Authentication and Security API Guide for Health IoT Devices

1. Introduction

This guide provides details on authentication and security endpoints for integrating Health IoT Devices with secure APIs.

2. Authentication Flow

- All endpoints require HTTPS.
- Bearer token authentication (OAuth 2.0) is used for all resources.

3. API Endpoints

3.1 Obtain Access Token

Send a POST request to obtain an OAuth 2.0 access token.

```
POST /oauth/token HTTP/1.1
Content-Type: application/x-www-form-urlencoded
grant_type=client_credentials&client_id=YOUR_CLIENT_ID&client_secret=YOUR_CLIENT_SECRET
```

Response

```
{
  "access_token": "string",
  "token_type": "Bearer",
  "expires_in": 3600
}
```

3.2 Device Registration

Register a new IoT device to establish a secure identity.

```
POST /api/v1/devices/register HTTP/1.1
Authorization: Bearer ACCESS_TOKEN
Content-Type: application/json
{
  "device_id": "string",
  "device_name": "string",
  "public_key": "string"
}
```

Response

```
{
  "status": "registered",
  "device_id": "string"
}
```

4. Security Best Practices

- Always use HTTPS for all API calls.
- Keep client credentials and device keys secure.
- Rotate access tokens and keys regularly.
- Validate and sanitize all inputs.

5. Error Responses

```
{
  "error": "invalid_token",
  "error_description": "The access token is invalid or expired"
}
```

```
{
  "error": "invalid_request",
  "error_description": "Missing required field: device_id"
}
```

6. Contact & Support

For further assistance, contact `support@healthiot.example.com`.