HUST

ĐẠI HỌC BÁCH KHOA HÀ NỘI

HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

ONE LOVE. ONE FUTURE.

ĐẠI HỌC
BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY
OF SCIENCE AND TECHNOLOGY

BÁO CÁO TIẾN ĐỘ MÔN HỌC MẬT MÃ ỨNG DỤNG

Nhóm 3:
Nguyễn Huy Được - 20225297
Đỗ Thế Quân - 20225382
Đỗ Hoàng Đức - 20225286

ONE LOVE. ONE FUTURE.

HUST

hust.edu.vn fb.com/dhbkhn

Project 3 – Team Secret Manager

1. Công việc đã làm

- Nguyễn Huy Được – Xử lý các thuật toán mã hóa
- Đỗ Thế Quân – Frontend
- Đỗ Hoàng Đức - Backend
- AI – Giúp đỡ dựng giao diện cho Frontend và các thuật toán mã hóa

2. Đặt vấn đề

- **Thực trạng:** Các nhóm phát triển phần mềm thường chia sẻ các thông tin nhạy cảm (API Keys, Database Passwords, SSH Keys, file .env) qua các kênh không an toàn như Zalo, Messenger, Slack hoặc lưu thẳng vào Git repository.
- **Giải pháp:** Xây dựng một ứng dụng web nơi mọi bí mật được **mã hóa ngay tại trình duyệt (Client-side encryption)** trước khi gửi lên server. Server chỉ đóng vai trò lưu trữ "rác" (dữ liệu đã mã hóa) và quản lý quyền truy cập

3. Ý tưởng

- **Mã hóa phía Client :** Mọi quá trình mã hóa/giải mã diễn ra trên trình duyệt người dùng. Dữ liệu rời khỏi máy tính luôn ở dạng bản mã.
- **Cơ chế Mã hóa Lai (Hybrid Encryption):**
  - **AES-256 (Symmetric):** Dùng để mã hóa nội dung bí mật (tốc độ nhanh).
  - **ECC/RSA (Asymmetric):** Dùng để mã hóa khóa AES khi cần chia sẻ cho thành viên khác (Key Wrapping).
- **Bảo vệ Danh tính:** Private Key của người dùng được mã hóa bằng Master Password và không được lưu dưới dạng Plaintext trên Server.

4. Công nghệ sử dụng

Frontend:

Backend:

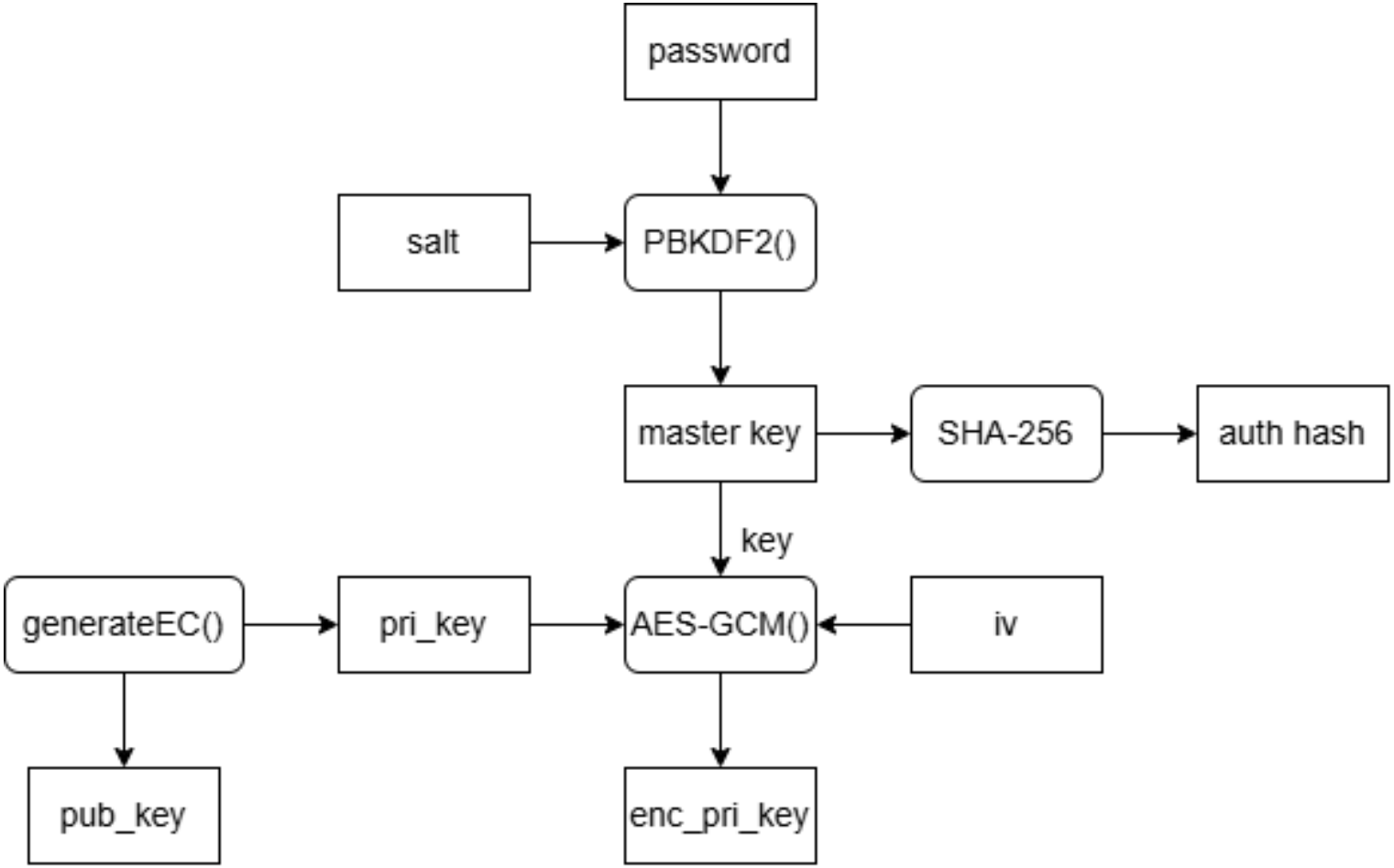
Database:

5. Luồng hoạt động của người dùng

- Người dùng đăng kí
- Người dùng đăng nhập
- Tạo tên gợi nhớ và nội dung bí mật bản thân muốn trong kho bí mật của bản thân
- Chọn người muốn chia sẻ nội dung khóa -> Chia sẻ
- Người kia sẽ nhận được nội dung đó trong Kho bí mật của mình

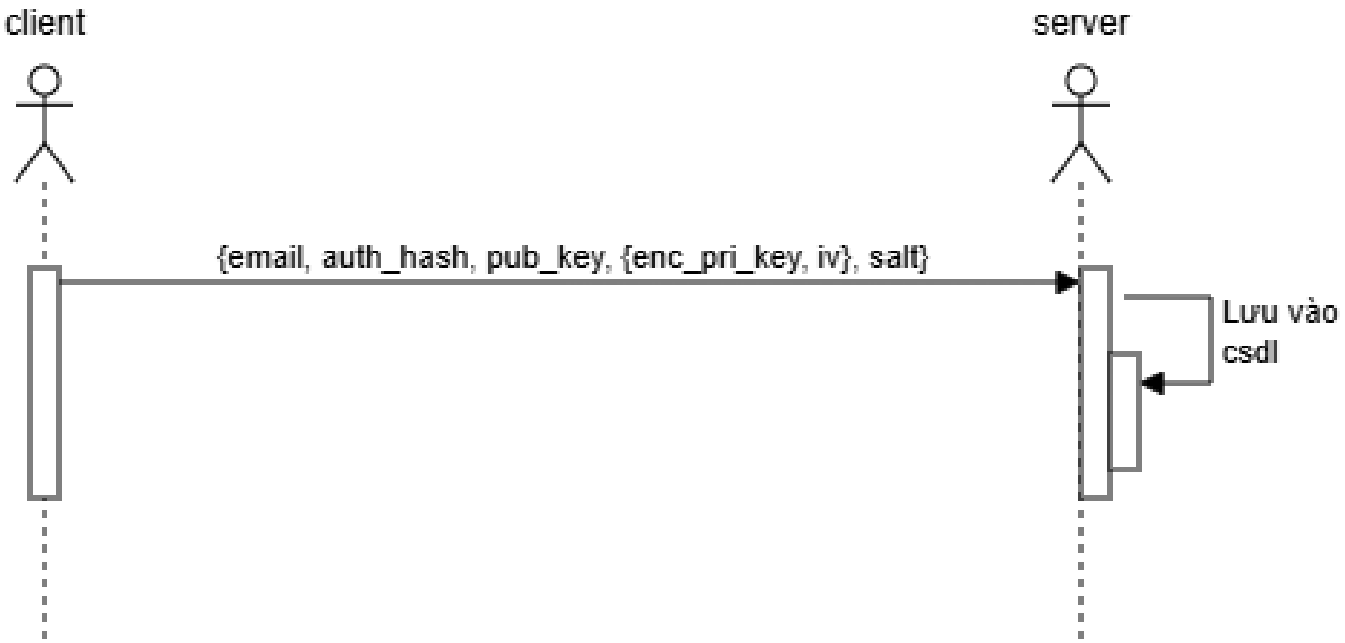
6. Luồng hoạt động chi tiết

Đăng ký



6. Luồng hoạt động chi tiết

Đăng ký



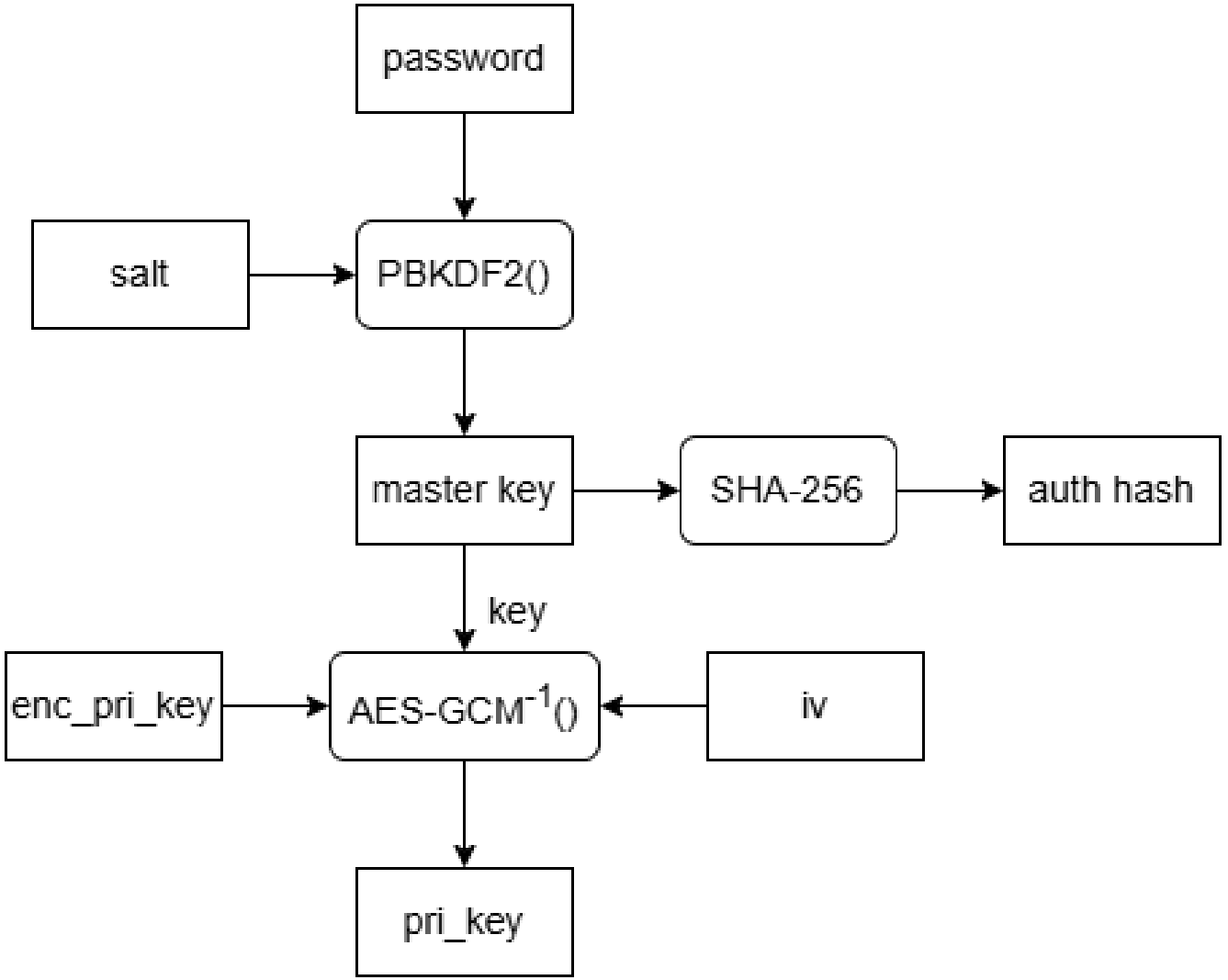
6. Luồng hoạt động chi tiết

Đăng ký


```
{
  "_id": "507f1f77bcf86cd799439011",
  "email": "alice@example.com",

  "auth_hash":
"9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08",

  "public_key": {
    "kty": "EC",
    "crv": "P-384",
    "x": "KpW8ZgMVBS37Qnr5bS...",
    "y": "afZTYKhsIanT8TXPx0...",
    "ext": true
  },

  "encrypted_private_key": {
    "iv": "a1b2c3d4e5f6...",
    "ciphertext": "4f8a2b3c1d9e..."
  },

  "salt": "f7d3c8b2a9e1...",

  "secrets_version": 15,
  "collection_checksum": "3a5c7d9f2e8b...",
  "last_checksum_update": "2026-01-19T08:54:36.000Z"
}
```

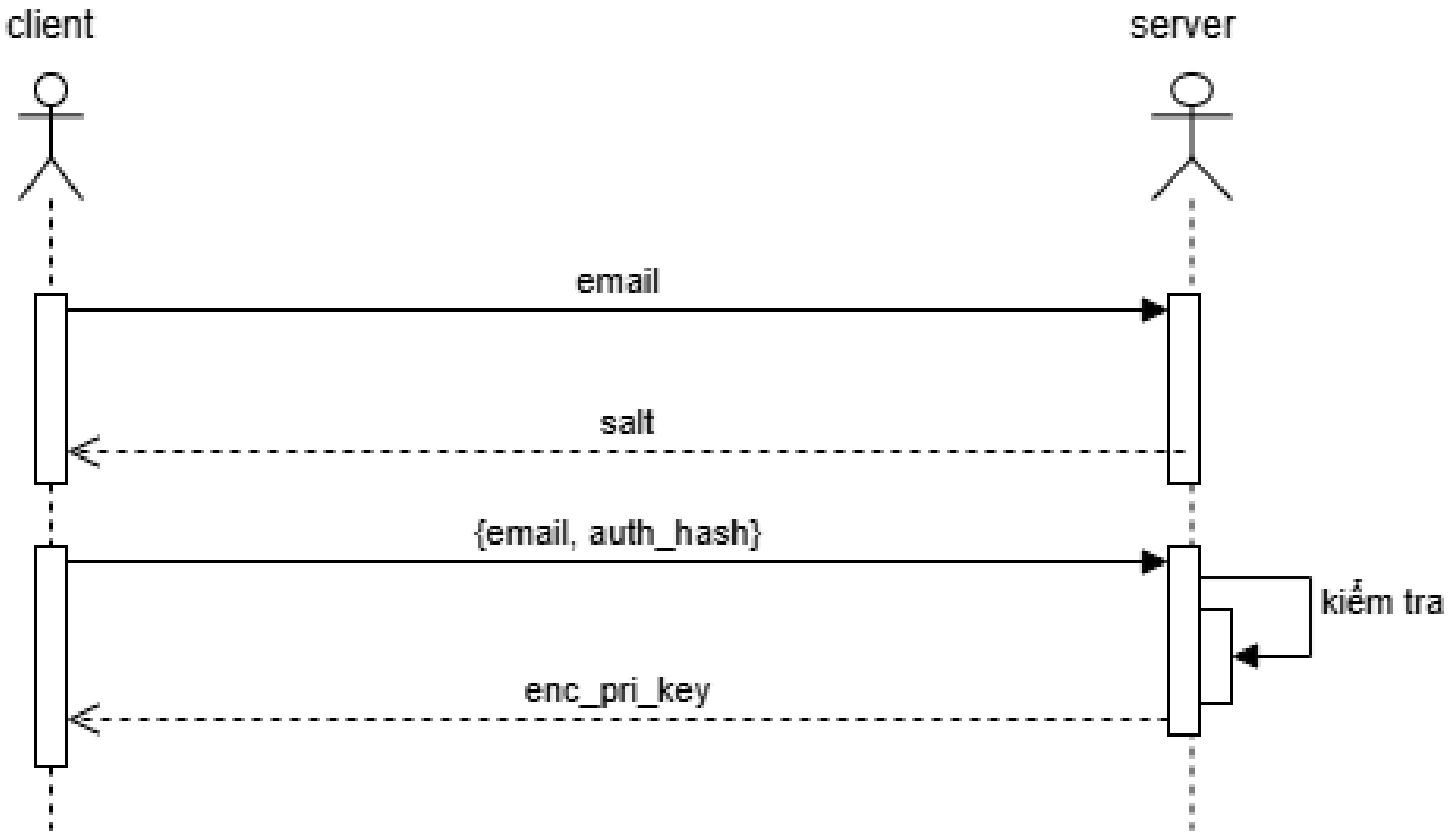
6. Luồng hoạt động chi tiết

Đăng nhập



6. Luồng hoạt động chi tiết

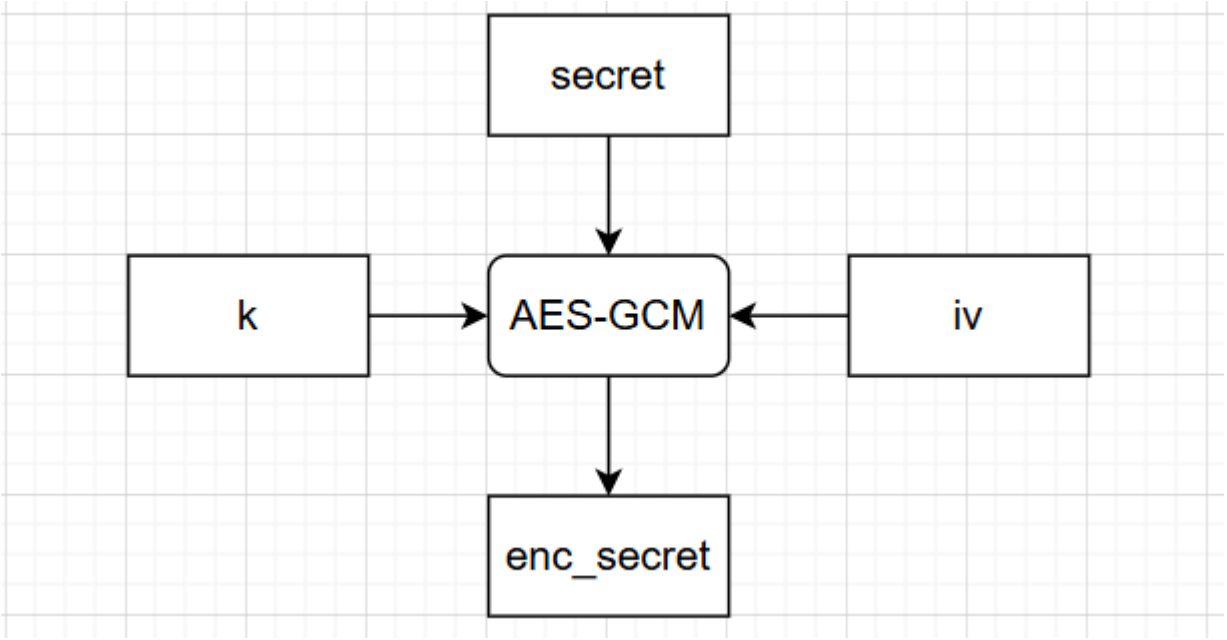
Đăng nhập



6. Luồng hoạt động chi tiết

Tạo secret

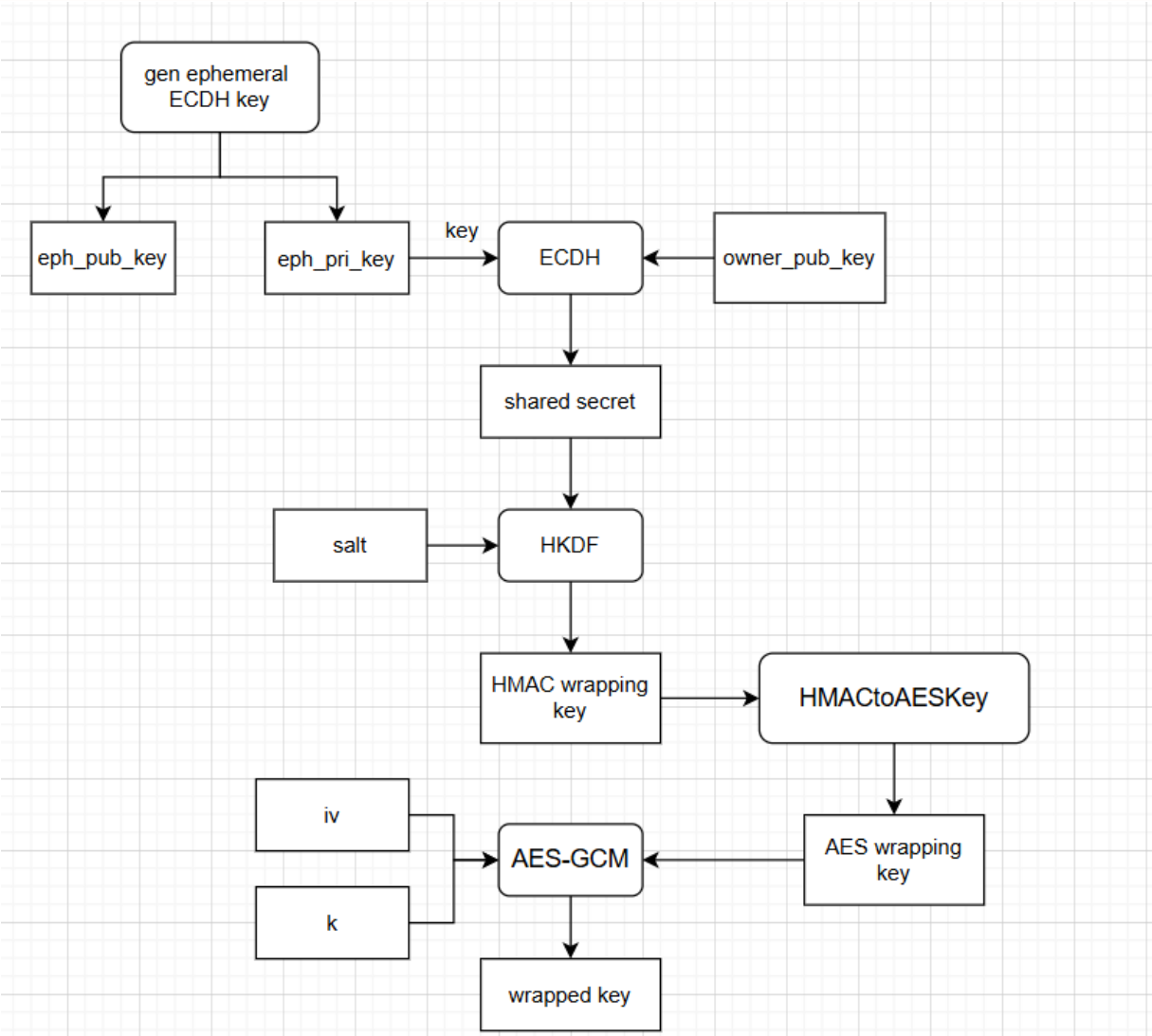
- Mã hóa secret



6. Luồng hoạt động chi tiết

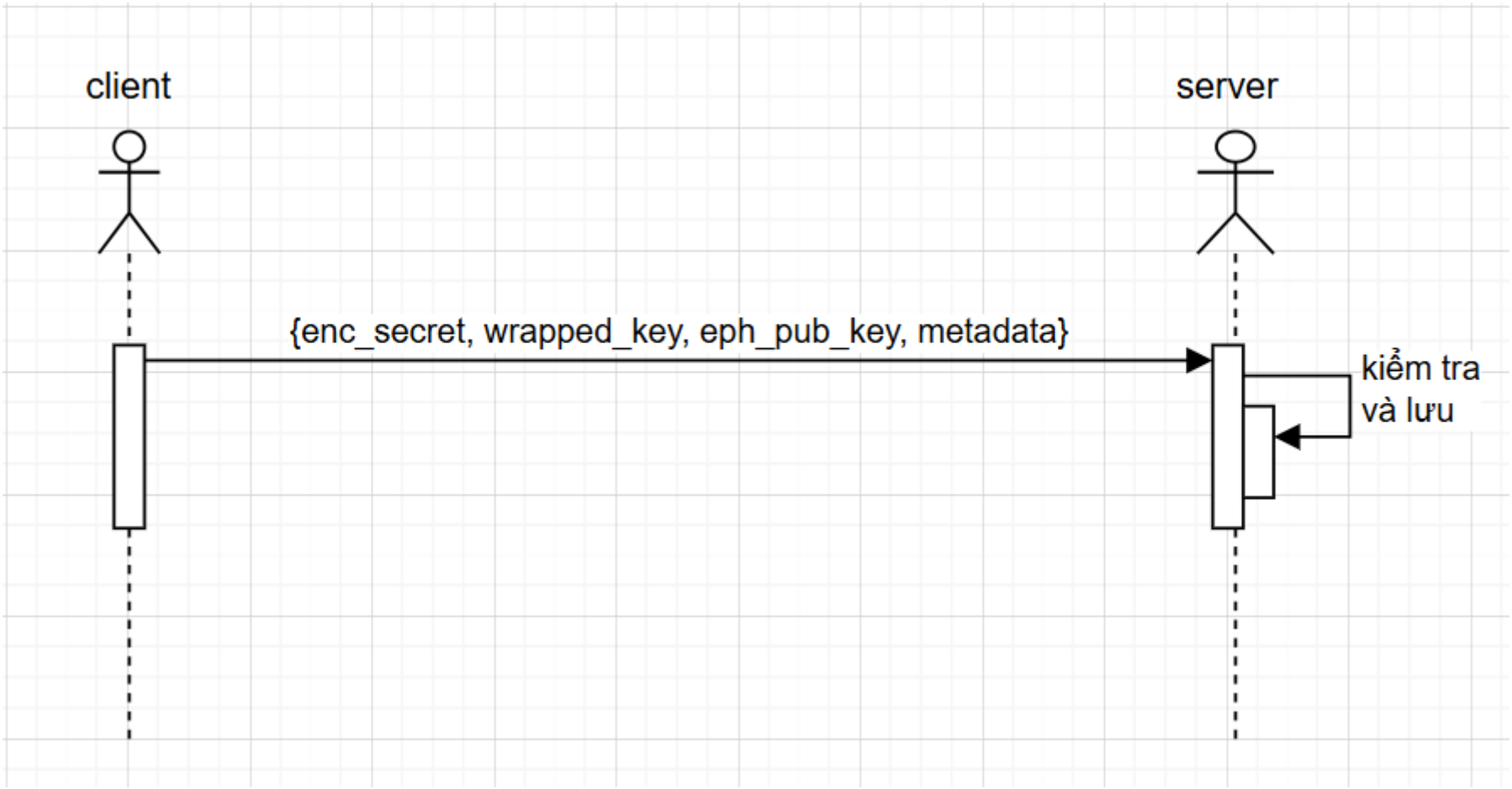
Tạo secret

- Bọc khóa



6. Luồng hoạt động chi tiết

Tạo secret



6. Luồng hoạt động chi tiết

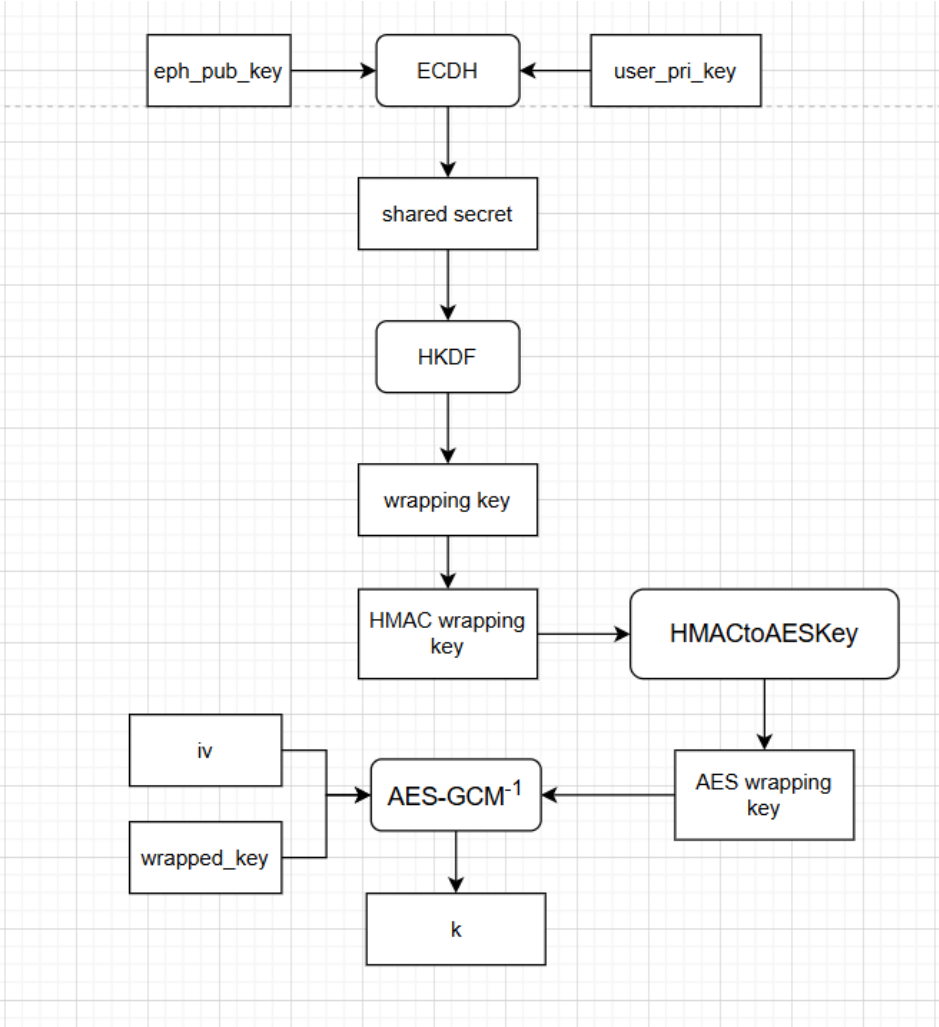
Tạo secret


```
_id: ObjectId('696a6c349319e4cb359c7eec')
name : "hh"
owner : ObjectId('6967600ec760633a6a3f10ec')
category : "general"
▸ tags : Array (empty)
▸ encrypted_data : Object
▾ access_list : Array (1)
  ▾ 0: Object
      user_id : ObjectId('6967600ec760633a6a3f10ec')
      role : "owner"
    ▸ permissions : Object
    ▾ wrapped_key : Object
      ▸ ephemeral_pub : Object
        iv : "cc4a7837813f316b01ef62d0"
        ciphertext : "4a08cd33b0013b2eb2106023f7fd715ab9a6ce9b542e3da507aa2b792bc33a1326d7d8…"
      granted_by : ObjectId('6967600ec760633a6a3f10ec')
      _id : ObjectId('696a6c349319e4cb359c7eed')
      granted_at : 2026-01-16T16:49:56.975+00:00
version : 1
current_version : 1
▸ rotation_policy : Object
checksum : "f8fd489801cddb101b9586908fa96f564150dddd034873eeb71af764414b4df7"
▸ expiration : Object
▸ key_versions : Array (empty)
created_at : 2026-01-16T16:49:56.975+00:00
updated_at : 2026-01-16T16:49:56.976+00:00
__v : 0
```

6. Luồng hoạt động chi tiết

Chia sẻ secret

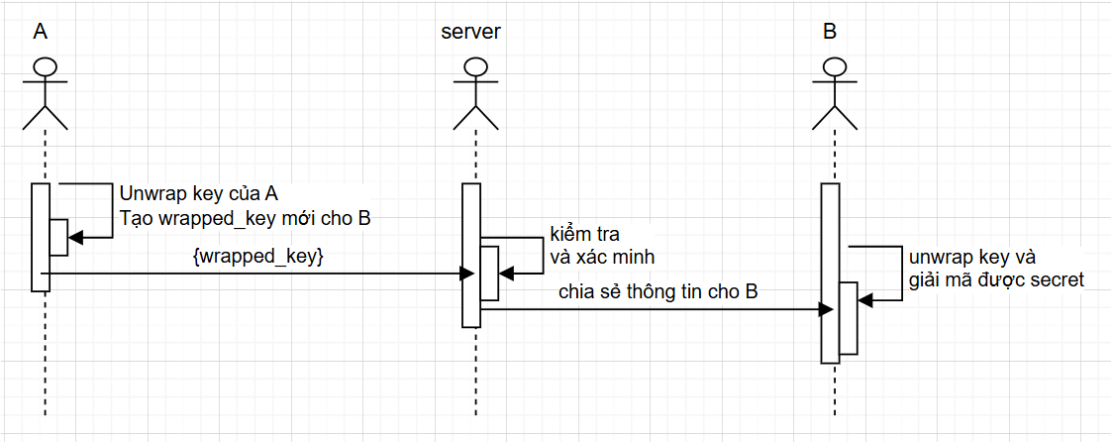
- Alice mở bọc khóa (unwrap key):



6. Luồng hoạt động chi tiết

Chia sẻ secret

- A thực hiện bọc lại khóa k cho B bằng khóa công khai của Bob và khóa private ephemeral mới được sinh ra. Sau đó A gửi đến server.
- Server xác minh và kiểm tra các quyền, tính toán mã checksum.
- B nhận được và mở bọc khóa, nhận được khóa k và dung nó để giải mã enc_secret.



7. Các tiêu chí bảo mật

- **Kiến trúc Zero-Knowledge**
  - Mã hóa bên Client
  - Server không biết plaintext
  - PBKDF2 (100,000 iterations)
- **Data Integrity**
  - SHA-256 checksums trên mỗi secret
  - Chống Rollback protection thông qua thông tin phiên bản
  - Chống Swap protection thông qua checksums
- **Đảm bảo Forward Secrecy**
  - Ephemeral ECDH P-384 key pairs
  - Each share = unique shared secret
  - Lộ bí mật không ảnh hưởng đến secret cũ

7. Các tiêu chí bảo mật

- **Key Wrapping**
  - Mỗi người dùng nhận được một khóa được đóng gói riêng biệt
  - HKDF để tạo khóa
  - Khả năng mở rộng
- **Role-Based Access Control (RBAC)**
  - Owner, Editor, Sharer, Viewer
  - Quyền hạn chi tiết cho từng người dùng
  - Nguyên tắc quyền hạn tối thiểu
- **Comprehensive Audit Logging**
- **Rate Limiting + Exponential Backoff**
  - Chống tấn công Brute-force

8. Demo

Demo

HUST

THANK YOU !