

# Darim

## 클라이언트 측 암호화를 지원하는 일기 애플리케이션

아주 훌륭한SW융합인의 도전

# 목차

---

1. 배경
2. 문제정의
3. 요구사항
4. 제안

# 배경

- 현대 사회에서 파편화된 개인이 자아를 반추하기 위한 일기.
- 시중에 많은 일기 애플리케이션이 있고, 비즈니스적인 성과도 내고 있다.
- 하지만 기존의 일기 애플리케이션에는 공통적인 문제가 있다.

# 문제정의

---

일기 콘텐츠를  
암호화하지 않음

일기 콘텐츠를  
범용적인 형식으로  
제공하지 않음

# 문제정의

일기 콘텐츠를  
암호화하지 않음

- 일기 콘텐츠는 매우 민감하고 사적인 데이터.
- 데이터에 접근하기 위한 인증 절차만 거칠 뿐, 데이터 자체를 암호화하지는 않는다.
- 일기 콘텐츠를 시스템 관리자가 확인할 수 있다는 사실 자체로 부정적인 UX 유발.

# 문제정의

- 일기 콘텐츠는 단순한 기록을 넘어서는 의미를 갖기 때문에 영속성이 매우 중요.
- 데이터를 플레인 텍스트 또는 렌더링된 HTML로만 제공할 뿐, 타 서비스와 호환되는 형식으로 제공하지 않는다.

**일기 콘텐츠를  
범용적인 형식으로  
제공하지 않음**

# 요구사항

클라이언트 측 암호화를  
통한 일기 콘텐츠 보호

마크다운을 통한  
범용 형식 텍스트 제공

# 요구사항

**클라이언트 측 암호화를  
통한 일기 콘텐츠 보호**

- 공격자는 물론, 시스템 관리자도 사용자의 일기 콘텐츠를 읽을 수 없어야 한다.
- 클라이언트 측 암호화를 통해 사용자의 비밀번호로 일기 콘텐츠를 암호화할 필요가 있다.



# 요구사항

- 서비스와 상관없이 사용자가 범용적인 형식의 일기 데이터를 제공받을 수 있어야 한다.
- 마크다운을 통해 시맨틱이 보장된 범용적인 텍스트 데이터를 사용자에게 제공해야 한다.



**마크다운을 통한  
범용 형식 텍스트 제공**

# 제안

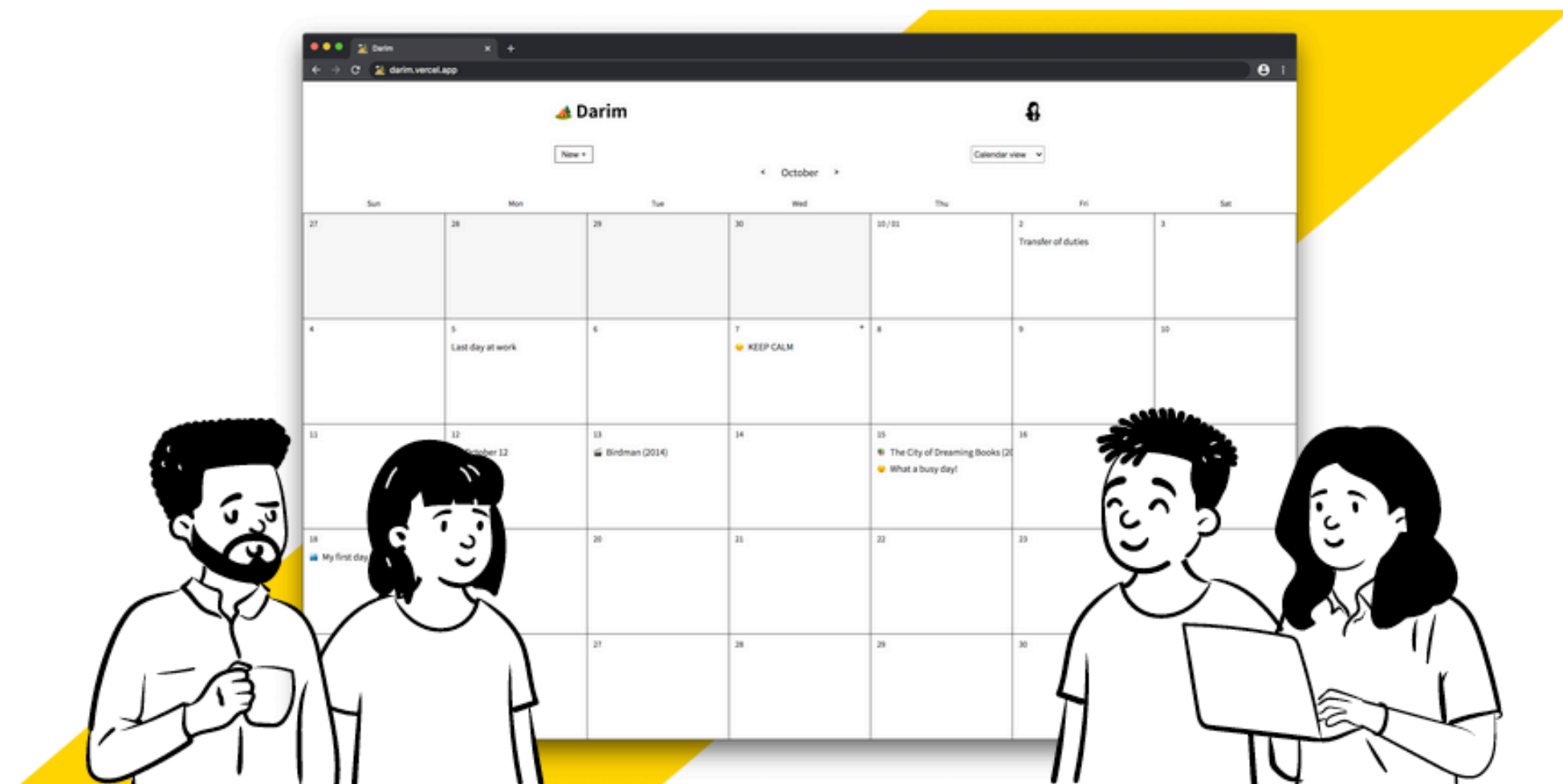
darim.vercel.app



## 📖 안전한 온라인 다이어리

다림은 비밀키 암호화를 사용하는 안전한 온라인 다이어리 서비스입니다.

이메일	비밀번호	이름	회원가입 ↗
-----	------	----	--------



이메일	비밀번호	로그인 ↗
-----	------	-------

비밀번호를 잊으셨나요?



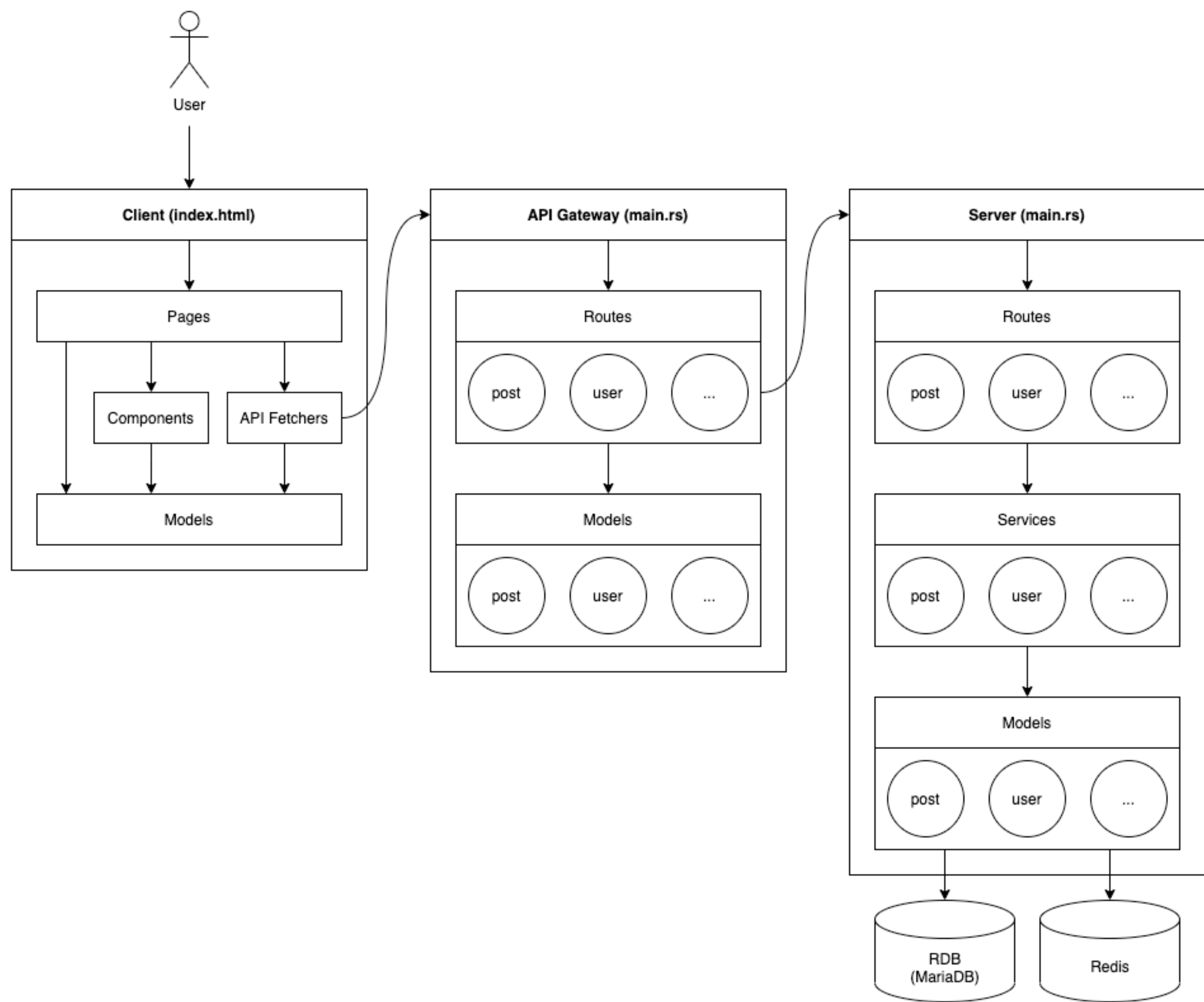
New +

< December >

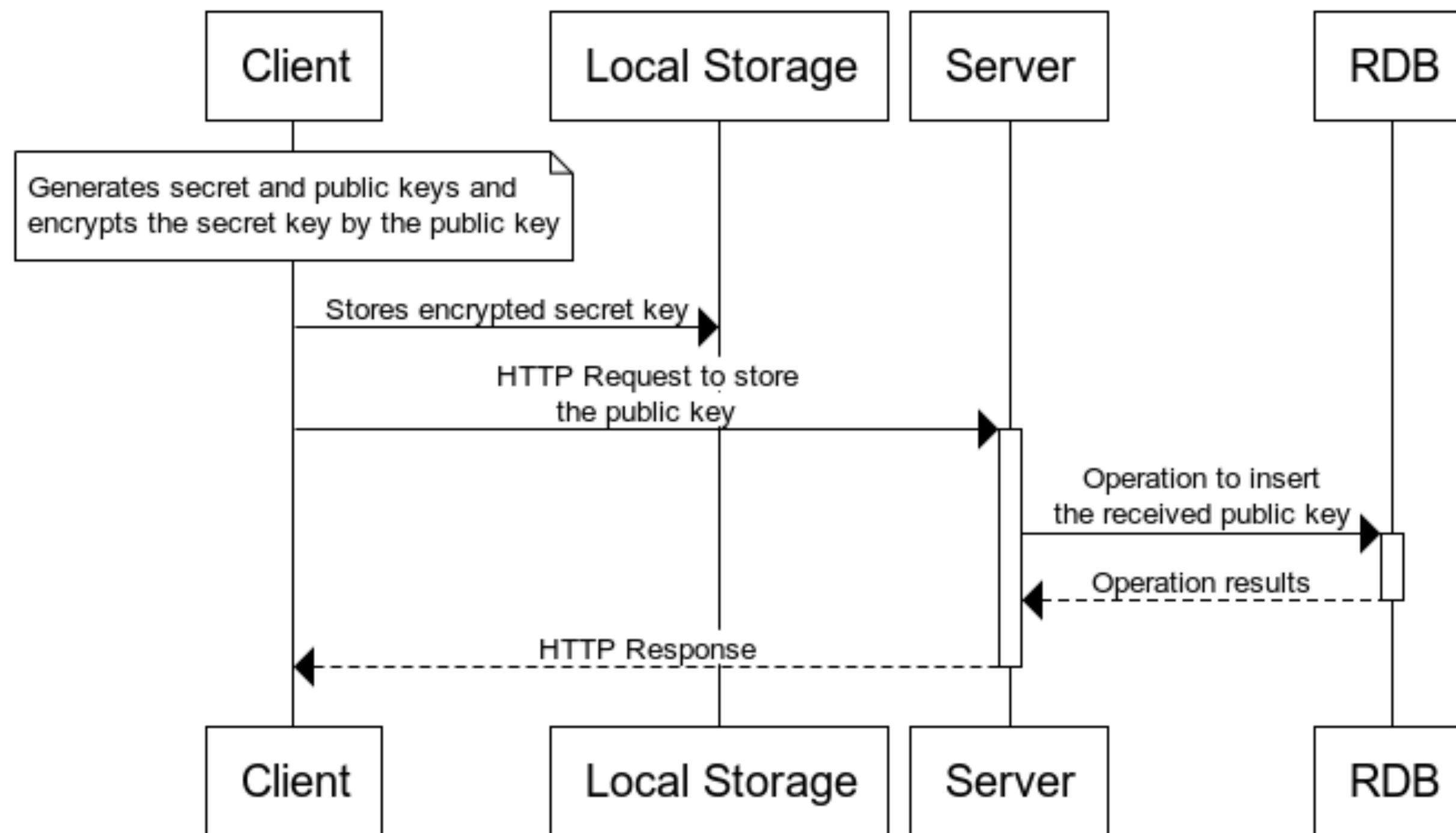
캘린더 뷰 ▾

일	월	화	수	목	금	토
27	28	29	30	12 / 01	2	3 📖 아르테미스를 읽고
4	5 😓 KEEP CALM	6	7	8 😓 너무 바쁜 하루	9	10
11	12 😓 첫 출근	13	14	15	16 ☕ 따뜻한 커피	17
18	19	20	21 😓 방학!	22 📌	23	24
25	26	27	28	29	30	31

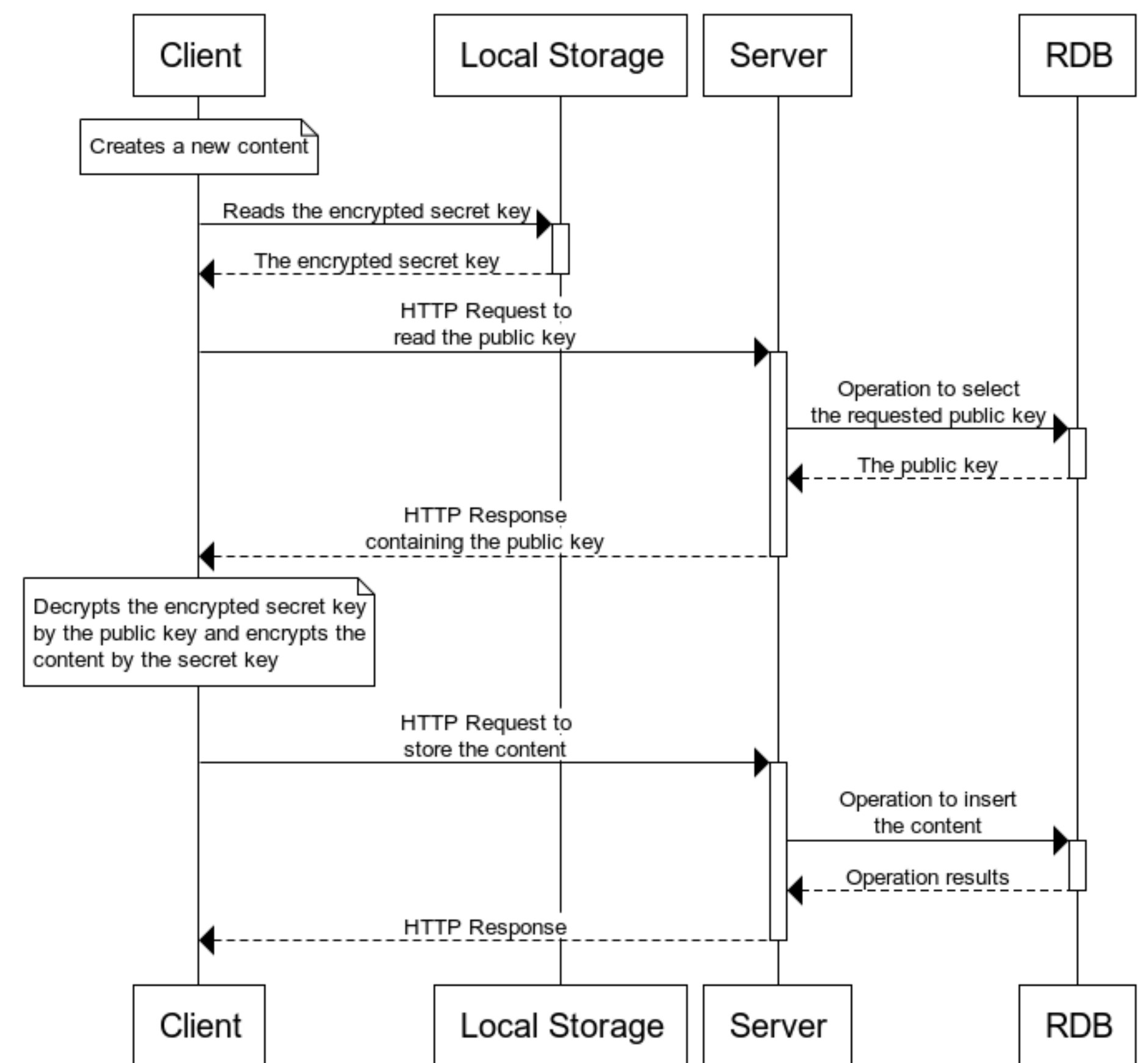
# 제안



# 제안



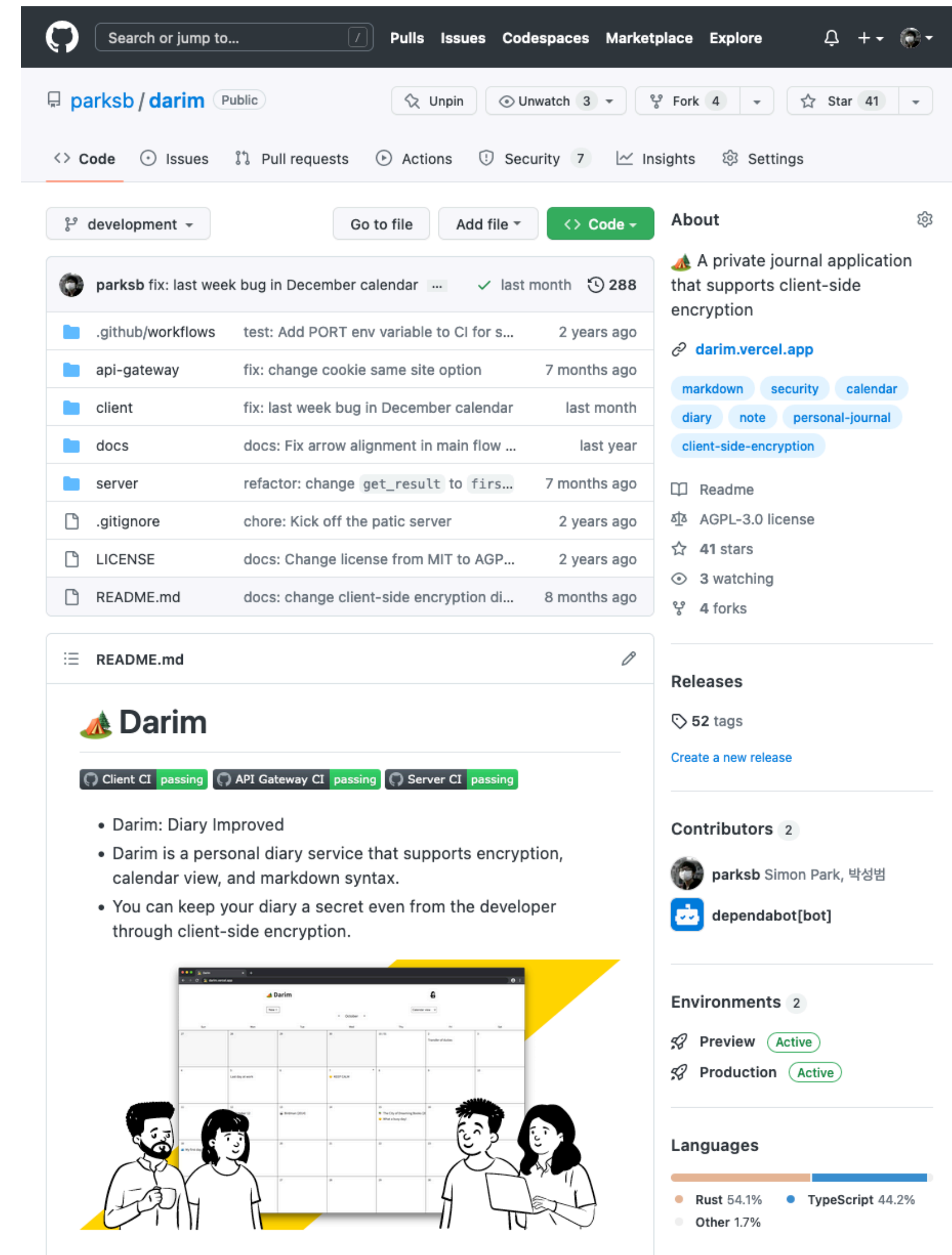
Key generation sequence



Write sequence

# 제안

- 오픈소스 공개 (AGPL-3.0):  
[github.com/parksb/darim](https://github.com/parksb/darim)
- (FE) TypeScript + React.js
- (BE) Rust: 높은 신뢰와 성능을  
확보할 수 있는 범용 프로그래밍 언어.



**감사합니다.**