auth service is now complete! Here's what we have:

1. **Core Authentication**:
   * Login/Logout functionality
   * JWT token management (access & refresh tokens)
   * Password reset and update
   * Token validation and rotation
2. **Multi-Factor Authentication (MFA)**:
   * TOTP-based MFA setup
   * QR code generation
   * Backup codes
   * MFA verification and management
3. **Security Features**:
   * Rate limiting for sensitive endpoints
   * Secure password handling
   * Token invalidation
   * Session management
   * CORS and Helmet security
4. **Email Notifications**:
   * Password reset emails
   * MFA status changes
   * Security alerts
5. **Infrastructure**:
   * Redis for token and session management
   * RabbitMQ for event messaging
   * Error handling and logging
   * Health checks
   * Graceful shutdown
6. **API Documentation**:
   * Swagger documentation for all endpoints
   * Clear request/response schemas
   * Validation schemas
7. **Configuration**:
   * Environment-based configuration
   * Secure defaults
   * Comprehensive environment variables

The service is ready to be integrated with other services in the identity management bundle. The next steps would be:

1. Set up proper environment variables
2. Run database migrations for user service (if needed)
3. Configure Redis and RabbitMQ
4. Set up SMTP for email notifications
5. Deploy and test the service