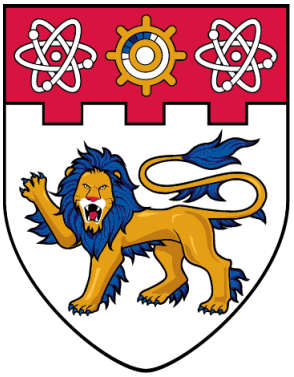
NANYANG TECHNOLOGICAL UNIVERSITY
COLLEGE OF COMPUTING AND DATA SCIENCE



NANYANG
TECHNOLOGICAL
UNIVERSITY
SINGAPORE

"TITLES TITLES"

By
NGUYEN PHUONG LINH

Project Supervisor: Prof Chng Eng Siong
Examiner: A/P Douglas Leslie Maskell

Singapore
Academic Year 2025/2026

Abstract

This project focuses on the design and implementation of the **Gateway Dashboard**, a comprehensive management interface for the Speech Gateway API, alongside critical backend enhancements to support secure authentication and monetization. The system addresses the need for a robust, user-friendly platform to manage access and subscriptions for speech processing services.

On the frontend, a responsive Single Page Application (SPA) was developed using **Vue.js** and **Vuetify**, featuring a modular architecture that ensures scalability and maintainability. Key implemented features include a secure authentication system supporting **Email/Password**, **Google OAuth 2.0**, and **Apple Sign-In**, enhancing user accessibility and security.

The backend, built with **NestJS**, was significantly upgraded to include a **Token Management System** ensuring session security through token blacklisting and automatic expiration handling using Redis and MongoDB TTL indexes. Furthermore, a **Subscription and Payment Module** was integrated using **Stripe**, enabling automated recurring billing, plan management, and real-time subscription status tracking. Storage solutions utilizing **MongoDB** for persistent data and **Redis** for caching were implemented to optimize performance.

The result is a production-ready dashboard that facilitates seamless user onboarding, secure identity management, and a flexible subscription model, thereby establishing a solid foundation for the commercialization of the Speech Gateway services.

Acknowledgement

I would like to express my deepest gratitude to my supervisor, [**Supervisor Name**], for their invaluable guidance, continuous encouragement, and expert advice throughout the course of this Final Year Project. Their insights were instrumental in shaping the direction and reliability of this system.

I extend my sincere thanks to the **NTU Speech Lab** team for providing the necessary resources and technical environment to develop this project. The opportunity to work with real-world technologies like NestJS, Vue.js, and cloud infrastructure has been an immensely rewarding learning experience.

I am also grateful to my friends and family for their unwavering support and patience during the intense periods of development and debugging. Their belief in my abilities kept me motivated to overcome the technical challenges encountered along the way.

Finally, I would like to thank [**University Name/School Name**] for providing the academic foundation that made this work possible.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

In the rapidly evolving landscape of speech processing technologies, the **Speech Gateway API** serves as a critical infrastructure for delivering advanced speech services to various applications. As the demand for these services grows, the need for a robust, centralized management system becomes paramount. Traditionally, interacting with such APIs required direct integration and manual management, which can be inefficient for end-users and administrators alike.

The **Gateway Dashboard** project was initiated to bridge this gap, providing a user-friendly graphical interface that empowers users to manage their speech processing tasks while giving administrators the tools needed to oversee system operations, manage users, and monetize services effectively.

1.2 Problem Statement

Prior to this project, the Speech Gateway ecosystem faced several challenges:

1. **Lack of User Interface:** Users had to rely on raw API calls or command-line tools to interact with speech services, which posed a high barrier to entry.

2. **Limited Access Control:** The existing system lacked a flexible authentication mechanism, supporting only basic credentials without modern Single Sign-On (SSO) capabilities.

3. **Absence of Monetization Infrastructure:** There was no automated system to handle subscriptions, billing, or tiered access plans, hindering the commercial viability of the services.

4. **Inefficient Administration:** Managing user accounts, permissions, and service plans required manual database interventions, which is not scalable.

1.3 Project Objectives

The primary objective of this project is to design and implement a comprehensive **Gateway Dashboard** and enhance the backend infrastructure to support commercial-grade features. Specific objectives include:

- **Develop a web-based dashboard** using Vue.js and Vuetify to provide an intuitive interface for users to access speech services and manage their data.
- **Implement a secure authentication system** supporting standard Email/Password login as well as OAuth 2.0 providers (Google) and Apple Sign-In for seamless user onboarding.
- **Design a subscription and payment module** integrating Stripe to handle recurring billing, automated invoicing, and subscription lifecycle management.
- **Create an administrative portal** for managing pricing plans, monitoring system usage, and overseeing user accounts with Role-Based Access Control (RBAC).
- **Enhance system security** through a robust token management system, including token blacklisting and session control using Redis.

1.4 Project Scope

The project scope encompasses both frontend and backend development:

1.4.1 Frontend Development

The frontend is built as a Single Page Application (SPA) using the **Vue.js 2** framework with **Vuetify** for UI components. Key deliverables include:

- Public pages for Authentication (Sign In, Sign Up, OAuth handling).
- User Dashboard for subscription management and service usage.
- Admin Dashboard for plans management (JSON editor with validation) and system monitoring.
- Navigation guards and interceptors for secure routing and API communication.

1.4.2 Backend Development

The backend enhancements are implemented within the existing **NestJS** API Gateway. The scope includes:

- **Auth Module:** Implementation of Google/Apple SSO strategies, JWT handling, and token security features (revocation, blacklisting).
- **Payment Module:** Integration with Stripe API for checkout sessions, webhooks, and subscription synchronization.
- **Plans Module:** A versioned, database-driven system for managing service plans with Redis caching for performance.
- **Subscription Module:** Logic for quota tracking (batch/live durations) and access control based on subscription status.

1.5 Report Organization

The remainder of this report is organized as follows:

- **Chapter 2**: Detailed overview of the system architecture and technology stack.
- **Chapter 3**: In-depth look at the authentication system, including SSO flows and security measures.
- **Chapter ??**: Design and implementation of the subscription and payment processing system.
- **Chapter ??**: Description of the frontend component architecture and user interface design.
- **Chapter ??**: Summary of the project achievements and suggestions for future work.

Chapter 2

System Architecture

This chapter provides a comprehensive overview of the Gateway Dashboard system architecture, detailing the technology stack, component interactions, and database design decisions that underpin the platform.

2.1 Overview

The Gateway Dashboard system follows a modern three-tier architecture consisting of a **Vue.js** frontend, a **NestJS** backend API, and integration with external services. This separation of concerns ensures scalability, maintainability, and clear boundaries between presentation, business logic, and data persistence layers.

2.1.1 High-Level Architecture

Figure 2.1 illustrates the overall system architecture. The frontend communicates with the backend through RESTful APIs, while the backend interacts with external services such as Stripe for payment processing and OAuth providers for authentication.

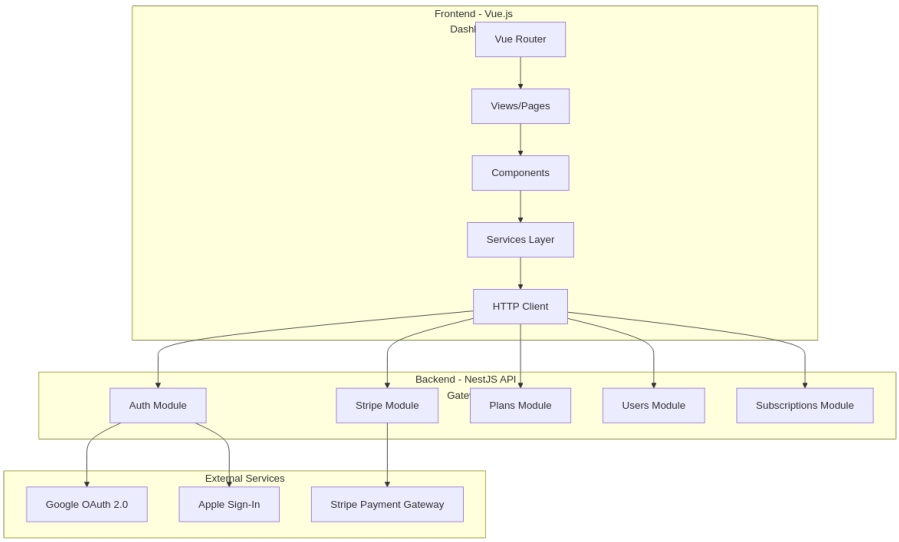


Figure 2.1: High-Level System Architecture

The architecture diagram details the data flow within the system. The **Frontend** layer consists of Vue Router directing requests to Views/Pages, which utilize Components and

a Services Layer that communicates via an HTTP Client. The **Backend** layer comprises modular NestJS components: Auth, Stripe, Plans, Users, and Subscriptions modules. The **External Services** layer includes Google OAuth 2.0, Apple Sign-In, and Stripe Payment Gateway for third-party integrations.

2.1.2 Component Overview

The system is composed of the following major components:

- **Frontend Dashboard**: A Single Page Application (SPA) built with Vue.js 2 and Vuetify, providing user interfaces for authentication, subscription management, and administrative functions.
- **Backend API Gateway**: A NestJS-based REST API that handles authentication, authorization, business logic, and orchestration of external services.
- **Database Layer**: MongoDB serves as the primary data store for users, subscriptions, plans, and tokens, with Redis providing caching for frequently accessed data.
- **External Services**: Integration with Google OAuth 2.0, Apple Sign-In, and Stripe for third-party authentication and payment processing.

2.1.3 Communication Flow

The typical request flow proceeds as follows:

1. The user interacts with the Vue.js frontend through the browser.
2. The frontend dispatches HTTP requests to the backend API via Axios interceptors.
3. The backend validates the JWT token, checks authorization, and processes the request.
4. Business logic is executed, interacting with MongoDB, Redis, or external APIs as needed.
5. The response is returned to the frontend, which updates the user interface accordingly.

2.2 Technology Stack

The Gateway Dashboard leverages modern, industry-standard technologies to ensure robustness, scalability, and developer productivity.

2.2.1 Frontend Technologies

Technology	Version	Purpose
Vue.js	2.x	Progressive JavaScript framework for building user interfaces
Vuetify	2.x	Material Design component framework for Vue.js
Vue Router	3.x	Official router for single-page application navigation
Axios	Latest	Promise-based HTTP client for API communication

Table 2.1: Frontend Technology Stack

Vue.js 2 was selected for its gentle learning curve, excellent documentation, and reactive data binding capabilities. The framework's component-based architecture facilitates code reuse and maintainability. **Vuetify** provides a comprehensive set of Material Design components, enabling rapid UI development with a professional appearance.

2.2.2 Backend Technologies

Technology	Version	Purpose
NestJS	9.x	Progressive Node.js framework for server-side applications
TypeScript	4.x	Typed superset of JavaScript for enhanced code quality
Passport	0.6.x	Authentication middleware for Node.js
JWT	Latest	JSON Web Token for stateless authentication

Table 2.2: Backend Technology Stack

NestJS provides a modular architecture with built-in dependency injection support, ideal for enterprise-grade applications. TypeScript ensures type safety and improved developer experience. **Passport** offers a flexible authentication framework with extensive strategy support for OAuth providers.

2.2.3 Data Storage and Caching

Technology	Version	Purpose
MongoDB	5.x	NoSQL document database for flexible schema design
Redis	6.x	In-memory data store for caching and session management

Table 2.3: Storage Technologies

MongoDB was chosen for its schema flexibility, horizontal scalability, and native JSON support. **Redis** serves dual purposes: caching frequently accessed data (plans, prices) and managing token blacklists for security.

Caching Architecture

Figure 2.2 illustrates the caching architecture for the Plan module. The service layer first checks Redis for cached data, falling back to MongoDB on cache misses.

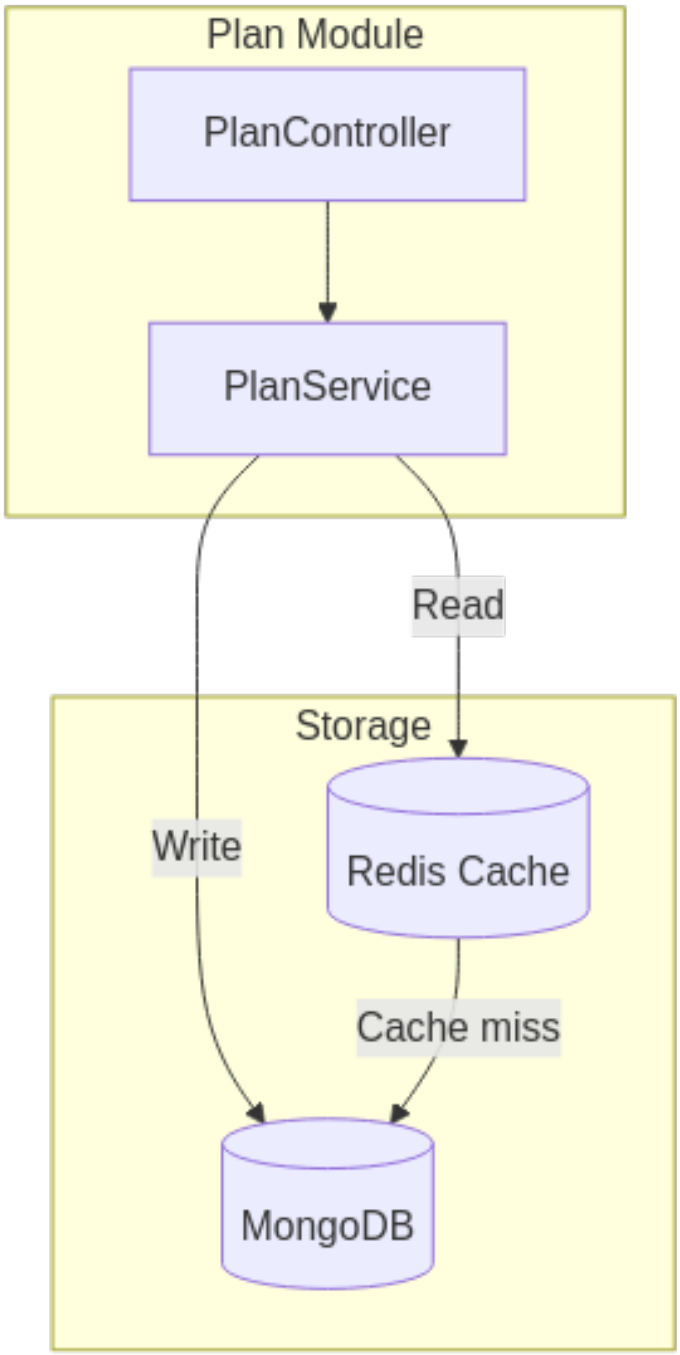


Figure 2.2: Plan Module Caching Architecture

As depicted in Figure 2.2, the Plan Module implements a read-through caching strat-

egy. When a request for plans is received, the `PlanService` first queries the Redis cache. If the data is found (cache hit), it is returned immediately. If not (cache miss), the service retrieves the data from MongoDB, stores it in Redis for future requests, and then returns it to the controller.

Figure 2.3 shows the detailed cache flow for retrieving the latest plans. This strategy includes cache penetration protection by caching NULL values for a short duration when no plans exist.

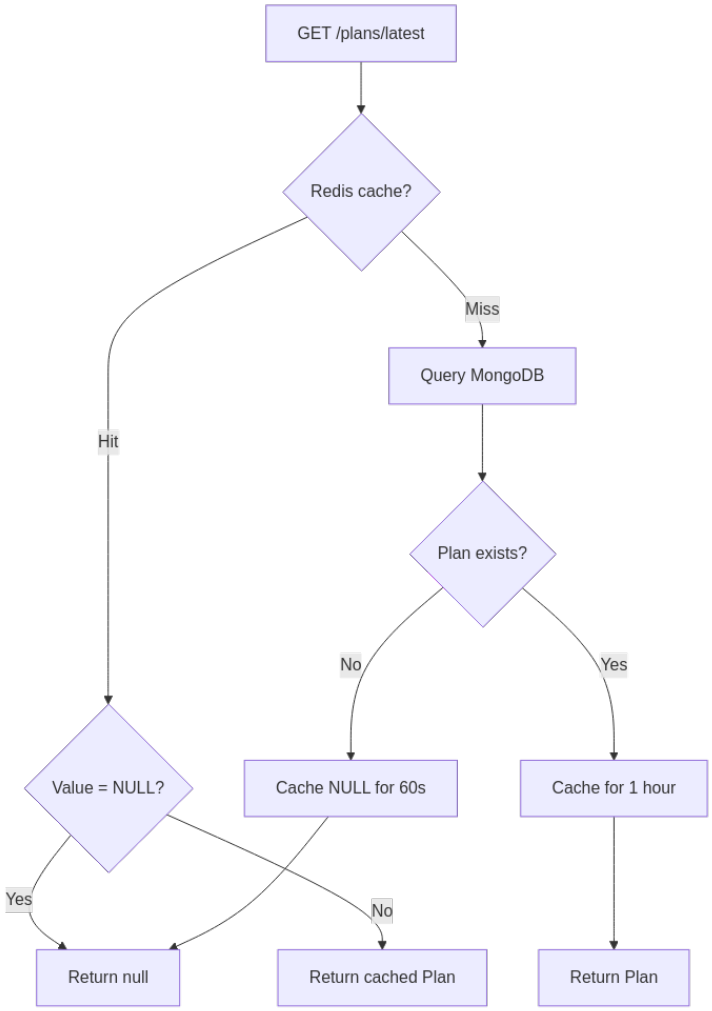


Figure 2.3: Cache Flow for Latest Plans Retrieval

Figure 2.3 provides a granular view of the "get latest plans" logic. It highlights the cache penetration protection mechanism: if a database query returns no plans, a special `NULL` value is cached for a short duration (e.g., 60 seconds). This prevents repeated queries for non-existent data from overwhelming the database essentially acting as a shield during high-traffic periods.

2.2.4 External Services

- **Stripe**: Payment processing platform for subscription billing, checkout sessions, and webhook handling.
- **Google OAuth 2.0**: Identity provider for social login functionality.

- **Apple Sign-In**: Authentication service for iOS and web users.

These third-party services were selected for their reliability, comprehensive documentation, and industry adoption, reducing development time while ensuring security and compliance.

2.3 Database Design

The database schema is designed to support user management, authentication, subscription tracking, and service plan versioning. MongoDB's document-oriented approach allows for flexible schema evolution.

2.3.1 Core Collections

The system utilizes the following primary collections:

Users Collection

The `users` collection stores user account information and authentication credentials.

Field	Type	Description
_id	ObjectId	Primary key
email	String	User email (unique)
password	String	Hashed password
name	String	Full name
role	String	User role (user/admin)
type	String	Account type (trial/paid)
isVerified	Boolean	Email verification status

Table 2.4: Users Collection Schema

Subscriptions Collection

The `subscriptions` collection tracks user subscriptions and quota usage.

Field	Type	Description
_id	ObjectId	Primary key
user	ObjectId	Reference to users collection
stripeSubscriptionId	String	Stripe subscription ID
stripeCustomerId	String	Stripe customer ID
status	String	Subscription status
quota	Object	Service quotas (batch, live duration)
usage	Object	Current usage tracking
startDate	Date	Subscription start date
endDate	Date	Subscription end date

Table 2.5: Subscriptions Collection Schema

The `quota` and `usage` fields store nested objects tracking batch and live processing durations in seconds. A value of -1 indicates unlimited access.

Plans Collection

The `plans` collection maintains versioned service plans.

Field	Type	Description
_id	ObjectId	Primary key
id	String	Unique plan identifier
plans	String	JSON string of plan details
version	Number	Plan version (auto-increment)
createdAt	Date	Creation timestamp

Table 2.6: Plans Collection Schema

Storing plans as JSON strings enables dynamic schema evolution without database migrations.

2.3.2 Authentication Collections

To ensure secure session management, two additional collections were introduced:

UserTokens Collection

The `usertokens` collection tracks active JWT tokens for each user.

Field	Type	Description
_id	ObjectId	Primary key
userId	String	User identifier
token	String	JWT token string
expiresAt	Date	Token expiration (TTL indexed)
userAgent	String	Client user agent
ipAddress	String	Client IP address

Table 2.7: UserTokens Collection Schema

MongoDB's TTL (Time-To-Live) index on `expiresAt` automatically removes expired tokens.

TokenBlacklist Collection

The `tokenblacklists` collection stores revoked tokens to prevent reuse.

Field	Type	Description
_id	ObjectId	Primary key
token	String	Revoked JWT token
userId	String	User identifier
expiresAt	Date	Original token expiration
reason	String	Revocation reason

Table 2.8: TokenBlacklist Collection Schema

2.3.3 Entity Relationships

Figure 2.4 illustrates the relationships between core collections:

- Each `user` has zero or one `subscription`.
- Each `subscription` references a `plan` by Stripe priceId.
- Each `user` may have multiple active `tokens`.
- Revoked tokens are stored in `tokenblacklist`.

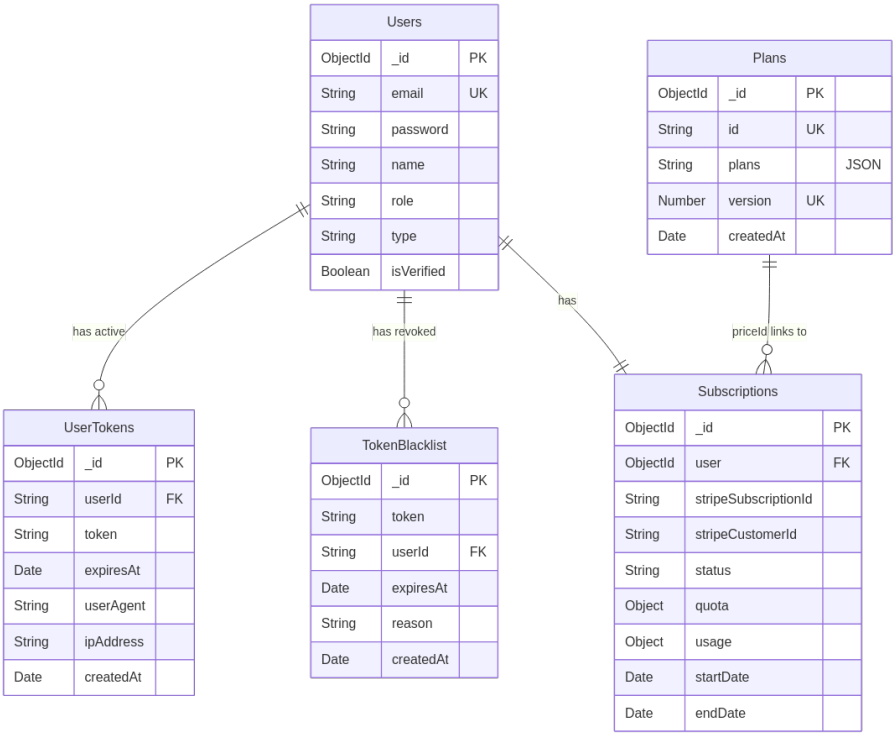


Figure 2.4: Entity Relationship Diagram

The Entity Relationship Diagram in Figure 2.4 showcases the database schema. The `Users` collection is central, linking to `Subscriptions` (1:1 relationship) and multiple `UserTokens`. The `Subscriptions` collection contains embedded objects for `quota` and `usage`, allowing efficient tracking of service limits. The `Plans` collection stands independently but is logically referenced by subscriptions via price IDs. The `TokenBlacklist` stores revoked tokens, ensuring security compliance.

Chapter 3

Authentication and Security

This chapter provides a comprehensive examination of the authentication system implemented in the Gateway Dashboard. It covers the supported authentication methods, detailed flow diagrams, token lifecycle management, and session security mechanisms.

3.1 Overview

The Gateway Dashboard implements a comprehensive authentication system supporting multiple identity providers with robust session management. This section provides an overview of the authentication architecture.

3.1.1 Supported Authentication Methods

The system supports three authentication methods:

Method	Provider	Description
Email/Password	Internal	Traditional credential-based login with bcrypt password hashing
Google OAuth 2.0	Google	Social login using Passport's Google strategy
Apple Sign-In	Apple	Authentication via identity token verification

Table 3.1: Supported Authentication Methods

3.1.2 Module Architecture

Figure 3.1 illustrates the overall architecture of the authentication modules.

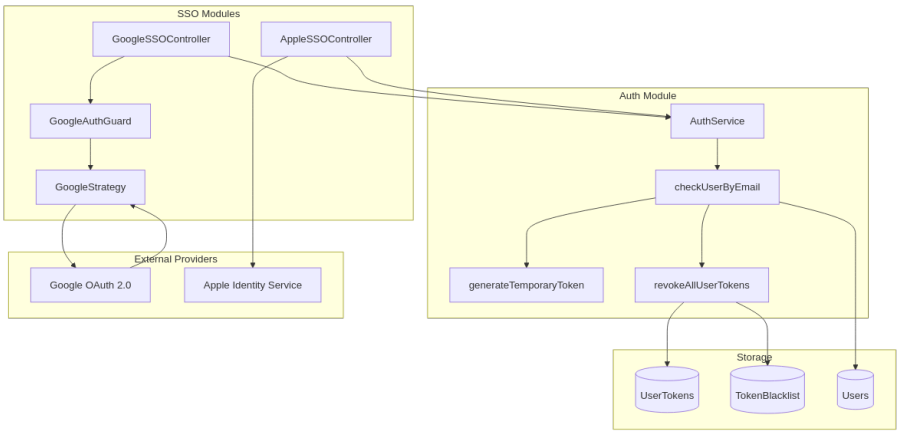


Figure 3.1: Authentication Module Architecture

The architecture consists of three main components:

- **SSO Modules**: GoogleSSOController and AppleSSOController handle OAuth flows with their respective providers.
- **Auth Module**: Central AuthService provides shared functionality including:
  - `checkUserByEmail()`
  - `generateTemporaryToken()`
  - `revokeAllUserTokens()`
- **Storage Layer**: UserTokens collection stores active sessions; TokenBlacklist stores revoked tokens; Users collection stores account data.

Both SSO controllers delegate user verification to the shared AuthService, ensuring consistent handling of new users (requiring password setup) and existing users (issuing access tokens).

3.1.3 Chapter Organization

This chapter is organized as follows:

- **Section 3.2**: Detailed authentication flows for each method
- **Section 3.3**: JWT token lifecycle and API endpoints
- **Section 3.4**: Session security mechanisms and database schemas

3.2 Authentication Flows

This section describes the detailed authentication flows for each supported method.

3.2.1 Email/Password Authentication

The traditional login flow uses Passport's LocalStrategy for credential validation. Figure 3.2 shows the sequence.

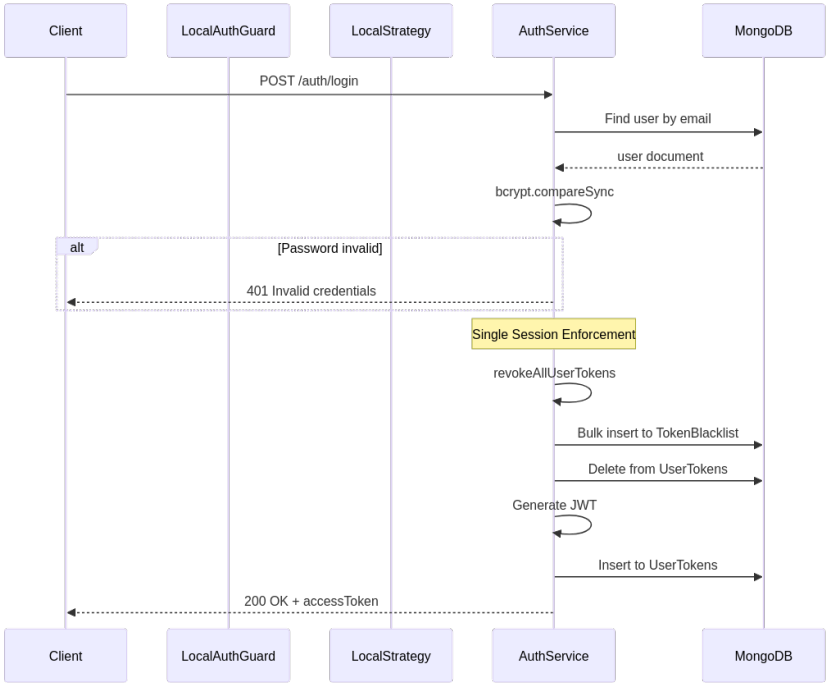


Figure 3.2: Email/Password Login Flow

The login process:

1. Client sends credentials to `POST /auth/login`.
2. LocalAuthGuard triggers LocalStrategy validation.
3. AuthService queries MongoDB and compares password hashes using bcrypt.
4. If valid, existing tokens are revoked (single session enforcement).
5. New JWT is generated and stored in UserTokens collection.
6. Response includes access token, subscription end date, and verification status.

3.2.2 Google OAuth 2.0

Google SSO uses Passport's OAuth 2.0 strategy with redirect-based authentication. This subsection covers the module architecture, authentication flow, and implementation details.

Google SSO Module Structure

Figure 3.3 shows the architecture of the Google SSO module, including its integration with Passport and the shared Auth module.

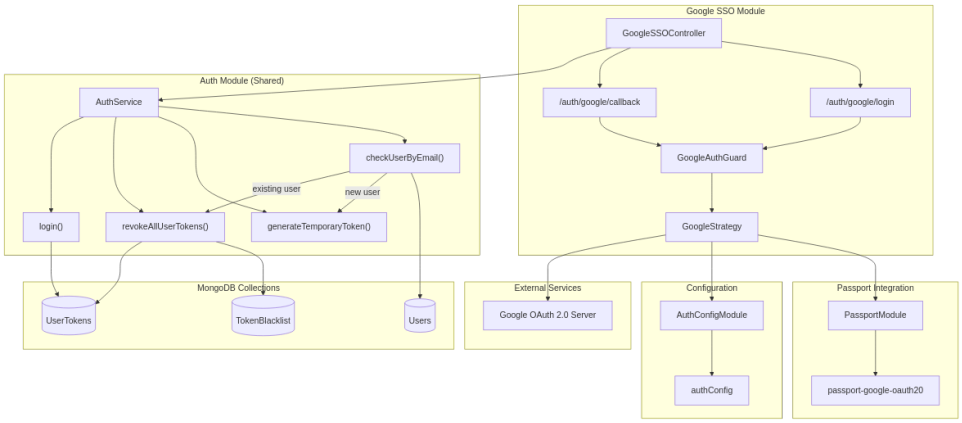


Figure 3.3: Google SSO Module Architecture

Key components include:

- **GoogleSSOController**: Exposes `/auth/google/login` and `/auth/google/callback` endpoints.
- **GoogleAuthGuard**: Extends Passport's AuthGuard with custom state parameter handling.
- **GoogleStrategy**: Implements Passport strategy with OAuth 2.0 configuration.
- **AuthService**: Shared service for user verification and token management.

Authentication Flow Overview

Figure 3.4 illustrates the high-level Google OAuth 2.0 flow.

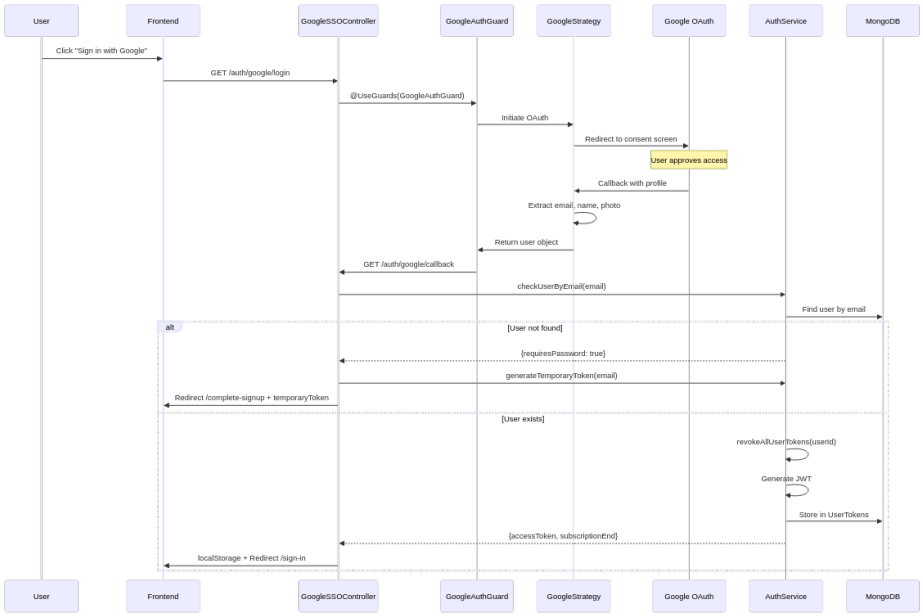


Figure 3.4: Google OAuth 2.0 Flow

Complete User Flow

Figure 3.5 provides a comprehensive flowchart of the entire Google Sign-In process, from initial click to session establishment.

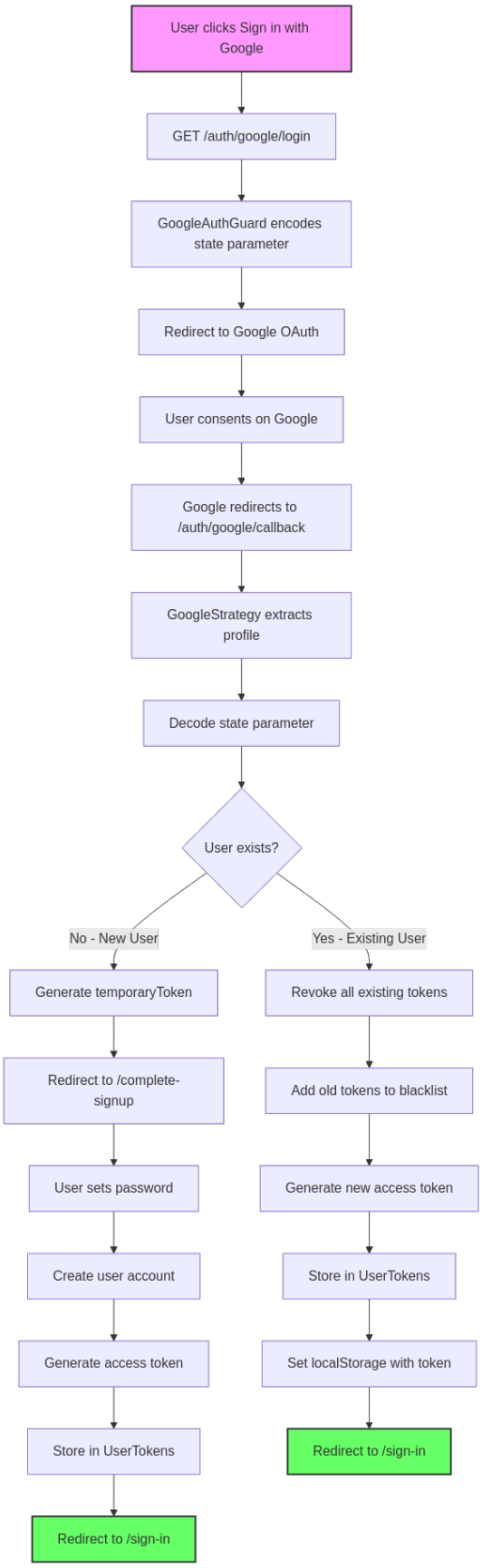


Figure 3.5: Complete Google SSO User Journey

The flow handles two scenarios:

- **New Users**: After Google authentication, the `checkUserByEmail` method indicates a new user by returning a result where `requiresPassword` is `true`. A temporary token is generated and stored in localStorage, after which the user is redirected to the complete-signup page to set their password.
- **Existing Users**: All previous tokens are revoked, a new access token is generated and stored in UserTokens collection and localStorage, then the user is redirected to sign-in.

Passport Authentication Flow

Figure 3.6 shows the detailed OAuth 2.0 authentication flow using Passport's Google strategy, including configuration and token exchange.

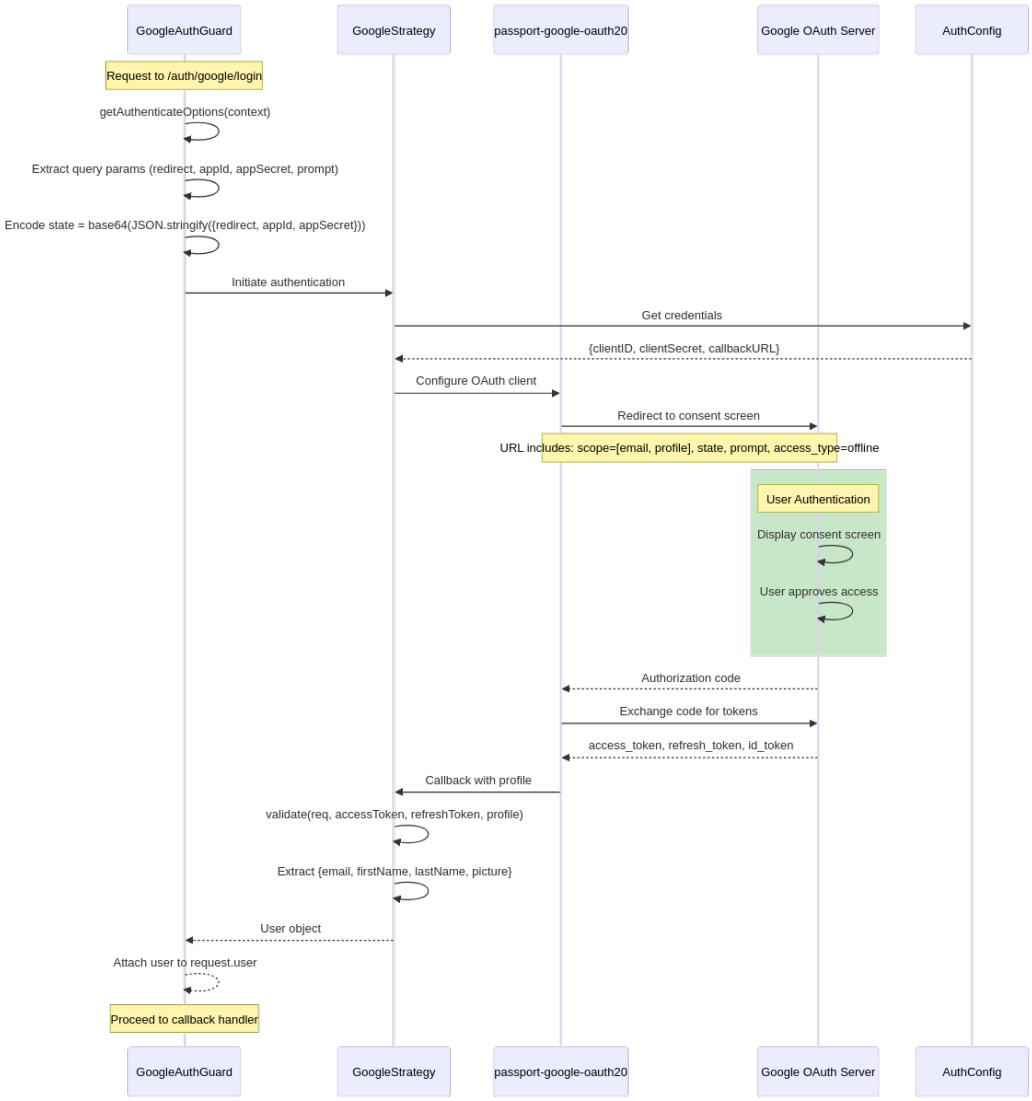


Figure 3.6: Google OAuth Passport Authentication Flow

The authentication process involves:

1. **Guard Initialization**: GoogleAuthGuard extracts query parameters and encodes them into a base64 state parameter.

2. **Strategy Configuration**: GoogleStrategy configures OAuth client with credentials from AuthConfig.

3. **Token Exchange**: After user consent, Google returns an authorization code which is exchanged for access tokens.

4. **Profile Extraction**: The strategy validates and extracts user information (email, name, photo) from the profile.

State Parameter for Context Preservation

A key feature of the Google SSO implementation is preserving query parameters through the OAuth redirect cycle using the state parameter. Figure 3.7 illustrates this mechanism.

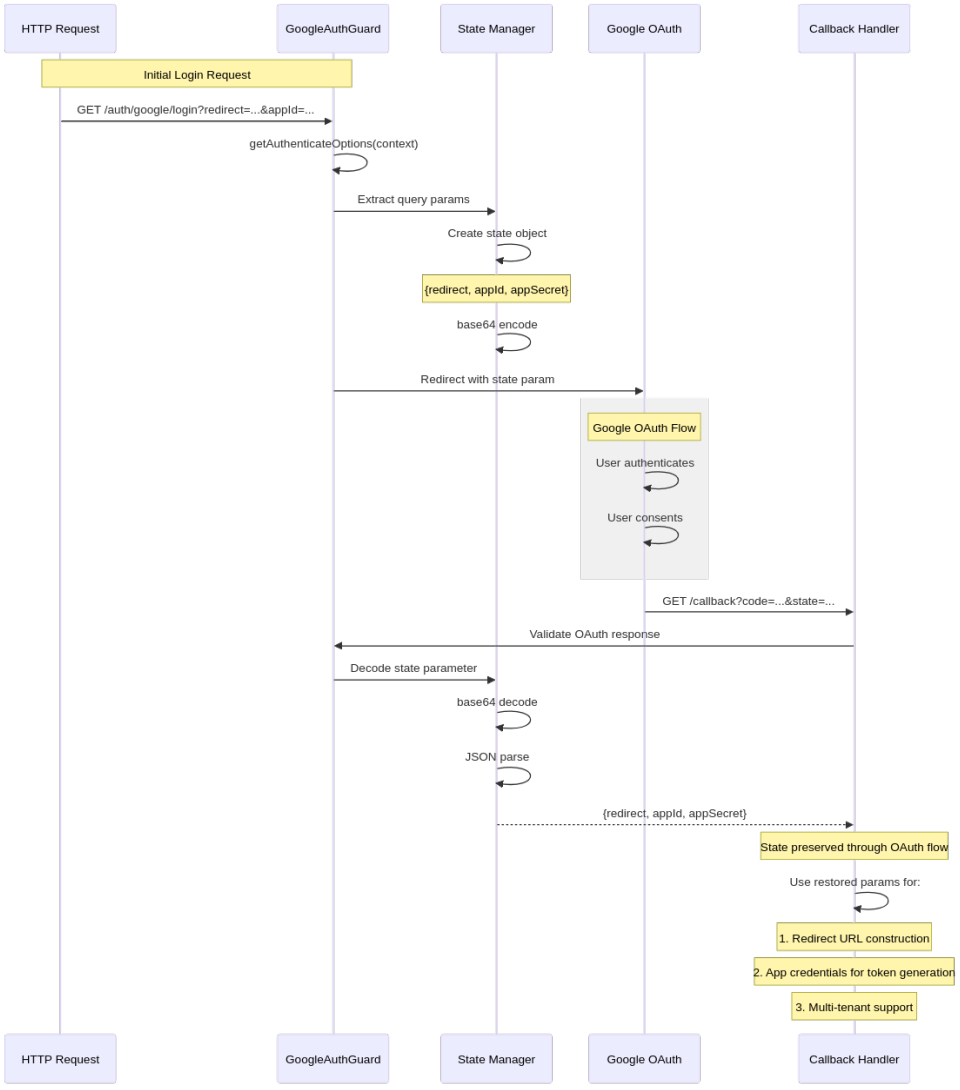


Figure 3.7: State Parameter Flow for Context Preservation

The state parameter enables:

- **Redirect URL Preservation**: Frontend callback URL is maintained across OAuth redirects.

- **Multi-tenant Support**: Application credentials (appId, appSecret) are preserved for token generation.
- **CSRF Protection**: The encoded state provides implicit protection against cross-site request forgery.

Implementation Details

Google Strategy Configuration. The GoogleStrategy extends Passport's base strategy with OAuth 2.0 configuration:

```
@Injectable()
export class GoogleStrategy extends
  PassportStrategy(Strategy, 'google') {
  constructor(@Inject(authConfig.KEY) private auth) {
    super({
      clientID: auth.googleClientId,
      clientSecret: auth.googleClientSecret,
      callbackURL: auth.googleCallbackURL,
      scope: ['email', 'profile'],
    });
  }

  async validate(req, accessToken, _refreshToken,
    profile, done) {
    const user = {
      email: profile.emails[0].value,
      firstName: profile.name.givenName,
      lastName: profile.name.familyName,
    };
    done(null, user);
  }
}
```

Listing 3.1: GoogleStrategy Implementation

Callback Handler Logic. The callback determines whether to redirect to complete-signup (new user) or sign-in (existing user):

```
@Get('callback')
@UseGuards(GoogleAuthGuard)
async googleAuthRedirect(@Req() req, @Res() res) {
  const result = await this.authService.checkUserByEmail(
    req.user.email, userAgent, ipAddress
  );

  if (result.requiresPassword) {
    // New user - generate temporary token
    const tempToken = await this.authService
      .generateTemporaryToken(result.email);
    // Redirect to /complete-signup
  } else if (result.accessToken) {
    // Existing user - store token and redirect
```

```
15    }
16 }
```

Listing 3.2: Google Callback Handler

3.2.3 Apple Sign-In

Apple Sign-In uses a POST callback with the identity token, differing from Google's redirect-based OAuth flow. This subsection covers the module architecture, authentication flow, and implementation details.

Apple SSO Module Structure

Figure 3.8 shows the architecture of the Apple SSO module and its integration with the shared Auth module.

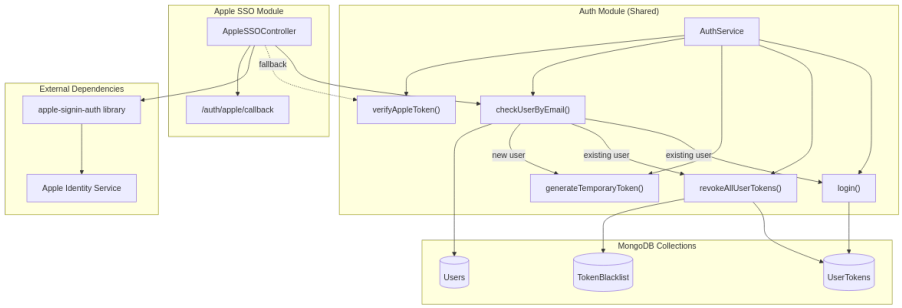


Figure 3.8: Apple SSO Module Architecture

Key components include:

- **AppleSSOController**: Handles the `POST /auth/apple/callback` endpoint.
- **apple-signin-auth library**: External dependency for token verification.
- **AuthService**: Shared service providing core functionality:
  - `verifyAppleToken()`
  - `checkUserByEmail()`
  - `generateTemporaryToken()`
  - `revokeAllUserTokens()`

Authentication Flow Overview

Figure 3.9 shows the high-level Apple Sign-In flow.

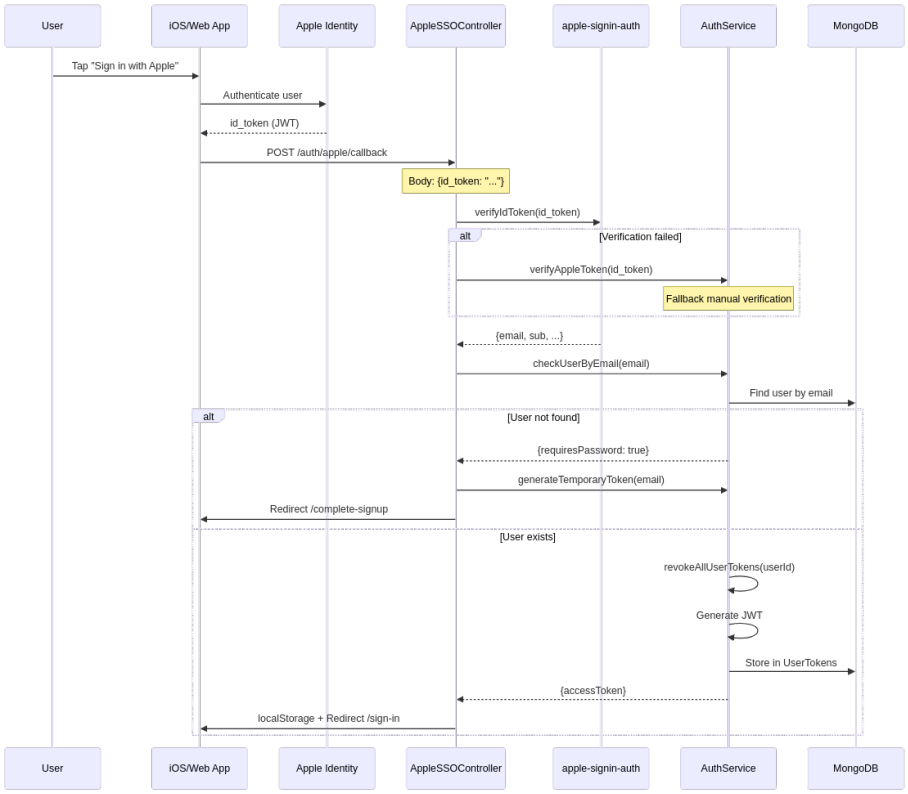


Figure 3.9: Apple Sign-In Flow

Complete User Flow

Figure 3.10 provides a comprehensive view of the entire Apple Sign-In process, from initial authentication to session establishment.

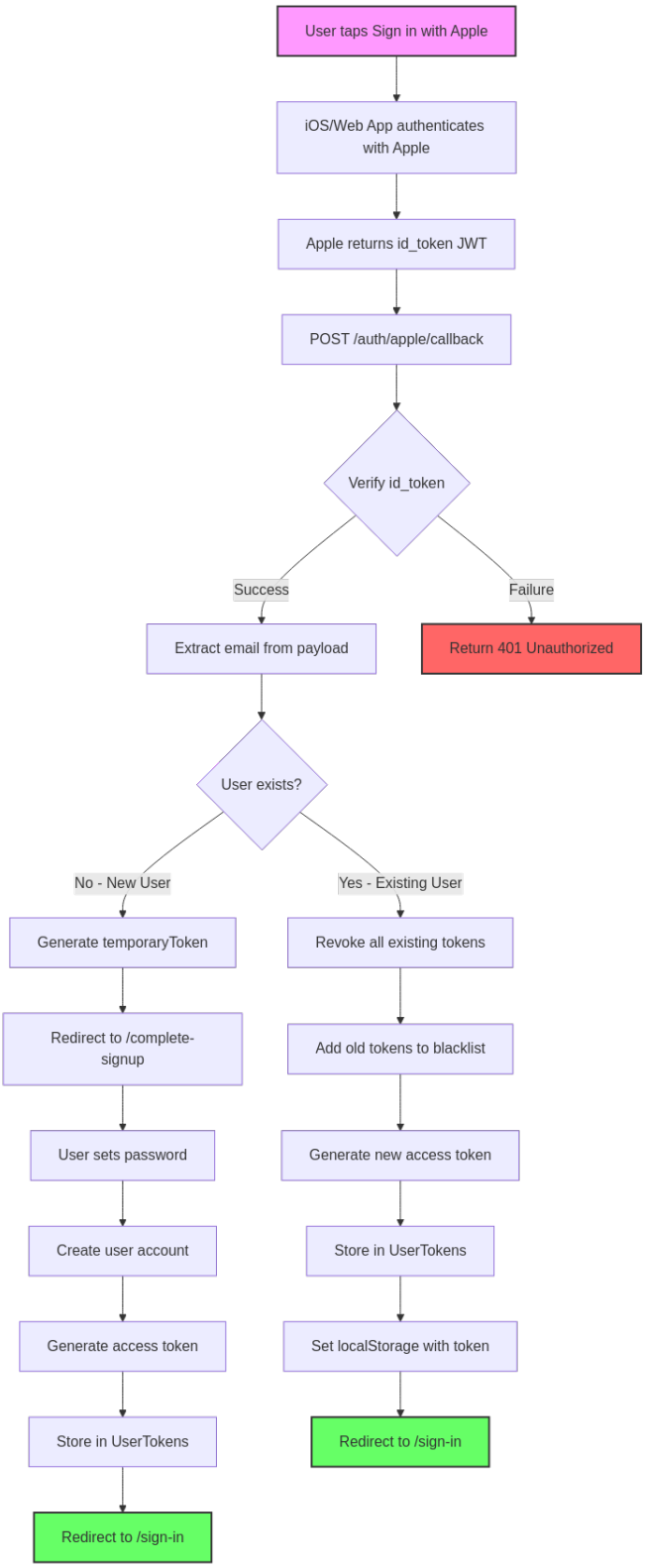


Figure 3.10: Complete Apple SSO User Journey

The flow branches based on whether the user exists:

- **New Users**: Receive a temporary token and are redirected to complete signup, where they set a password before account creation.
- **Existing Users**: Have their previous tokens revoked (single session enforcement),

receive a new access token stored in `UserTokens`, and are redirected with the token in localStorage.

Token Verification Architecture

The token verification process in Apple SSO is dual-layered. It primarily utilizes the `apple-signin-auth` library, but retains a manual fallback mechanism. Figure 3.11 illustrates this verification strategy.

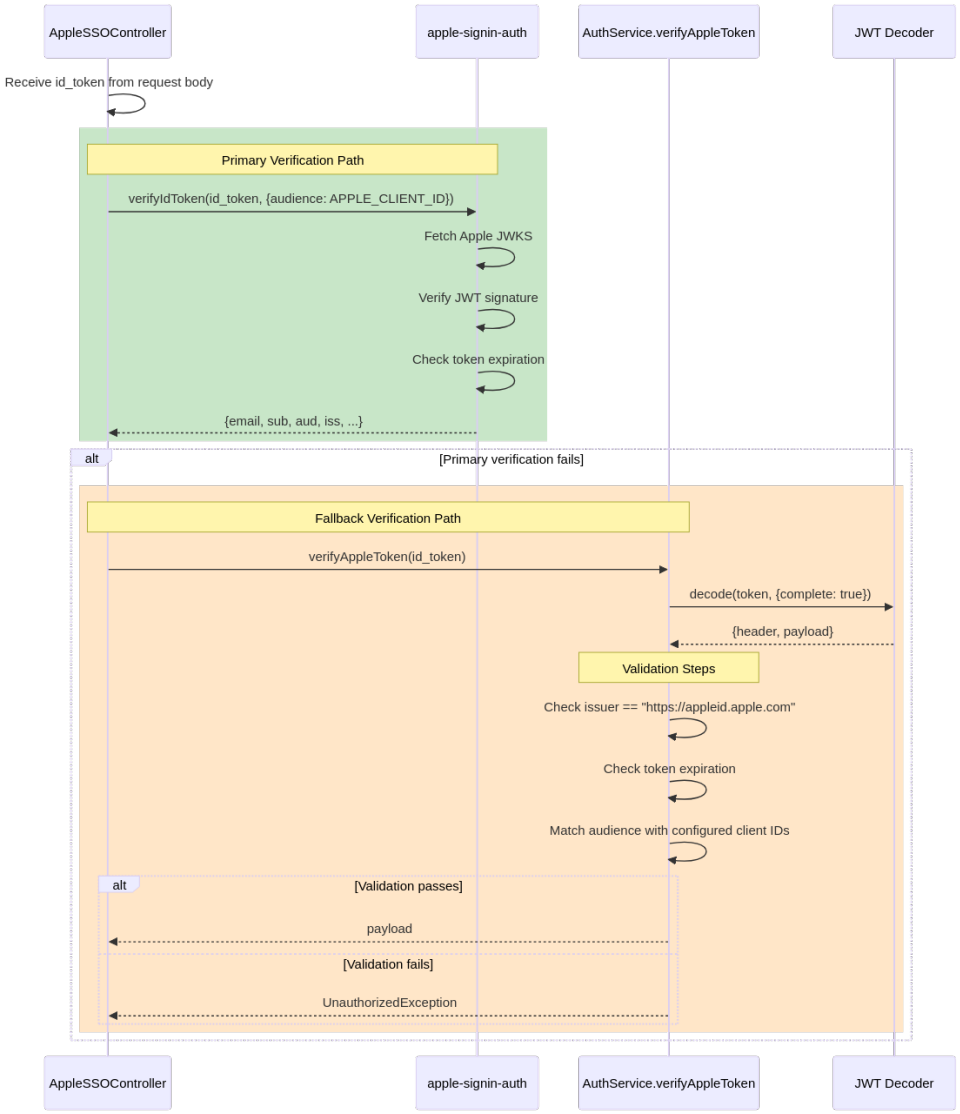


Figure 3.11: Apple SSO Token Verification Flow

The verification process:

1. **Primary Path**: The controller uses the `apple-signin-auth` library to verify the id_token. The library fetches Apple's JWKS, verifies the JWT signature, and checks token expiration.

2. **Fallback Path**: If the primary verification fails, the controller falls back to the `verifyAppleToken()` method of the `AuthService`, which manually decodes and validates the token by checking the issuer, expiration, and audience against configured Apple Client IDs.

Implementation Details

```
@Post('callback')
async appleAuthCallback(@Body() body, @Res() res) {
  let appleResponse;
  try {
    // Primary: use apple-signin-auth library
    appleResponse = await appleSignin.verifyIdToken(
      body.id_token,
      { audience: process.env.APPLE_CLIENT_ID }
    );
  } catch (error) {
    // Fallback: manual verification
    appleResponse = await this.authService
      .verifyAppleToken(body.id_token);
  }

  const result = await this.authService
    .checkUserByEmail(appleResponse.email);
  // Handle new user or existing user...
}
```

Listing 3.3: Apple Token Verification

3.2.4 Comparison of SSO Methods

Table 3.2 compares the key differences between Google OAuth and Apple Sign-In implementations.

Aspect	Google OAuth	Apple Sign-In
Flow Type	OAuth 2.0 redirect	POST with id_token
Guard	GoogleAuthGuard (Passport)	None (manual verification)
Verification	Passport strategy	apple-signin-auth library
Email Privacy	Direct email provided	May use relay email
State Management	Base64-encoded state parameter	Not applicable

Table 3.2: Google vs Apple SSO Comparison

3.3 Token Management

This section covers the JWT token lifecycle, including the API endpoints for token operations and the Auth module architecture.

3.3.1 Auth Module Architecture

Figure 3.12 shows the architecture of the Auth module, including the relationships between controllers, guards, strategies, services, and storage.

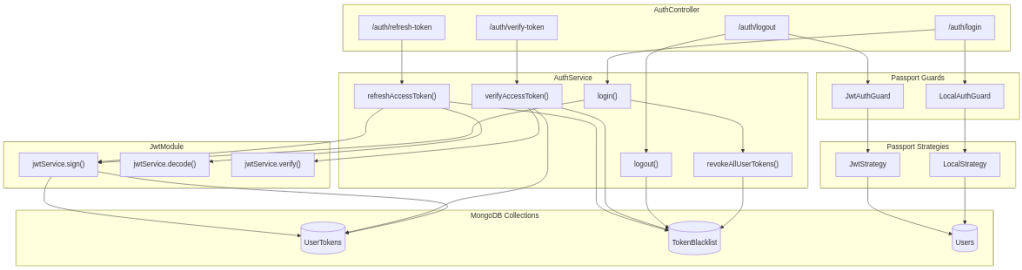


Figure 3.12: Auth Module Architecture

The module consists of:

- **AuthController**: Exposes endpoints for login, logout, token verification, and token refresh.
- **Guards**: LocalAuthGuard for credential-based login, JwtAuthGuard for protected endpoints.
- **Strategies**: LocalStrategy validates email/password, JwtStrategy validates JWT tokens with dynamic key selection.
- **AuthService**: Core business logic for token operations.
- **Storage**: UserTokens tracks active sessions, TokenBlacklist stores revoked tokens.

3.3.2 Token Lifecycle Overview

Stage	API Endpoint	Description
Generation	POST /auth/login	Creates JWT on successful authentication
Verification	POST /auth/verify-token	Validates token against blacklist and expiry
Refresh	POST /auth/refresh-token	Issues new token, blacklists old one
Revocation	POST /auth/logout	Adds token to blacklist immediately

Table 3.3: Token Lifecycle Stages

Figure 3.13 illustrates the complete token lifecycle sequence.

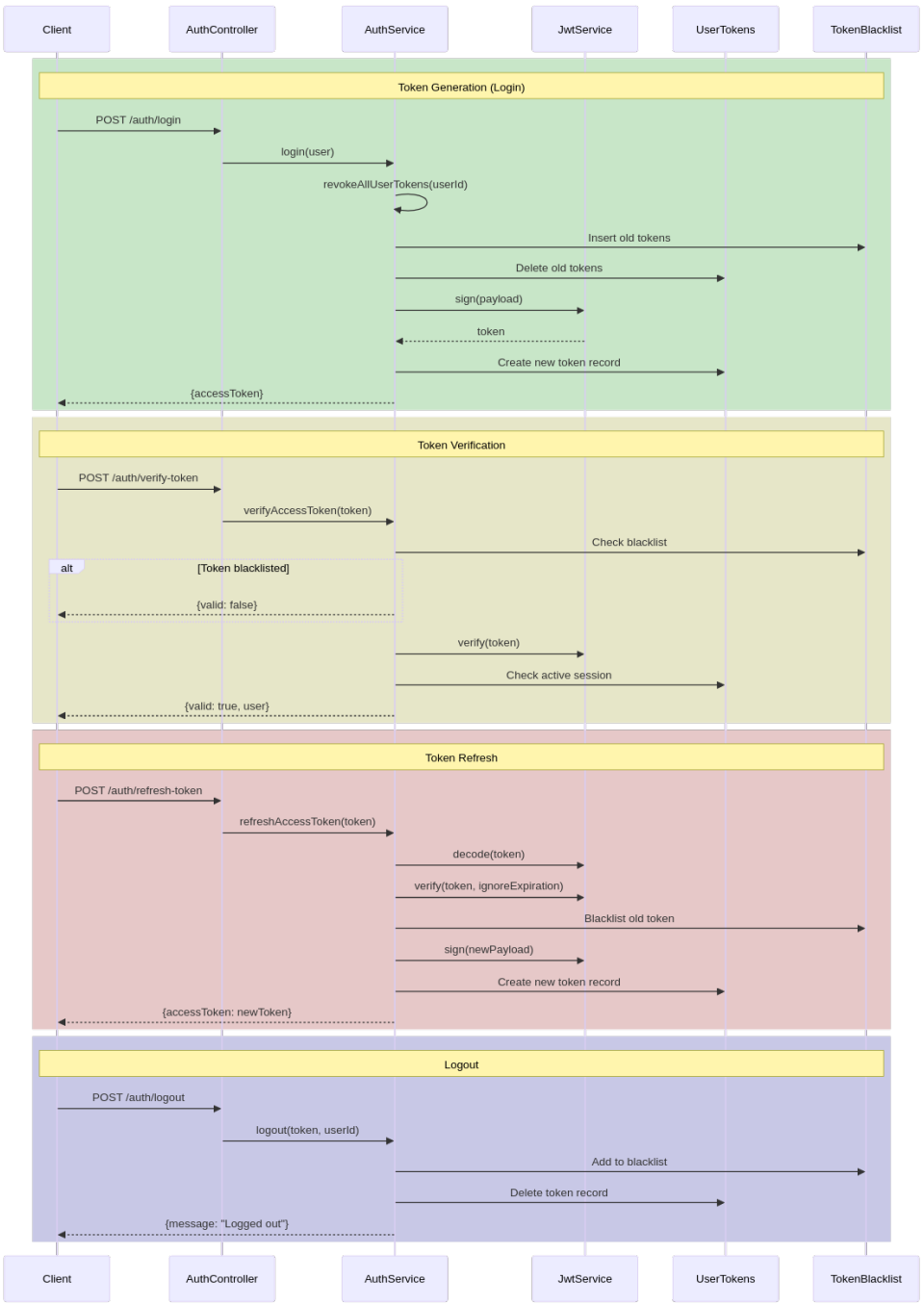


Figure 3.13: Token Lifecycle Sequence

3.3.3 Token Generation

Upon successful authentication, the AuthService generates a JWT containing user claims:

```
async login(user, userAgent, ipAddress) {
  // Revoke existing tokens (single session)
  await this.revokeAllUserTokens(user._id.toString());

  const payload = {
    email: user.email,
    role: user.role,
    name: user.name,
```

```
    type: user.type,
  };

  const token = this.jwtService.sign(payload, {
    subject: user._id.toString()
  });
  const decoded = this.jwtService.decode(token);

  // Store active token
  await this.userTokenModel.create({
    userId: user._id.toString(),
    token,
    expiresAt: new Date(decoded.exp * 1000),
    userAgent,
    ipAddress,
  });

  return { accessToken: token, ... };
}
```

Listing 3.4: JWT Token Generation

3.3.4 Token Verification

The verification process involves multiple validation steps. Figure 3.14 shows the complete decision tree.

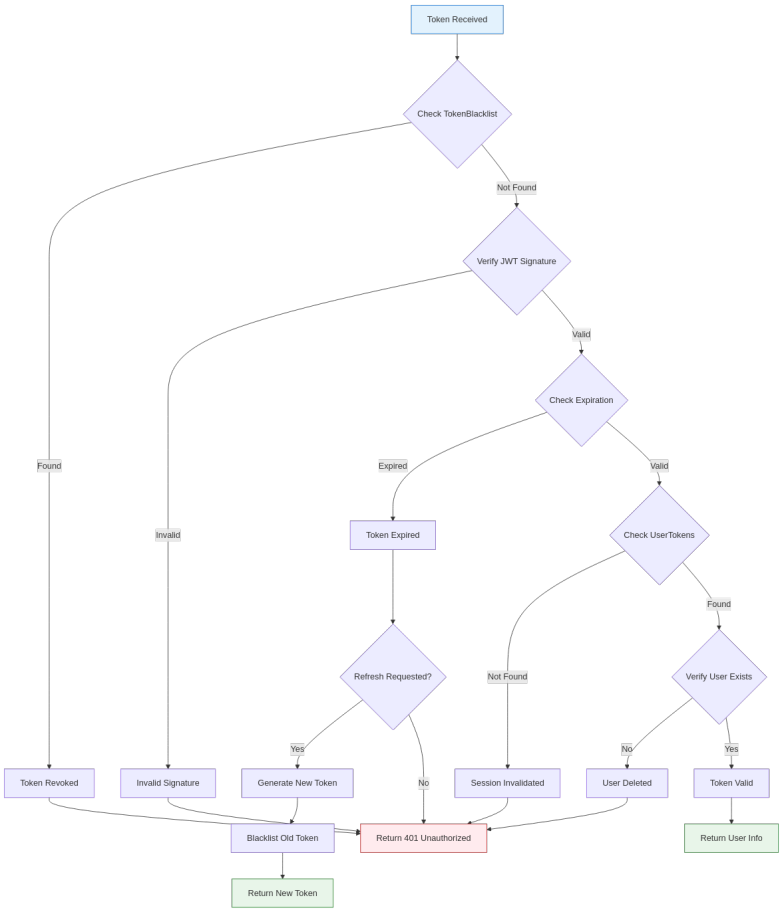


Figure 3.14: Token Verification Decision Flow

The verification endpoint checks blacklist status, signature validity, and active session existence:

```
async verifyToken(token: string) {
  // 1. Check blacklist
  const isBlacklisted = await this.tokenBlacklistModel
    .findOne({ token });
  if (isBlacklisted) {
    throw new UnauthorizedException('Token revoked');
  }

  // 2. Verify signature and expiration
  const decoded = await this.jwtService.verifyAsync(token);

  // 3. Check active session
  const activeToken = await this.userTokenModel
    .findOne({ token });
  if (!activeToken) {
    throw new UnauthorizedException('Session expired');
  }

  return { user: decoded };
}
```

Listing 3.5: Token Verification

3.3.5 JWT Validation with Dynamic Keys

The JwtStrategy supports multi-tenant authentication with dynamic key selection. Figure 3.15 shows this process.

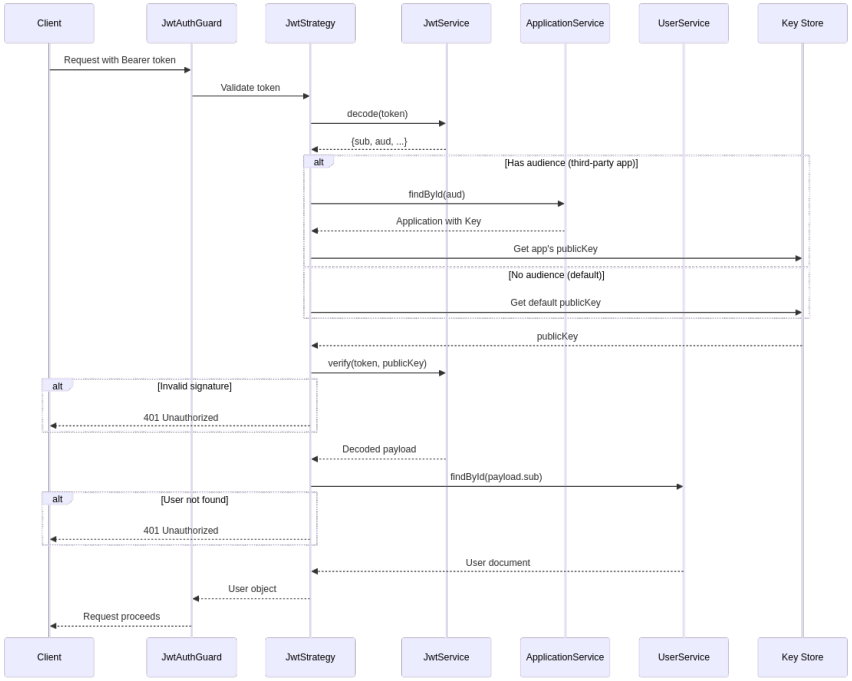


Figure 3.15: JWT Validation with Dynamic Key Selection

The strategy determines which public key to use based on the token's audience claim:

- **Default tokens**: Use the platform's default public key.
- **Third-party app tokens**: Use the application's specific public key for verification.

3.3.6 Token Refresh

The token refresh process allows clients to obtain a new access token using an expired token, provided the signature is valid. Figure 3.16 illustrates this flow.

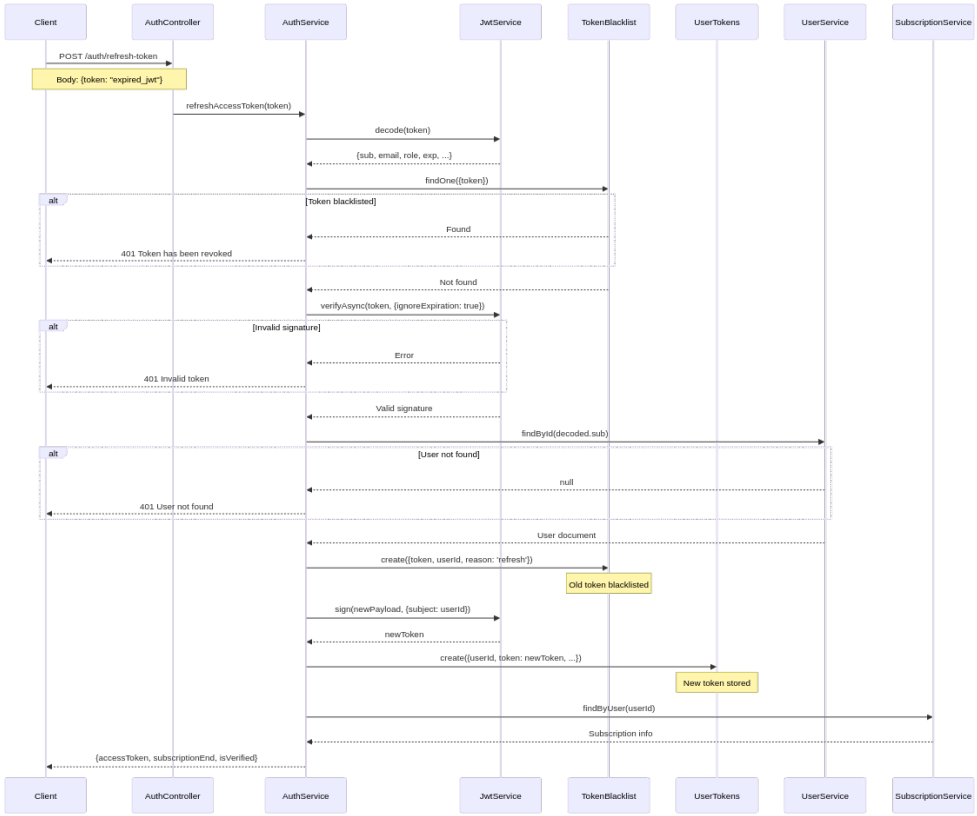


Figure 3.16: Token Refresh Flow

Refresh enables session continuation with expired tokens (signature must still be valid):

```
async refreshAccessToken(expiredToken: string) {
  // Decode without expiration check
  const decoded = this.jwtService.decode(expiredToken);

  // Verify signature only
  await this.jwtService.verifyAsync(expiredToken, {
    ignoreExpiration: true
  });

  // Blacklist old token
  await this.tokenBlacklistModel.create({
    token: expiredToken,
    userId: decoded.sub,
    expiresAt: new Date(decoded.exp * 1000),
    reason: 'refresh',
  });

  // Generate new token
  const newToken = this.jwtService.sign({...}, {
    subject: decoded.sub
  });

  return { accessToken: newToken };
}
```

Listing 3.6: Token Refresh

3.3.7 Token Revocation (Logout)

The logout process involves removing the active session and blacklisting the current token. Figure 3.17 details this sequence.

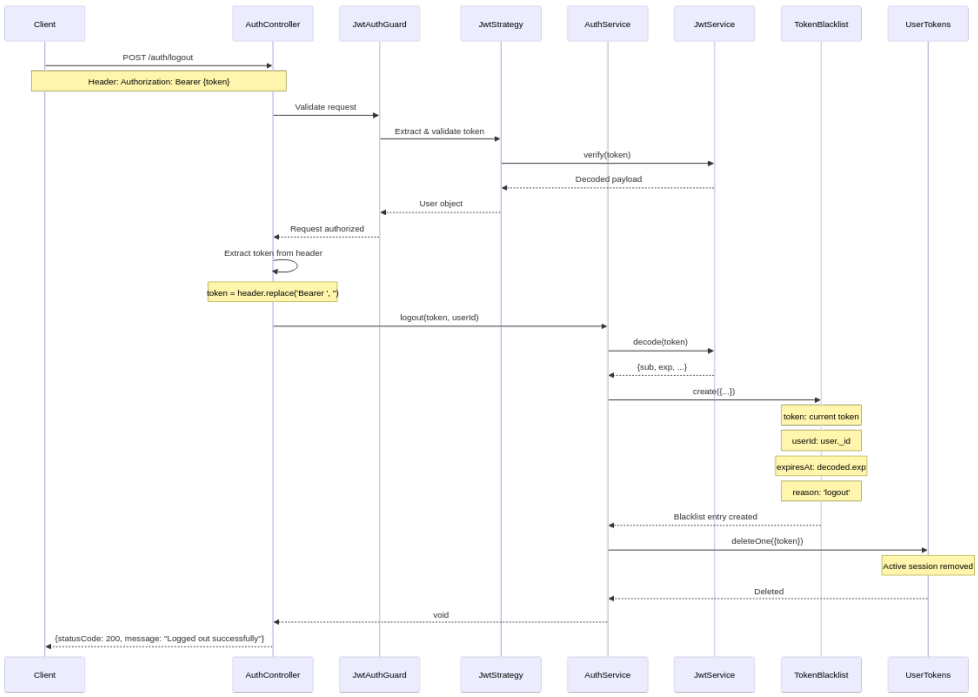


Figure 3.17: Token Revocation (Logout) Flow

```
async logout(token: string, userId: string) {
  const decoded = this.jwtService.decode(token);

  // Add to blacklist
  await this.tokenBlacklistModel.create({
    token,
    userId,
    expiresAt: new Date(decoded.exp * 1000),
    reason: 'logout',
  });

  // Remove from active tokens
  await this.userTokenModel.deleteOne({ token });
}
```

Listing 3.7: Logout Implementation

3.4 Session Security

This section details the security mechanisms including database schemas, single session enforcement, and token blacklisting.

3.4.1 Database Schema Design

Two MongoDB collections support the session security system.

UserTokens Collection

Tracks all active sessions with metadata for auditing:

```
@Schema({ timestamps: true })
export class UserToken extends Document {
  @Prop({ required: true, index: true })
  userId: string;

  @Prop({ required: true })
  token: string;

  @Prop({ required: true, type: Date })
  expiresAt: Date;

  @Prop({ type: String })
  userAgent?: string;

  @Prop({ type: String })
  ipAddress?: string;
}

// TTL index - auto delete when expired
UserTokenSchema.index(
  { expiresAt: 1 },
  { expireAfterSeconds: 0 }
);
```

Listing 3.8: UserToken Schema

TokenBlacklist Collection

Stores revoked tokens to prevent reuse:

```
@Schema({ timestamps: true })
export class TokenBlacklist extends Document {
  @Prop({ required: true, index: true })
  token: string;

  @Prop({ required: true, index: true })
  userId: string;

  @Prop({ required: true, type: Date })
  expiresAt: Date;

  @Prop({ enum: ['logout', 'new-login', 'refresh'] })
  reason: string;
}

// TTL index for automatic cleanup
```

```
TokenBlacklistSchema.index(
  { expiresAt: 1 },
  { expireAfterSeconds: 0 }
);
```

Listing 3.9: TokenBlacklist Schema

3.4.2 Single Session Enforcement

When a user logs in, all existing sessions are invalidated:

```
async revokeAllUserTokens(userId: string) {
  // Find all active tokens
  const activeTokens = await this.userTokenModel.find({
    userId,
    expiresAt: { $gt: new Date() },
  });

  if (activeTokens.length === 0) return;

  // Bulk insert to blacklist
  const entries = activeTokens.map(t => ({
    token: t.token,
    userId: t.userId,
    expiresAt: t.expiresAt,
    reason: 'new-login',
  }));

  await this.tokenBlacklistModel.insertMany(entries);
  await this.userTokenModel.deleteMany({ userId });
}
```

Listing 3.10: Single Session Enforcement

Figure 3.18 illustrates the session security flow.

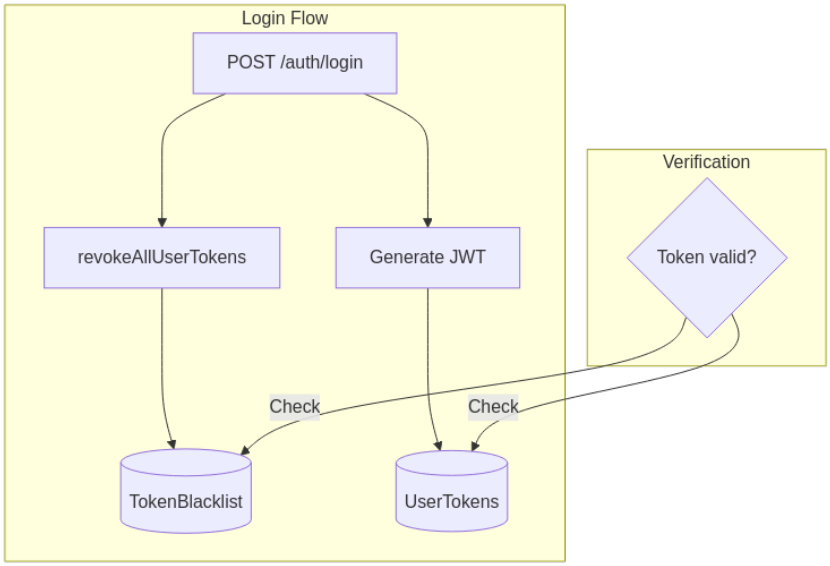


Figure 3.18: Session Security Flow

3.4.3 Token Blacklisting Flow

Figure 3.19 shows how tokens are blacklisted under different scenarios.

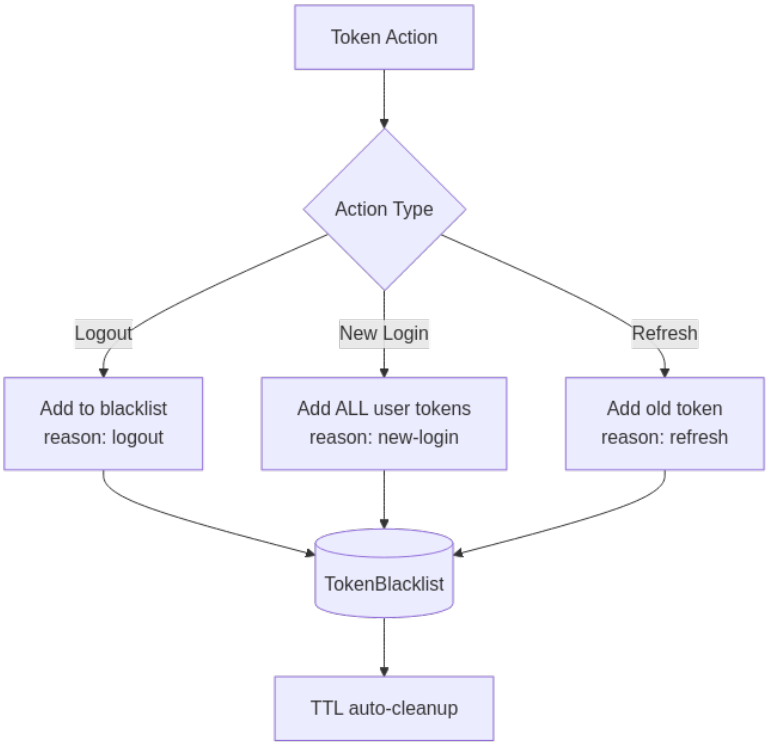


Figure 3.19: Token Blacklisting Flow

Reason	Trigger	Method
logout	User logout	`logout()`
new-login	New login revokes old	`revokeAllUserTokens()`
refresh	Token refresh	`refreshAccessToken()`

Table 3.4: Token Blacklist Reasons

3.4.4 Security Benefits

Feature	Benefit
Single Session	Stolen tokens invalidated on new login
IP/UserAgent Tracking	Audit trail for security review
Token Blacklisting	Immediate revocation capability
TTL Auto-cleanup	MongoDB automatically removes expired entries

Table 3.5: Security Features and Benefits

Bibliography

[1] L[eslie] A. Aamport. “The Gnats and Gnus Document Preparation System”. In: *G-Animal's Journal* (1986).

Appendix A

Proof

A long proof that you expect no one will read