# Overview:

This document outlines the key concepts, design considerations, and workflow of file verification within our system. Its primary aim is to provide a comprehensive understanding of how file verification work.

## Purpose of the document:

The purpose of this document is to provide guidance for technical and non-technical stakeholders to gain insight into the basic principles and practices of document validation mechanisms. By detailing the processes involved, this document ensures that team members, developers, and users have an in-depth understanding of the steps and principles of document validation.

## Key Concepts and Design Considerations:

1. Authentication:

* Authentication ensures that the entity (user, system, or process) interacting with the document validation process is legitimate and authorized.
* It involves verifying the identity of a user or system before allowing access to the validation process.
* A strong authentication mechanism prevents unauthorized access to the document validation system.

1. Verification Steps:

* File type refers to the format and structure of the data in a file.
* JSON has a valid recipient, a valid issuer and a valid signature
* The recipient must have a name and email.
* The value of the valid issuer must be found in the DNS TXT record for the domain specified by the issuer
* The system should calculate the "target hash" of the json file and it must match the target hash in the JSON

1. Database Design:

* Define a well-structured database schema that captures all necessary data related to documents, validation statuses, users, and other related entities.
* Organize tables and relationships to efficiently store and retrieve authentication-related information.
* Design tables for user authentication and authorization, including roles and permissions to access authentication services.
* Implement foreign keys and indexes to establish relationships between users and their verification activities.
* Encrypt sensitive data such as user credentials to improve data security.

1. API Design:

* Define clear and intuitive API endpoints for login and file verification
* Use RESTful principles to structure routes and enable easy integration
* Implement strong authentication mechanisms, such as token-based authentication (JWT or OAuth), to ensure secure access to API endpoints.
* Plan application program interface versions to accommodate future changes without break existing integrations.
* Implement input validation and request parameter verification to prevent invalid requests.
* Define standardized request and response formats, including JSON or other suitable formats, for consistent communication between clients and the API.

## Workflow of File Verification:

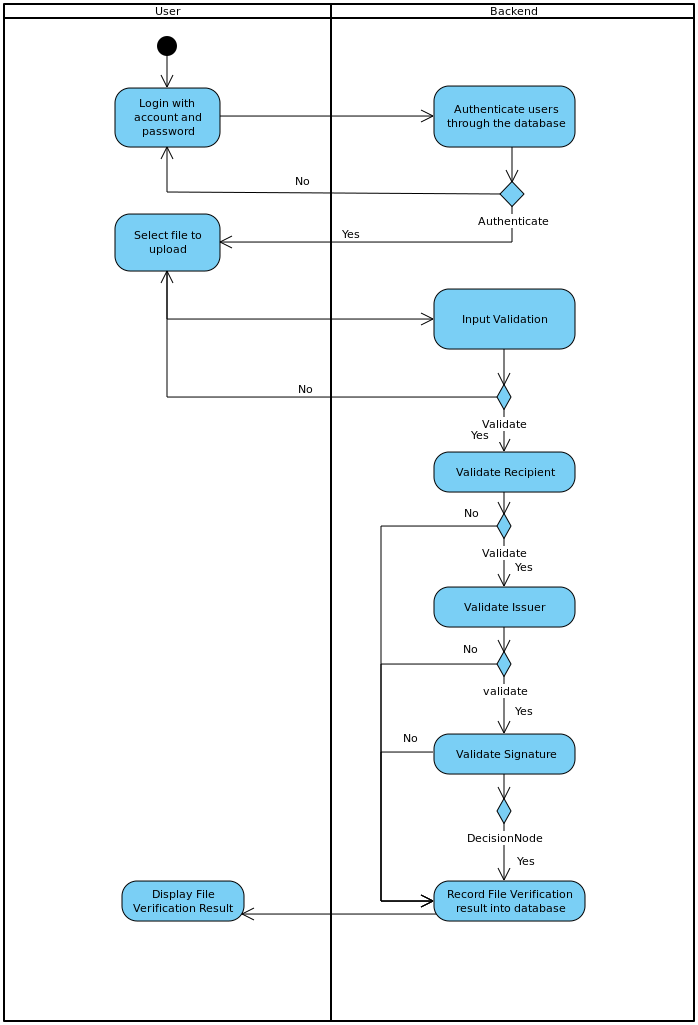


Diagram 1 : Activity Diagram of File Validation

From the activity diagram above, the user must log in to the system and get authorization before they can upload files to the system and authenticate them. Once the user is authorized and given a token, the user uses the token to upload the file to the system. If the token is valid and the file is in the correct format, the system will begin validation. The system will verify the recipient, issuer and hash signature in turn. When validation fails or succeeds at any stage, the system will return the validation result to the user and record it in the database.