**Xây dựng hệ thống quản lý tài sản số**

Loại tài sản: lyric, các định dạng file mp3, mp4.

Ứng dụng hướng tới bảo vệ các quyền của chủ sở hữu tài sản. Gồm hai quyền cơ bản: quyền sử dụng, quyền sở hữu.

Các file nhạc được sử dụng trên hệ thống được xây dựng.

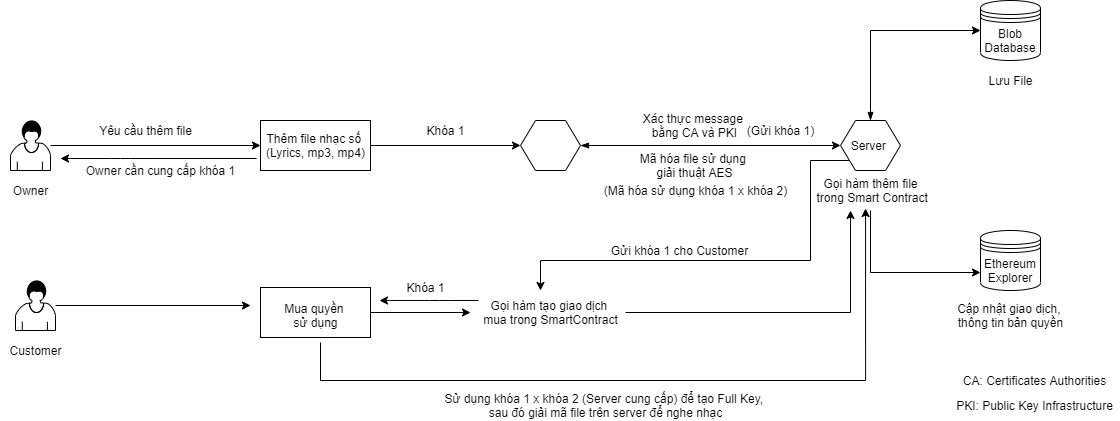
1. Quyền sử dụng:
   1. Hướng quản lý:

* Quản lý về số lần sử dụng.
* Quản lý về thời gian sử dụng.
  1. Các loại tình huống sử dụng:

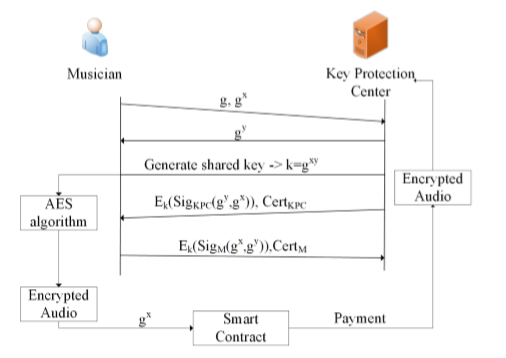
Ban đầu, khi tải lên file nhạc, file sẽ được mã hóa dựa theo khóa đầy đủ (Gộp từ khóa 1 x khóa 2).

* + 1. Đối với người sở hữu: (Chính)
  + Sở hữu đầy đủ full key mã hóa
  + Cho phép tải về file gốc (File chưa mã hóa)
  + Cập nhật thông tin file nhạc: Title, Thể loại,…
  + Chuyển quyền sở hữu tài sản cho người khác
  + Chia sẻ quyền sở hữu
    1. Tình huống chia sẻ quyền sở hữu:
  + Lúc này, hệ thống sẽ gồm 2 loại người sở hữu đối với file nhạc đó:
    - Người sở hữu chính: (Người tải lên file nhạc lần đầu tiên)
      * Có tất cả các quyền như ở mục 1.2.1
      * Nhận lợi nhuận thu được từ bản quyền nhạc số
      * Thay đổi người nhận lợi nhuận (Nếu có nhu cầu)
    - Người sở hữu phụ:
      * Sở hữu full key mã hóa
      * Cho phép tải về file gốc
      * Sẽ được hưởng lợi nhuận nếu được sở hữu chính cho phép
    1. Tình huống chuyển quyền sở hữu:
  + Cập nhật thông tin chủ sở hữu mới cho file nhạc
  + Xóa bỏ khóa cũ của file nhạc, tạo ra khóa đầy đủ mới và mã hóa lại file
  + Cấp cho người sỡ hữu mới full key đã tạo
    1. Tình huống đối với quyền sử dụng:
  + Cấp cho người dùng khóa 1, người dùng cần kết nối với Server (Giữ khóa 2) để có thể play file trên hệ thống
  + Mỗi file nhạc sẽ có định danh riêng, thời gian sử dụng, số lần sử dụng
  + Mỗi lần người dùng kết nối với Server sẽ cập nhật số lần sử dụng, kiểm tra thời gian sử dụng, nếu đã quá hạn sẽ không cho phép play file
    1. Tình huống khi người dùng không có quyền sử dụng:
  + File nhạc đã được mã hóa, đối với người không có quyền sử dụng, kể cả khi họ có lấy được file, nhưng không có khóa 1 và thông tin tài khoản có quyền sử dụng để có thể mã hóa file, thì file không thể play được
  + Kiểm tra file có được chỉnh sửa dựa vào tác động của bên ngoài:
    - File trước khi được giải mã sẽ được chuyển đổi sang dạng bit, hệ thống sẽ kiểm tra sự thay đổi của file dựa vào CheckSum

1. Hướng kiểm soát tài sản:
   1. Thực hiện kiểm soát tài sản từ lúc bắt đầu đưa lên hệ thống.
   2. Thực hiện các loại mã hóa để xác thực tài sản và bảo vệ quyền lợi của chủ sở hữu.
   3. Thực hiện truy xuất nguồn gốc khi xảy ra tranh chấp, kiện tụng liên quan tới tài sản trên hệ thống Smart Contract.



Cụ thể, quy trình xác thực Message bằng CA và PKI như sau:



B1: Owner chọn g và random x, sau đó tính đc g^x (Khóa 1)

Sau đó gửi khóa 1 và giá trị g cho Server

B2: Khi Server nhận được khóa 1 thì sẽ khởi tạo g^y (Khóa 2), gửi cho Owner

B3: Server tạo chữ kí số với private key của nó, sau đó mã hóa chữ kí đó với key shared (k)

Đồng thời cũng gửi Certificate Server kèm với chữ kí sau khi mã hóa cho Owner

Owner sẽ lấy Public key từ Certificate Server để xác nhận chữ kí trên

B4: Tác giả tạo chữ kí với các bước như trên, sau đó Server sẽ dùng Certificate Owner lấy public key của Owner ra và xác nhận chữ kí của Server

Trong quá trình này, cả Owner và Server sẽ sở hữu shared key g^(xy) (Full Key)

Đối với mã hóa file:

B5: Tác giả sẽ sử dụng shared key (Full Key) để mã hóa file audio với (AES giải thuật), khóa 1 được lưu vào smart contract

B6: Khi Customer thanh toán giao dịch nhạc, họ có thể lấy khóa 1, sau đó kết nối tới (Server) để tạo Full Key, key đó để giải mã file.

* Việc này đảm bảo: 1. File tải về chỉ có thể dùng ở Server

2. File của Customer 1 tải về, copy cho Fan 2 thì Fan 2 không mở được vì Customer chỉ sở hữu khóa 1, không đủ để giải mã file

*Message được mã hóa gửi kèm với chữ kí điện tử bao gồm:*

Định danh file + TimeStamp (Thời gian giao dịch) + PubKey Server + Số lần sử dụng.

*Kiểm tra file đã bị sửa đổi bằng Checksum:*

Cụ thể, *Thứ tự file đã tạo dạng binary 8 bit* + mã hóa file sang dạng binary

Mỗi lần Customer yêu cầu play file sẽ check sự thay đổi so với mã gốc

**Các nguồn tài liệu tham khảo:**

**A Blockchain and Smart Contract Based Application for Music Copyright Protection**

Link cụ thể tài liệu: <https://dl.acm.org/doi/pdf/10.1145/3301403.3301404?download=true>

**Digital Certificates and Public Key Infrastructure (PKI)**

<http://cuonglv1109.blogspot.com/2020/03/digital-certificate-and-certificate.html>

**Thuật giải mã hóa AES:**

<https://viblo.asia/p/tim-hieu-thuat-toan-ma-hoa-khoa-doi-xung-aes-gAm5yxOqldb>

**Ebook Laudon - E-Commerce 2016**: Phần Public Key Cryptography Using Digital Signatures