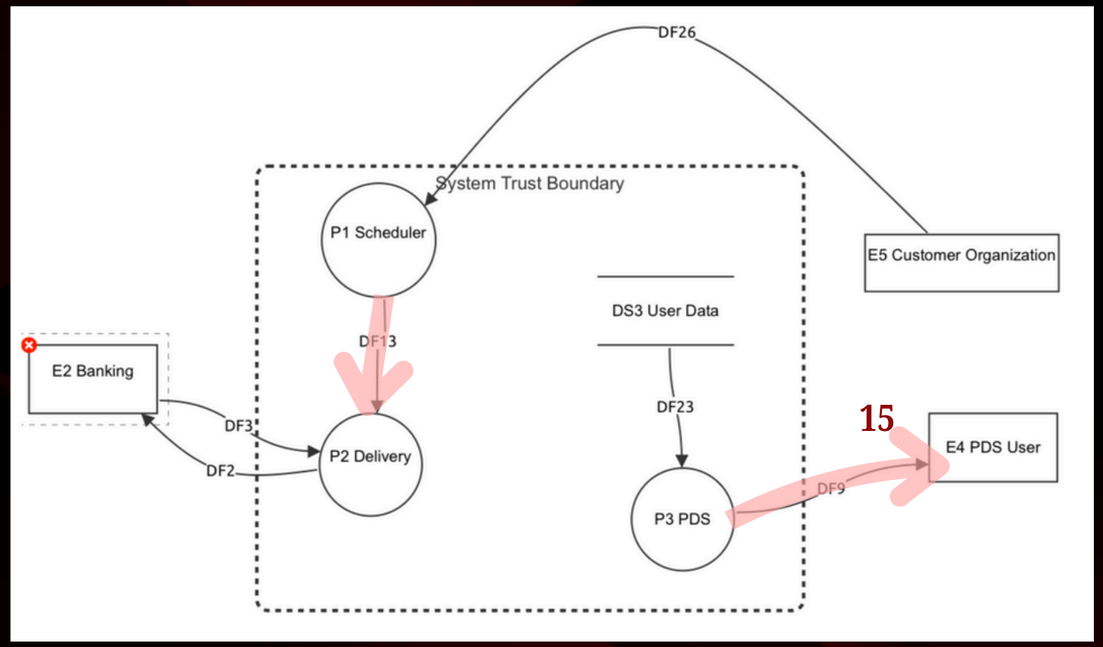
(P3)

14. Transaction parties may deny sending or receiving financial data *(DF2)*

In Data Flow DF2, transaction-related data is sent from the Delivery process to the Banking service. If the system lacks strong non-repudiation mechanisms, either party may later deny having sent or received specific financial transactions. This can lead to disputes, accountability gaps, and privacy risks in financial processing.

LINDDUN THREATS

DETECTABILITY (D.1, D.2) & DETECTABILITY (D.3)



15. Document delivery events to the PDS user are detectable *(DF9)*

In Data Flow DF9, the PDS process delivers requested documents to the user. While the document content itself may be protected, the delivery and access event can still be observed through network traffic, access logs, or monitoring systems. This makes user interactions with the system detectable and may reveal when a user receives or accesses documents, exposing activity patterns over time.

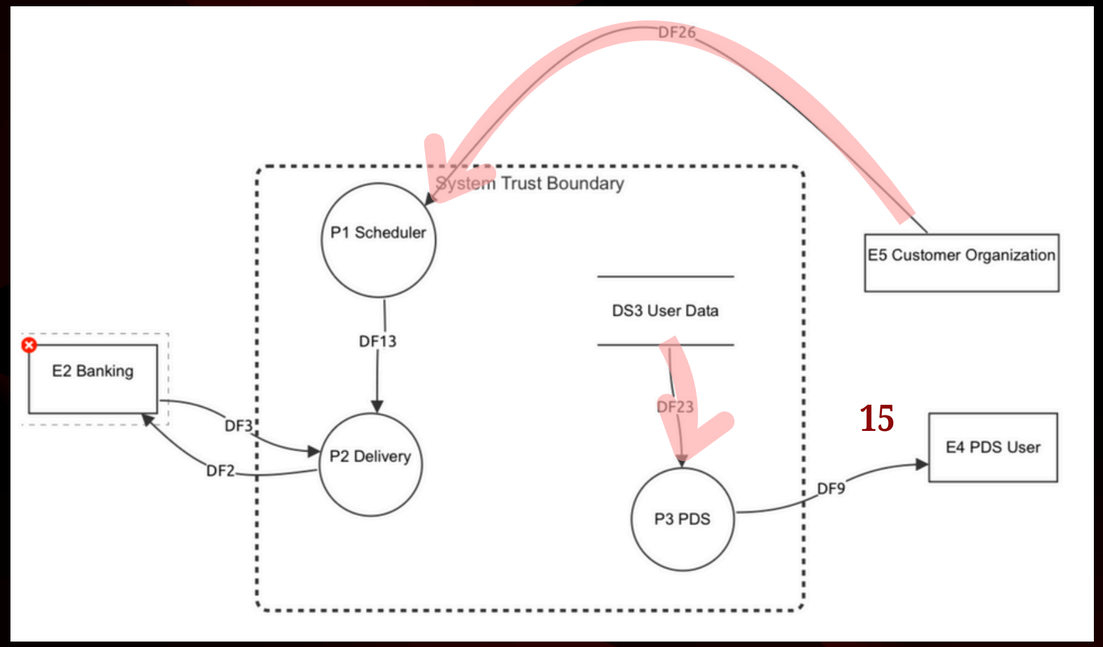
(P3)

16. Scheduling triggers to the Delivery process may be detectable *(DF13)*

DF13 represents the flow of scheduling commands from the Scheduler to the Delivery process.
These triggers control when delivery tasks start and how they are executed.
If observed through logs or monitoring, they may reveal system timing and workload patterns.

LINDDUN THREATS

LINKABILITY (1.2.1,1.2.2)



17. Repeated access to user preferences may reveal user behavior *(DF23)*

DF23 represents the retrieval of stored user information and preferences from the Personal Data Store by the PDS process.
These accesses may occur repeatedly during normal system operation.
Over time, linking these repeated accesses can reveal user behavior and preferences even without direct identification

(P3)

18. Scheduling data may expose organizational activity patterns over time. *(DF26)*

DF26 represents scheduling instructions sent from the customer organization to control when document delivery occurs.
These scheduling instructions may be repeated and follow regular patterns.
Over time, observing these patterns can reveal organizational behavior such as business volume or peak periods.