2□. Restfull API □□

- Gate Token □□
- □□□ API □□□ □□ □□

Gate Token 개념

> “
>
> ## 인증 & OAuth 2.0

인증이란 특정 사용자가 본인임을 확인하는 절차를 의미합니다. 일반적으로 아이디와 비밀번호가 일치하면 해당 사용자가 본인이라고 판단할 수 있습니다. 예를 들어, 다보리에 로그인할 때 다보리 계정의 아

하지만, 다보리 오픈API를 활용하여 개발한 애플리케이션에서 사용자가 다보리 계정의 아이디와 비밀번호를 직접 입력하도록 하면 보안상의 위험이 발생할 수 있습니다. 이를 방지하기 위해, 사용자가 제

이러한 **OAuth** [illegible] **OAuth 2.0** 프로토콜 을 적용하여 안전한 인증 서비스를 제공하고 있습니다.

> “
>
> ## Gate Token

dabory sso(OAuth2 기반)을 통해 사용자가 인증되면 이후 GateToken을 사용하여 API 서버와 DB에 연동할 수 있습니다. GateToken 자체는 사용자 인증을

다보리 Frontend에서는 로그인 체크 이전에 session에 저장된 gatetoken을 check합니다. 만약 gatetoken이 존재하지 않는다면 main_api server
접근정보와 api server와의 정상적인 연동 권한을 갖췄는지 체크하기 위해 사용되는 암호화된 토큰입니다.

api 서버로부터 반환받은 GateToken은 프론트엔드 session에 저장됩니다. 이 session은 권한이 필요한 모든 프론트엔드 요청의 header에 포함됩니다.

다보리 API 설계의 기본 지식

HTTP Method 및 보안성

- 다보리 ERP의 모든 API는 단순성과 보안성을 고려하여 POST method만 사용합니다.
- 이는 데이터 변경 및 전송의 안정성을 보장할 수 있습니다.

DaborySSO 및 환경 변수

- DaborySSO를 사용하여 API 서버에 인증 및 권한 관리를 권장하지만 필요에 따라 Key Pair를 API 서버의 환경 변수에 저장하여 SSO 서버와 독립적으로 사용할 수

GateToken:

- 모든 API 요청은 API 서버로부터 반환받은 GateToken을 포함해야 합니다. 이를 통해 인증 및 권한 부여가 이루어집니다.
- GateToken은 타켓 DB의 접근 정보를 PKI 암호화한 BeforeBase64 Key로만 발급받을 수 있습니다. 이는 데이터 보안을 강화합니다.
- 모든 Frontend Server는 ClientID 값을 가집니다. 이는 DaborySSO에서 App 레코드를 생성하는 과정에서 생성됩니다.
- Client(Frontend)의 GateToken은 API 서버의 메모리 DB에 저장됩니다. 또한 유효기간 설정이 가능합니다. 이를 통해 인증된 클라이언트만이 API를 사용할 수

이러한 설계 원칙을 준수하여 안전하고 효율적인 API 시스템을 구축할 수 있습니다.