**Password Manager Web Project** system. This diagram represents the flow and interaction between the various components, such as the web app, APIs, and external services like AWS, Azure, AD, and certificate authorities.



**Explanation of the diagram:**

1. **Web Interface**: The admin or user interacts with a web-based dashboard to manage and access passwords.
2. **Backend APIs**: This is the core logic that handles password generation, storage, and retrieval. It communicates with external services through specific APIs.
3. **API Layer**:
   * **AWS API**: Integrates with AWS to manage passwords for IAM roles, access keys, etc.
   * **Azure API**: Handles password storage, generation, and rotation for Azure resources.
   * **AD API**: Communicates with Active Directory (LDAP) to update and manage AD passwords.
   * **Certificate API**: Manages SSL/TLS certificates (e.g., creation and renewal).
4. **Certificate Authority**: A trusted entity responsible for issuing and managing SSL/TLS certificates.
5. **LDAP (Active Directory)**: Integrates with your organization’s AD to securely update user passwords.