# 

# ESA Coding Lab Project:

## Project 1: Zidyia Library

* Create a web app “Zidyia Library”:   
  A library repository is a collection of books and reference materials that users utilize for accessing books and citations.
  + Users can register using the following information:
    - Full Name
    - ID (Copy to be uploaded)
    - Password
    - Student Id
    - Email/Mobile
  + Users have profiles that include:
    - Profile picture
    - Bio (Short description)
    - Location
  + Users can request information or resources from libraries.
    - Users select a library from a drop-down menu.
    - Fill in a form where fields are predefined by the library.
    - Submit the request for verification.
  + Users can upload research papers or other documents.
    - Users select the owning library.
    - Upload the document.
    - Submit the document for verification.
  + Users can view:
    - Verified Documents.
    - Pending Document Requests.
    - Rejected Documents with a note explaining the reason.
  + Users can share verified documents only. (Unique QR Code for each verified document)
* Create an “Admin Dashboard” for libraries.
  + Super Admin can view analytics and data of:
    - Number of Issued Documents.
    - Number of Pending Requests.
    - Number of Approved Requests.
    - Number of Rejected Requests.
    - Number of Pending Documents.
    - Number of Approved Documents.
    - Number of Rejected Documents.
  + Super Admin can create a Tenant.
    - Data used to create a Tenant:
      * Library name
      * Location.
      * Tenant admin email.
    - Once created, tenant admin should receive an email with an auto-generated password.
    - The email and auto-generated password are used to log in to the Admin Dashboard.
    - On the first log in, the admin is requested to create a new password of their choice.
  + Super Admin can create a verifier subscription.
    - Data used to create verifier subscription:
      * Organization name.
      * Location.
      * Organization admin/HR/hiring manager email.
      * Subscription Expiry date.
    - Expiry date can be a specific date, or an auto-generated date for one year from creation.
    - Once a subscription is expired, the admin of the organization can no longer access the Verification Platform.
    - Users with expired licenses can log in, but instead of accessing the Verification Platform, they will be redirected to an HTTP 498 "Expired License Page."
    - Once created, subscribers should receive an email with an auto-generated password.
    - The email and auto-generated password are used to log in to the Verifier Platform.
    - On the first log in, the subscriber is requested to create a new password of their choice.

Note: Students are required to implement API integration. Please be aware that the design will be provided to you. Students are tasked with creating an API that transmits data in a format similar to what is anticipated in the Zendy Search Library API. Students have to utilize dummy resources and data from the database to demonstrate their work.

## Project 2: Zidyia Passport

* Create a web app “Zidyia Passport.”
  + Students can register using the following information:
    - Full Name
    - ID (Copy to be uploaded)
    - Password
    - Student Id
    - Email/Mobile
  + Students have profiles that include:
    - Profile picture
    - Bio (Short description)
    - Location
  + Students can add/create a certificate.
    - Students write the certificate name and body.
    - Specify the issuing and expiry dates.
    - Submit the certificate for verification.
  + Students can view:
    - Verified Certificates/Badges.
    - Pending Certificates.
    - Rejected Certificate with a note explaining the reason.
  + Students can share verified certificate only. (Unique QR Code for each verified certificate)
  + Verify a Certificate:
    - Meaning: Upload it from your files to confirm the authenticity and accuracy of a certificate.
    - Usage: Blockchain technology becomes ideally suited in this scenario. Simply put, Blockchain is a distributed ledger technology that securely records transactions. Data kept in the Blockchain is impossible to tamper with and when a certificate gets created and stored in the Blockchain, it automatically becomes immutable. With no single point of control for Blockchain, data once written cannot be altered. This ensures that a certificate is not a counterfeit one. When someone verifies a certificate, they typically check its details and validate that it was issued by a legitimate authority. This process ensures that the certificate is genuine and trustworthy.
  + Mint a Certificate:
    - Meaning: To create or generate a new certificate.
    - Usage: In the context of digital or blockchain certificates, "minting" refers to the process of creating a new certificate. This involves generating the certificate, assigning relevant information, and often adding it to a blockchain or a secure database.
  + Share an academic transcript
    - Student Initiation: Students, registered on the Zidyia Passport platform, can initiate the process of sharing their academic transcript.
    - Requesting Transcript: The student sends a request to share their academic transcript with a specific institution or individual. This request may involve selecting the target institution or individual from a list provided on the platform.
    - Institutional Verification: If the request is directed towards an educational institution, the platform contacts the institution to verify the authenticity of the request.
    - Authorization and Form Filling: Once verified, the student may be required to fill in a form with specific fields as defined by the institution. This ensures that the information shared is accurate and in the format expected by the receiving party.
    - Uploading Certificates and Documents: Students may be given the option to upload additional certificates or documents to support the information on their academic transcript.
    - Verification and Approval: The institution or relevant authority reviews the submitted information, verifies it, and decides whether to approve or reject the request. Reasons for rejection may be provided.
    - Viewing Shared Transcript: If approved, the recipient (institution or individual) can view the shared academic transcript. This may be accessible through the Zidyia Passport platform.
    - Unique QR Code for Verification: To enhance security and prevent tampering, each shared academic transcript may come with a unique QR code. This QR code can be used by third parties, such as employers or other educational institutions, to quickly verify the authenticity of the transcript.
* Create an “Admin Dashboard” for institutions.
  + Admins can view analytics:
    - Number of **Issued Certificates**.
    - Number of **Pending Requests**.
    - Number of **Approved Request**.
    - Number of **Rejected Requests**.
    - Number of **Pending Documents**.
    - Number of **Approved Documents**.
    - Number of **Rejected Documents**.
    - Analytics should be filterable by date span.
  + Admins can customize the fields for certificate requests.
    - Specify fields.
    - Fields types.
    - Select whether a field is optional or mandatory.
  + Admins can view students’ requests for certification.
    - Requests have 3 statuses:
      * Initially Pending
      * Verified if admin confirm applicant (Student) credentials and rightfulness of the requested certificate.
      * Rejected if admins can’t authenticate applicant (student) credentials or validate the rightfulness of the requested certificate.
      * Rejected request should have a note with the reason for rejection.
  + Admins can view students’ uploaded certificates for validation.
    - Uploaded certificates have 3 statuses:
      * Initially Pending
      * Verified if the admin can verify the student’s credentials and the authenticity of the uploaded degree.
      * Rejected if the admin can’t verify the student's credentials or the authenticity of the uploaded degree.
  + Admins can issue verified certificates for students registered (have Zidyia Passport accounts)
* Create a “Verification Platform” to be used by Employers and External Organizations.
  + The Verification Platform is only accessed by subscribed organization.
  + Subscribed organizations should have user credentials used to log in to the platform.
  + Once authenticated users can use the platform to scan Certificate QR codes shared by the student to validate the authenticity of the certificate.
* Create a “Super Admin Dashboard”
  + Super Admin can view analytics and data of:
    - Number of **Passport Users.**
    - Number of **Tenants (Issuing Institutions)**
    - Number of **Subscribers to the “Verification Platform”**
    - Number of **Issued Certificates**.
    - Number of **Pending Requests**.
    - Number of **Approved Request**.
    - Number of **Rejected Requests**.
    - Number of **Pending Documents**.
    - Number of **Approved Documents**.
    - Number of **Rejected Documents**.
  + Super Admin can create a Tenant.
    - Data used to create a Tenant:
      * Organization name
      * Location.
      * Tenant admin email.
    - Once created tenant admin should receive an email with an auto generated password.
    - The email and autogenerated password are used to log in to the Admin Dashboard.
    - On the first Log in the admin is requested to create a new password of their choice.
  + Super Admin can create a verifier subscription.
    - Data used to create verifier subscription:
      * Organization name.
      * Location.
      * Organization admin/HR/hiring manager email.
      * Subscription Expiry date.
        + Expiry date can be a specific date, or an auto generated date for one year from creation.
        + Once a subscription is expired the admin of the organization can no longer access the Verification Platform.
        + Users with expired license can log in but instead of accessing the Verification Platform they will be redirected to a HTTP 498 “Expired License Page.”
    - Once created Subscribers should receive an email with an auto generated password.
    - The email and autogenerated password are used to log in to the Verifier Platform.
    - On the first Log in the subscriber is requested to create a new password of their choice.