EnterpriseAuth Full Documentation

Overview

EnterpriseAuth is a production-grade passwordless authentication system built with ASP.NET Core (.NET 8). It uses Ed25519 public/private key cryptography and JWT tokens to provide SSH-style authentication. This ensures maximum security by eliminating passwords entirely.

Core Features

- Passwordless authentication
- SSH-style challenge-response authentication
- Ed25519 asymmetric cryptography
- JWT authentication and authorization
- Refresh tokens
- Logout and token revocation
- Key rotation support
- Audit logging
- Rate limiting protection
- PostgreSQL compatibility
- Enterprise-grade architecture

Architecture

Client: • Stores private key securely
• Signs authentication challenge

Server: • Stores public key
• Verifies signatures
• Issues JWT tokens

Database: • Users
• Keys
• RefreshTokens
• AuditLogs

Authentication Flow

1. User registers
2. Client generates key pair
3. Client registers public key
4. Client requests challenge
5. Client signs challenge
6. Server verifies signature
7. Server issues JWT token

API Endpoints

POST /register-user
POST /register-key
POST /auth/request
POST /auth/verify
POST /auth/refresh
POST /auth/logout
POST /auth/add-key
GET /secure

JWT Authentication

JWT tokens contain user identity and expiration time.
JWT is required for accessing protected endpoints.

Example header:
Authorization: Bearer JWT_TOKEN

Refresh Tokens

Refresh tokens allow clients to obtain new JWT tokens without re-authentication.
Refresh tokens can be revoked to prevent unauthorized access.

Key Rotation

Users can add or revoke keys without downtime.
This allows seamless security updates.

Audit Logging

Logs authentication events including:

- User ID
- IP address
- Timestamp
- Action performed

Rate Limiting

Protects authentication endpoints from brute-force attacks.
Default: 5 authentication attempts per minute.

Database Schema

Users table
UserKeys table
Challenges table
RefreshTokens table
AuditLogs table

Security Model

Private keys remain only on the client.
Server stores only public keys.
Server verifies cryptographic signatures.
Prevents credential theft and phishing.

Production Deployment

Recommended stack:

- ASP.NET Core
- PostgreSQL
- HTTPS
- Docker
- Reverse proxy (nginx)
- Firewall protection

Cryptography

Algorithm: Ed25519
Advantages:

- Secure
- Fast
- Modern
- Resistant to brute force

Scalability

Supports millions of users.
Stateless authentication allows horizontal scaling.

Conclusion

EnterpriseAuth provides enterprise-grade passwordless authentication using modern cryptography and JWT tokens.
Suitable for enterprise, cloud, and high-security applications.