**Phần mềm quản lý chữ ký số**

**I. Chức Năng Người Dùng**

Hệ thống chữ ký số cung cấp đa dạng các chức năng cho người dùng. Các chức năng này bao gồm:

**1. Đăng ký, Đăng nhập**

- Đăng ký: Người dùng có thể nhập thông tin và đăng ký tài khoản mới.

- Đăng nhập: Người dùng đăng nhập với tài khoản đã đăng ký và sử dụng các chức năng của hệ thống.

**2. Thay đổi thông tin**

- Thay đổi mật khẩu: Người dùng có thể đổi mật khẩu.

- Thay đổi thông tin cá nhân: Người dùng có thể thay đổi các thông tin cá nhân ví dụ họ và tên, địa chỉ, email, số điện thoại.

**3. Đăng ký bộ khóa**

- Gửi yêu cầu đăng ký: Người dùng có thể gửi yêu cầu nhận bộ khóa số (Public Key và Private Key) và chờ quản trị viên phê duyệt.

- Nếu yêu cầu bị từ chối thì phải thay đổi thông tin cá nhân để được đăng ký lại.

- Nếu quản trị viên xóa bộ khóa thì có thể đăng ký lại để nhận bộ khóa mới.

**4. Quản lý bộ khóa**

- Xem bộ khóa: Người dùng có thể xem thông tin bộ khóa số sau khi được cấp.

- Tải xuống: Người dùng có thể tải xuống nội dung của bộ khóa theo dạng file txt.

**5. Xác thực người gửi**

- Băm văn bản: Người dùng upload một file lên, và sau đó băm nội dung của file sử dụng mã băm SHA-256.

- Ký: Người dùng upload và sử dụng khóa bí mật (Private Key) để mã hóa đoạn băm của văn bản ở trên, kết quả thu được sẽ là một đoạn mã (gọi là văn bản đã ký). Có thể tải xuống văn bản đã ký thành dạng file txt.

- Xác thực: Người dùng upload văn bản gốc, văn bản đã ký và khóa công khai (Public Key) tương ứng. Chỉ khi cả 3 file đều đúng thì sẽ cho ra kết quả là “Văn bản và chữ ký đều hợp lệ”. Nếu một trong 3 file trên upload không đúng thành file khác thì cho ra kết quả “Chữ ký không hợp lệ hoặc văn bản đã bị thay đổi”. Mã hóa và giải mã đều sử dụng thuật toán RSASSA-PKCS1-v1\_5.

**II. Chức Năng Quản Trị**

Hệ thống quản lý chữ ký số cung cấp một số chức năng cho quản trị viên nhằm hỗ trợ việc quản lý các bộ khóa số một cách hiệu quả. Các chức năng này bao gồm:

**1. Đăng nhập**

Quản trị viên đăng nhập với tài khoản đã được cấp và sử dụng các chức năng quản trị của hệ thống.

**2. Phê duyệt**

- Quản trị viên có quyền xem xét, phê duyệt hoặc từ chối các yêu cầu tạo bộ khóa từ phía người dùng.

- Phê duyệt thì cấp bộ khóa số cho người dùng, không cho phép người dùng đăng ký lại.

- Nếu từ chối thì yêu cầu người dùng phải thay đổi thông tin thì mới được đăng ký lại bộ khóa.

**3. Quản lý**

- Hỗ trợ quản trị viên quản lý danh sách các tài khoản đã được cấp bộ khóa.

- Cho phép thực hiện thao tác xóa bộ khóa. Sau đó người dùng có thể đăng ký lại bộ khóa mới.

**III. Kết Quả Đạt Được**

Phần mềm quản lý chữ ký số có giao diện bắt mắt và dễ sử dụng giúp người dùng cũng như quản trị viên cung cấp và quản lý bộ khóa số nhanh chóng. Ngoài ra còn có chức năng xác thực người gửi để đảm bảo người gửi hợp lệ và tài liệu không bị thay đổi trong quá trình gửi đi.