**Feature List for New Authentication Engine**

**Feature1:** Add Sign up Basic field details in Authentication Engine  
**Feature2:** Add the Google Identity Services (GIS)  
**Feature3:** Add the Password Reset or Account Recovery Process.

**Feature 1: Add Sign-Up Basic Field Details in Authentication Engine**

Full Name – Text Input (Required)

* Captures both first and last names of the user.
* Must be 8-12 characters long, containing at least one uppercase letter, one number, and one special character.

Implementation Steps:

1️. Update the UI – Add a Full Name field in the Sign-Up Form.  
2. Modify the Database – Create a Full Name column in the authentication table.  
3️.Integrate UI with DB – Ensure that when a user creates an account, their Full Name is stored in the database.  
4️. Display in the App – Show the Full Name in the UI instead of Email ID where applicable.

**Feature 2:**

**Add Sign up Basic field details in Authentication Engine**

**Google Identity Services (GIS) - Brief Documentation**

Google Identity Services (GIS) provides a seamless and secure way to integrate Google authentication into applications. It enables users to sign in using their Google account credentials, reducing friction in authentication processes while ensuring security and ease of use**.**

**1. Key Features of Google Identity Services (GIS)**

✅ OAuth 2.0 & OpenID Connect – Secure authentication protocol for single sign-on (SSO).  
✅ One Tap Sign-In – Users can sign in without entering credentials every time.  
✅ Token-Based Authentication – Uses JWT (JSON Web Tokens) for secure session handling.  
✅ Multi-Device & Cross-Platform Support – Works across web, mobile, and native applications.  
✅ Enhanced Security & Privacy – Protects against phishing and unauthorized access.

**2. How GIS Works in the Authentication Engine**

**A. User Sign-Up/Login Flow**

1. User clicks "Sign in with Google".
2. Redirects to Google Authentication Page – Requests user consent for account access.
3. Google verifies credentials and generates an ID token.
4. The ID token is sent back to the application (backend validation is recommended).
5. The application validates the token using Google's public key and logs in the user.

**3. Steps to Implement Google Identity Services (GIS)**

**A. Register Your App in Google Cloud Console**

1. Go to Google Cloud Console.
2. Create a new OAuth 2.0 Client ID.
3. Configure redirect URIs (e.g., https://yourapp.com/auth/callback).
4. Obtain the Client ID and Client Secret.

**Feature3:**

**Add the Password Reset or Account Recovery Process.**

**Password Reset or Account Recovery Process - Documentation**

The Password Reset or Account Recovery Process is a critical feature in any Authentication Engine, allowing users to recover their accounts securely if they forget their passwords or lose access.

**1. Key Features of Password Reset / Account Recovery**

✅ Secure User Identity Verification – Validate user identity via email, phone number, or security questions.  
✅ Token-Based Password Reset Links – One-time, time-limited reset links to prevent unauthorized access.  
✅ Multi-Factor Authentication (MFA) Support – Extra layer of security using OTP or biometric authentication.  
✅ Rate Limiting & CAPTCHA – Prevents brute-force attacks and automated spam requests.  
✅ Logging & Monitoring – Tracks password reset attempts for security auditing.

**2. Password Reset Workflow**

**A. Standard Password Reset Flow**

1. User clicks "Forgot Password?" on the login screen.
2. User enters email or phone number associated with the account.
3. System sends a one-time reset link or OTP to the provided email/phone.
4. User clicks the reset link or enters OTP to verify identity.
5. System prompts user to set a new password.
6. User confirms the new password and submits the request.
7. Password is updated, and the user can log in with the new password.