Zabala Gailetak API Dokumentazioa

Bertsioa: 1.0
Oinarrizko URL: `https://api.zabala-gailetak.com/api`
Autentikazioa: JWT Bearer Token + MFA

Aurkibidea

---

1. Autentikazioa

1.1 Erabiltzaile Berria Erregistratu

Erabiltzaile kontu berria sortzen du.

Endpoint: `POST /auth/register`
Autentikazioa: Ez da beharrezkoa
Tasa Muga: 5 eskaera / 15 minutu

Eskaera Gorputza (Request Body):

```
{
  "username": "johndoe",
  "email": "john@example.com",
  "password": "SecurePass123!"
}
```

Eskaera Balidazioa:

Eremua	Mota	Beharrezkoa	Balidazioa
username	string	Bai	3-30 karaktere, alfanumerikoa
email	string	Bai	Email formatu balioduna
password	string	Bai	Gutxienez 8 karaktere

Arrakasta Erantzuna (201):

```
{
  "message": "Erabiltzailea ondo sortu da",
  "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...",
  "userId": 1
}
```

Errore Erantzuna (400):

```
{
  "errors": [
    {
      "msg": "Username must be between 3 and 30 characters",
      "param": "username",
      "location": "body"
    }
  ]
}
```

Errore Erantzuna (409):

```
{
  "error": "Erabiltzailea jada existitzen da"
}
```

1.2 Saioa Hasi (Login)

Erabiltzailea autentikatzen du eta JWT token bat itzultzen du.

Endpoint: `POST /auth/login`
Autentikazioa: Ez da beharrezkoa
Tasa Muga: 5 eskaera / 15 minutu

Eskaera Gorputza:

```
{
  "username": "johndoe",
```

```
  "password": "SecurePass123!"
}
```

Arrakasta Erantzuna MFArekin (200):

```
{
  "requiresMFA": true,
  "userId": 1,
  "message": "MFA kodea behar da"
}
```

Arrakasta Erantzuna MFA gabe (200):

```
{
  "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...",
  "userId": 1
}
```

Errore Erantzuna (401):

```
{
  "error": "Erabiltzailea edo pasahitza okerra"
}
```

1.3 MFA Konfiguratu

Autentikatutako erabiltzailearentzat MFA konfigurazioa hasten du.

Endpoint: `POST /auth/mfa/setup`
Autentikazioa: Beharrezkoa (Bearer Token)
Tasa Muga: 3 eskaera / orduko

Eskaera Goiburuak (Headers):

```
Authorization: Bearer
```

Arrakasta Erantzuna (200):

```
{
  "secret": "JBSWY3DPEHPK3PXP",
  "qrCode": "...",
  "message": "Eskaneatu QR kodea autentikatzaile aplikazioarekin"
}
```

Errore Erantzuna (400):

```
{
  "error": "MFA jada gaituta dago"
}
```

1.4 MFA Egiaztatu

MFA TOTP kodea egiaztatzen du eta autentikazioa osatzen du.

Endpoint: `POST /auth/mfa/verify`
Autentikazioa: Beharrezkoa (Bearer Token)
Tasa Muga: 10 eskaera / 15 minutu

Eskaera Goiburuak:

```
Authorization: Bearer
```

Eskaera Gorputza:

```
{
  "token": "123456"
}
```

Eskaera Balidazioa:

Eremua	Mota	Beharrezkoa	Balidazioa
token	string	Bai	6 digitu, zenbakizkoa

Arrakasta Erantzuna (200):

```
{
  "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...",
  "message": "MFA balidazioa arrakastatsua"
}
```

Errore Erantzuna (401):

```
{
  "error": "MFA kodea baliogabea"
}
```

1.5 MFA Desgaitu

Autentikatutako erabiltzailearentzat MFA desgaitzen du.

Endpoint: `POST /auth/mfa/disable`
Autentikazioa: Beharrezkoa (Bearer Token)
Tasa Muga: 1 eskaera / orduko

Eskaera Goiburuak:

```
Authorization: Bearer
```

Arrakasta Erantzuna (200):

```
{
  "message": "MFA desgaitu da"
}
```

---

2. Produktuak

2.1 Produktu Guztiak Lortu

Eskuragarri dauden produktu guztien zerrenda lortzen du.

Endpoint: `GET /products`
Autentikazioa: Aukerakoa
Tasa Muga: 50 eskaera / 15 minutu

Arrakasta Erantzuna (200):

```
[
  {
    "id": 1,
    "name": "Gaileta Tradizionalak",
    "price": 2.50,
    "description": "Betiko zaporea, osagai naturalekin egina.",
    "category": "Cookies",
    "stock": 100
  },
  {
    "id": 2,
    "name": "Txokolatezko Gailetak",
    "price": 3.00,
    "description": "Txokolate beltz onenarekin estaliak.",
    "category": "Chocolate",
    "stock": 75
  },
  {
    "id": 3,
    "name": "Zereal Gailetak",
    "price": 2.80,
```

```
    "description": "Zereal zaporearekin, osasuntsuak.",
    "category": "Cookies",
    "stock": 50
  }
]
```

Orrialdekatzea (Etorkizunean):

```
GET /products?page=1&limit=10&sort=name&order=asc
```

2.2 Produktua ID bidez Lortu (Etorkizunean)

Produktu zehatz baten xehetasunak lortzen ditu.

Endpoint: `GET /products/:id`
Autentikazioa: Aukerakoa

Arrakasta Erantzuna (200):

```
{
  "id": 1,
  "name": "Gaileta Tradizionalak",
  "price": 2.50,
  "description": "Betiko zaporea, osagai naturalekin egina.",
  "category": "Cookies",
  "stock": 100,
  "images": [
    "https://cdn.zabala-gailetak.com/products/1/image1.jpg",
    "https://cdn.zabala-gailetak.com/products/1/image2.jpg"
  ],
  "createdAt": "2024-01-08T10:00:00Z",
  "updatedAt": "2024-01-08T10:00:00Z"
}
```

Errore Erantzuna (404):

```
{
  "error": "Produktua ez da aurkitu"
}
```

---

3. Eskaerak

3.1 Eskaera Sortu

Autentikatutako erabiltzailearentzat eskaera berria sortzen du.

Endpoint: `POST /orders`
Autentikazioa: Beharrezkoa (Bearer Token)
Tasa Muga: 25 eskaera / 15 minutu

Eskaera Goiburuak:

```
Authorization: Bearer
Content-Type: application/json
```

Eskaera Gorputza:

```
{
  "productId": 1,
  "quantity": 2,
  "customerEmail": "john@example.com",
  "customerName": "John Doe",
  "shippingAddress": "123 Main St, City, Country"
}
```

Eskaera Balidazioa:

Eremua	Mota	Beharrezkoa	Balidazioa
productId	integer	Bai	Existitu behar da
quantity	integer	Bai	1-100
customerEmail	string	Bai	Email balioduna
customerName	string	Bai	2-100 karaktere
shippingAddress	string	Bai	10-500 karaktere

Arrakasta Erantzuna (201):

```
{
  "message": "Eskaera ondo jaso da",
  "orderId": 1234,
  "orderDate": "2024-01-08T10:30:00Z",
  "estimatedDelivery": "2024-01-10T00:00:00Z",
  "total": 5.00
}
```

Errore Erantzuna (400):

```
{
  "errors": [
    {
```

```
      "msg": "Quantity must be between 1 and 100",
      "param": "quantity",
      "location": "body"
    }
  ]
}
```

Errore Erantzuna (422):

```
{
  "error": "Ez dago nahiko stock"
}
```

3.2 Erabiltzailearen Eskaerak Lortu (Etorkizunean)

Autentikatutako erabiltzailearen eskaerak lortzen ditu.

Endpoint: `GET /orders`
Autentikazioa: Beharrezkoa (Bearer Token)

Eskaera Goiburuak:

```
Authorization: Bearer
```

Arrakasta Erantzuna (200):

```
{
  "orders": [
    {
      "id": 1234,
      "productId": 1,
      "productName": "Gaileta Tradizionalak",
      "quantity": 2,
      "total": 5.00,
      "status": "pending",
      "createdAt": "2024-01-08T10:30:00Z"
    }
  ],
  "total": 1,
  "page": 1,
  "limit": 10
}
```

3.3 Eskaera ID bidez Lortu (Etorkizunean)

Eskaera zehatz baten xehetasunak lortzen ditu.

Endpoint: `GET /orders/:id`
Autentikazioa: Beharrezkoa (Bearer Token)

Arrakasta Erantzuna (200):

```
{
  "id": 1234,
  "productId": 1,
  "productName": "Gaileta Tradizionalak",
  "quantity": 2,
  "total": 5.00,
  "status": "shipped",
  "customerName": "John Doe",
  "customerEmail": "john@example.com",
  "shippingAddress": "123 Main St, City, Country",
  "trackingNumber": "ZG123456789",
  "createdAt": "2024-01-08T10:30:00Z",
  "updatedAt": "2024-01-08T14:00:00Z"
}
```

---

4. Sistema

4.1 Osasun Egiaztapena (Health Check)

APIaren osasun egoera itzultzen du.

Endpoint: `GET /health`
Autentikazioa: Ez da beharrezkoa

Arrakasta Erantzuna (200):

```
{
  "status": "healthy",
  "timestamp": "2024-01-08T10:00:00Z",
  "version": "1.0.0",
  "services": {
    "database": "up",
    "cache": "up",
    "queue": "up"
  }
}
```

Errore Erantzuna (503):

```
{
  "status": "unhealthy",
```

```
  "error": "Service unavailable"
}
```

4.2 API Informazioa

APIaren informazioa itzultzen du.

Endpoint: `GET /`
Autentikazioa: Ez da beharrezkoa

Arrakasta Erantzuna (200):

```
{
  "message": "Zabala Gailetak API - Bertsioa 1.0",
  "status": "active",
  "security": "enabled",
  "version": "1.0.0",
  "documentation": "https://docs.zabala-gailetak.com"
}
```

---

5. Errore Kodeak

5.1 HTTP Egoera Kodeak

Kodea	Deskribapena
200	OK - Eskaera arrakastatsua
201	Created - Baliabidea sortua
400	Bad Request - Sarrera baliogabea
401	Unauthorized - Autentikazioa beharrezkoa edo okerra
403	Forbidden - Baimen nahikorik ez
404	Not Found - Baliabidea ez da aurkitu
409	Conflict - Baliabidea jada existitzen da
422	Unprocessable Entity - Negozio logika errorea
429	Too Many Requests - Tasa muga gainditua
500	Internal Server Error - Zerbitzariaren errorea

Kodea	Deskribapena
503	Service Unavailable - Zerbitzua erorita

5.2 Errore Erantzun Formatua

Balidazio Errorea (400):

```
{
  "errors": [
    {
      "msg": "Error message",
      "param": "parameter_name",
      "location": "body|query|params"
    }
  ]
}
```

Negozio Errorea (422):

```
{
  "error": "Error message",
  "code": "STOCK_UNAVAILABLE",
  "details": {
    "available": 5,
    "requested": 10
  }
}
```

Zerbitzari Errorea (500):

```
{
  "error": "Zerbitzariaren errorea",
  "requestId": "req_abc123"
}
```

---

6. Tasa Mugatzea (Rate Limiting)

6.1 Tasa Muga Arauak

Endpoint	Muga	Leihoa
POST /auth/register	5	15 minutu
POST /auth/login	5	15 minutu

Endpoint	Muga	Leihoa
POST /auth/mfa/verify	10	15 minutu
GET /products	50	15 minutu
POST /orders	25	15 minutu
Besteak	100	15 minutu

6.2 Tasa Muga Goiburuak

Erantzun Goiburuak:

```
X-RateLimit-Limit: 100
X-RateLimit-Remaining: 95
X-RateLimit-Reset: 1704729600
```

6.3 Tasa Muga Errorea (429)

```
{
  "error": "Eskari gehiegi jaso dira IP honetatik, mesedez saiatu berriro geroago.",
  "retryAfter": 900
}
```

---

7. Segurtasuna

7.1 Autentikazioa

JWT Token Formatua:

```
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...
```

Token Claims:

```
{
  "userId": "12345",
  "username": "johndoe",
  "mfaVerified": true,
  "iat": 1704729600,
  "exp": 1704733200
}
```

Token Iraungitzea: 1 ordu

7.2 Segurtasun Goiburuak (Headers)

Erantzun Goiburuak:

```
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Security-Policy: default-src 'self'
Referrer-Policy: strict-origin-when-cross-origin
```

7.3 CORS

Baimendutako Jatorriak (Origins):

- `https://zabala-gailetak.com`
- `https://www.zabala-gailetak.com`

Baimendutako Metodoak:

- GET, POST, PUT, DELETE, OPTIONS

Baimendutako Goiburuak:

- Content-Type, Authorization, X-Requested-With

7.4 Sarrera Balidazioa

Sarrera guztiak balidatu eta sanitizatzen dira:

- SQL injection prebentzioa
- XSS prebentzioa
- CSRF babesa
- Command injection prebentzioa

7.5 Enkriptatzea

- **Pasahitza**: bcrypt (cost factor: 10)
- **MFA Sekretua**: Enkriptatuta geldirik (at rest)
- **TLS**: TLS 1.2 / TLS 1.3
- **Zifratzeak**: HIGH security cipher suites

Eranskina A: Test Adibideak

cURL Adibideak

Erregistratu:

```
curl -X POST https://api.zabala-gailetak.com/api/auth/register \
  -H "Content-Type: application/json" \
  -d '{"username":"johndoe","email":"john@example.com","password":"SecurePass123!"}'
```

Saioa Hasi:

```
curl -X POST https://api.zabala-gailetak.com/api/auth/login \
  -H "Content-Type: application/json" \
  -d '{"username":"johndoe","password":"SecurePass123!"}'
```

Produktuak Lortu:

```
curl https://api.zabala-gailetak.com/api/products
```

Eskaera Sortu:

```
curl -X POST https://api.zabala-gailetak.com/api/orders \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer " \
  -d '{"productId":1,"quantity":2,"customerEmail":"john@example.com",
       "customerName":"John Doe","shippingAddress":"123 Main St"}'
```

Eranskina B: SDK Adibideak

JavaScript (Axios)

```
import axios from 'axios';

const apiClient = axios.create({
  baseURL: 'https://zabala-gailetak.infinityfreeapp.com/api',
  timeout: 10000
});

// Saioa Hasi
const login = async (username, password) => {
  const response = await apiClient.post('/auth/login', {
    username,
    password
  });

  if (response.data.token) {
    apiClient.defaults.headers.common[
```

```
      'Authorization'
    ] = `Bearer ${response.data.token}`;
  }

  return response.data;
};

// Produktuak Lortu
const getProducts = async () => {
  const response = await apiClient.get('/products');
  return response.data;
};

// Eskaera Sortu
const createOrder = async (orderData) => {
  const response = await apiClient.post('/orders', orderData);
  return response.data;
};
```

Eranskina C: Aldaketa Erregistroa

1.0 Bertsioa (2024-01-08)

- Hasierako API argitalpena
- Autentikazio endpoint-ak
- Produktu endpoint-ak
- Eskaera endpoint-ak
- MFA euskarria
- Tasa mugatzea (Rate limiting)
- Segurtasun goiburuak

Dokumentu Bertsioa: 1.0
Azken Eguneratzea: 2024-01-08
Mantentzailea: Zabala Gailetak Garapen Taldea