ĐẠI HỌC BÁCH KHOA HÀ NỘI
KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO TỔNG KẾT ĐỀ TÀI NGHIÊN CỨU
THEO NGHỊ ĐỊNH THƯ

HỆ THỐNG AN NINH THÔNG TIN DỰA TRÊN SINH TRẮC HỌC Bio-PKI (Bio-PKI Based Information Securyty System)

CHỦ NHIỆM ĐỀ TÀI: PGS.TS. NGUYỄN THỊ HOÀNG LAN

7327
04/5/2009

HÀ NỘI - 2009

BỘ GIÁO DỤC VÀ ĐÀO TẠO
Trường Đại học Bách khoa Hà Nội

BÁO CÁO TỔNG HỢP

Đề tài nhiệm vụ theo nghị định thư

Hệ thống an ninh thông tin dựa trên sinh trắc học Bio-PKI (Bio-PKI Based Information Security System)

Mã số: 12/2006/HĐ-NĐT

Chủ nhiệm đề tài

PGS.TS Nguyễn Thị Hoàng Lan
Khoa Công nghệ thông tin,
Đại học Bách khoa Hà Nội

Hà Nội 1 - 2009

MỤC LỤC

DANH SÁCH CÁC CÁN BỘ VÀ SINH VIÊN THAM GIA THỰC HIỆN ĐỀ TÀI

A. DANH SÁCH CÁC CÁN BỘ THAM GIA TRỰC TIẾP

1. PGS.TS Nguyễn Thị Hoàng Lan	Khoa CNTT, ĐHBK HN, chủ nhiệm đề tài
2. TS Nguyễn Linh Giang	Khoa CNTT, ĐHBK HN
3. TS Hà Quốc Trung	Khoa CNTT, ĐHBK HN
4. ThS Bành Quỳnh Mai	Khoa CNTT, ĐHBK HN
5. ThS Nguyễn Anh Hoàn	Khoa CNTT, ĐHBK HN
6. TS Ngô Hồng Sơn	Khoa CNTT, ĐHBK HN
7. KS Nguyễn Thị Hiền	Khoa CNTT, ĐHBK HN

B. DANH SÁCH CÁC CÁN BỘ THAM GIA TƯ VẤN

1. PGS.TS Đặng Văn Chuyết	Khoa CNTT, ĐHBK HN
2. ThS Đỗ Văn Uy	Khoa CNTT, ĐHBK HN
3. ThS Ngô Minh Dũng	Viện Khoa học hình sự, Bộ Công An

C. DANH SÁCH CÁC SINH VIÊN THAM GIA THỰC HIỆN ĐỀ TÀI

1. Các sinh viên đại học

Tóm tắt các phiên bản đã thiết kế triển khai theo tiến độ

- **Phiên bản hệ thống BioPKI Ver.1 (tháng 6 đến 12- 2006)**

- Nghiên cứu và thử nghiệm các thuật toán: Thu nhận vân tay, trích chọn đặc trưng, sinh khóa sinh trắc và thẩm định xác thực vân tay
- Nghiên cứu các hướng tiếp cận hệ thống BioPKI
- Xây dựng phương án và môi trường phần mềm hệ thống BioPKI dựa trên bộ thư viện mở OpenSSL và ngôn ngữ C++

Danh sách nhóm sinh viên tốt nghiệp 6-2006 đã tham gia đề tài:

1. Lê Anh Tuấn — TTM - K46
2. Ngô Trọng Cảnh — TTM – K46
3. Nguyễn Sinh Chung — Tin Pháp – K46
4. Nguyễn Văn Hạnh — KSCLC – K46

- **Phiên bản hệ thống BK-BioPKI Ver.2 (tháng 1-2007 đến 6-2007)**

- Phân tích thiết kế các mô đun cơ sở hạ tầng hệ thống PKI: CA, RA User
- Tiếp tục nghiên cứu và thử nghiệm các thuật toán sinh trắc học vân tay
- Xây dựng và thiết kế phần mềm phần hệ sinh trắc học (Biometric) bao gồm: Ký mã sinh trắc và thẩm định vân tay trong hệ thống BK-BioPKI

Danh sách nhóm sinh viên tốt nghiệp 6-2007 đã tham gia đề tài:

1. Nguyễn Thạc Hiếu TTM - K47
2. Nguyễn Quang Thụ TTM - K47
3. Phạm Quang Thịnh TTM - K47
4. Nguyễn Hoàng Anh Tin Pháp - K47
5. Phạm Sỹ Lâm KSCLC - K47
6. Tống Mạnh Cường TTM - K47

- **Phiên bản hệ thống BK-BioPKI Ver. 3.1 và phiên bản Ver.4 tích hợp hệ thống (tháng 7-2007 đến 6-2008)**

- Phân tích thiết kế phát triển và lập trình toàn bộ Protoptye cơ sở hạ tầng hệ thống BK-BioPKI trong môi trường mạng PTN
- Phân tích thiết kế phát triển phân hệ sinh trắc Biometric với 2 môđun và thử nghiệm vào ứng dụng hệ thống Ver.4
- Phân tích thiết kế tích hợp phân hệ sinh trắc vào toàn bộ hệ thống BK-BioPKI phiên bản Ver.4
- Xây dựng mô hình kịch bản 3 ứng dụng trong hệ BK-BioPKI Ver. 4

Danh sách nhóm sinh viên tốt nghiệp 6-2008 đã tham gia thiết kế phát triển hệ thống BioPKI và tham gia viết báo cáo tổng hợp đề tài:

1. Lê Tiến Dũng (trưởng nhóm) TTM - K48
2. Bùi Thành Đạt TTM - K48
3. Nguyễn Thị Thu Hằng KSTN - K48
4. Trần Hải Anh Tin Pháp - K48
5. Dương Văn Đô Tin Pháp - K48
6. Hoàng Trần Đức TTM - K48
7. Ngô Tiến Dũng TTM - K48
8. Trần Nguyên Ngọc TTM - K48
9. Vũ Ngọc Hà TTM - K48

2. Các học viên cao học đã tốt nghiệp thạc sĩ theo hướng đề tài

1. Trần Tuấn Vinh khóa 2003-2005 đã bảo vệ 2006
2. Nguyễn Anh Tài khóa 2004-2006 đã bảo vệ 2007
3. Vũ Thanh Thắng khóa 2005-2007 đã bảo vệ 2007
4. Lê Quang Tùng khóa 2006-2008 đã bảo vệ 11- 2008
5. Lê Trần Vũ Anh khóa 2006-2008 đã bảo vệ 11- 2008
6. Hà Tiến Dũng khóa 2006-2008 đã bảo vệ 11- 2008

Phần I. THÔNG TIN CHUNG VỀ ĐỀ TÀI

1. Tên đề tài

Hệ thống an ninh thông tin dựa trên sinh trắc học Bio-PKI (Bio-PKI Based Information Security System)

Mã số: 12/ 2006/ HĐ-NĐT

2. Chủ nhiệm đề tài: PGS. TS Nguyễn Thị Hoàng Lan

Học hàm, học vị, chuyên môn: PGS.TS ngành Công nghệ Thông tin

Chức danh: Phó Trưởng khoa Công nghệ Thông tin, Đại học Bách Khoa Hà Nội

Điện thoại cơ quan : (84. 4) 38.68.25.96

Điện thoại nhà riêng : (84. 4) 38.32.89.25

Email: lannth@it-hut.edu.vn

3. Cơ quan chủ trì

Đại học Bách Khoa Hà Nội, Khoa Công nghệ Thông tin

Số 1 đường Đại Cồ Việt, Hà Nội

4. Họ và tên Chủ nhiệm phía đối tác nước ngoài:

TS. Ong Thian Song

Chức danh: Giám đốc điều hành Trung tâm nghiên cứu Sinh trắc học (CBB)

Trường Đại học Đa phương tiện Malaysia (MMU)

Tel: +606-252.33.43

Fax: +606-231.88.40

Emal: tsong@mmu.edu.vn

5. Cơ quan đối tác nước ngoài: Trường Đại học Đa phương tiện Malaysia (Malaysia Multimedia University -MMU),

Trung tâm nghiên cứu Sinh trắc học và Sinh –Tin học (Center of Biometrics and Bioinformatics – CBB)

Khoa Khoa học và Công nghệ thông tin (Faculty of Information Science and Technology - FIST)

Malaysia Multimedia University (MMU),

Jalan Ayer Keroh Lama, 75450 Melaka Malaysia

http:///www.mmu.edu.my

6. Thời gian thực hiện đề tài: Từ 6/2006 đến 6/2008

7. Tổng kinh phí thực hiện đề tài: 800.000.000 VNĐ

Tổng kinh phí đã cấp 2006: 450.000.000 VNĐ
Tổng kinh phí đã cấp 2007: 350.000.000 VNĐ
Đề tài đã nhận được cấp đủ kinh phí đến 6/2008.

8. Mục tiêu của Nhiệm vụ

Hệ thống an ninh thông tin (Bio-PKI Based Information Security System) kết hợp các dấu hiệu đặc trưng sinh trắc học vân tay con người vào hạ tầng cơ sở bảo mật khóa công khai PKI là hướng nghiên cứu mới cho phép mang lại những ưu điểm hơn các hệ thống khóa công khai hiện có về độ an toàn bảo mật, về tính xác thực thẩm định trong các giao dịch, các dịch vụ điện tử qua mạng máy tính.

Mục tiêu của Nhiệm vụ đề tài theo nghị định thư hợp tác với Malaysia chủ yếu bao gồm:

- Nghiên cứu đề xuất phương án kết hợp các đặc trưng của vân tay với mã bảo mật khóa công PKI tạo khóa mã sinh trắc học hệ BioPKI.
- Xây dựng thử nghiệm hạ tầng cơ sở hệ thống an ninh thông tin Bio-PKI (protoptype). Thiết kế và xây dựng thử nghiệm phần mềm hệ thống an ninh thông tin dựa trên mã sinh trắc học Bio-PKI nhằm hướng tới ứng dụng trong xác thực, thẩm định sinh trắc học và kiểm soát truy cập dùng trong các lĩnh vực an ninh, thương mại điện tử, ngân hàng, giao dịch điện tử, chính phủ điện tử….
- Tích hợp các kết quả nghiên cứu của 2 phía Việt Nam và Malaysia, thử nghiệm phát triển ứng dụng hệ thống Bio-PKI.

9. Yêu cầu khoa học đối với sản phẩm tạo ra (kết quả dạng III)

- ***Tên sản phẩm***:

Hệ thống an ninh thông tin dựa trên mã sinh trắc học Bio-PKI (gọi tắt là Hệ thống an ninh thông tin Bio-PKI), bao gồm:

- Kết quả giải pháp tích hợp đặc trưng vân tay với mã bảo mật trong hệ PKI thành hệ BioPKI.
- Kết quả thử nghiệm Prototype về hạ tầng hệ thống BioPKI để thẩm định vân tay trong hệ BioPKI.
- Kết quả phần mềm máy tính cho hệ thống BioPKI, phân hệ sinh trắc bao gồm: phần mềm phân hệ mã hóa khóa sinh trắc học vân tay BioPKI và phần mềm xác thực thẩm định vân tay.
- Báo cáo phân tích hệ thống và hướng xây dựng ứng dụng trong xác thực thẩm định vân tay và điều khiển truy nhập trong hệ BioPKI. Báo cáo tổng hợp đề tài.

- ***Các sản phẩm khác***:

- Đào tạo thạc sĩ, kỹ sư
- Các bài báo khoa học

Phần II. BÁO CÁO NGHIÊN CỨU TỔNG HỢP

Chương 1.
KHẢO SÁT VỀ GIAO DỊCH ĐIỆN TỬ, CÁC YÊU CẦU AN NINH THÔNG TIN. XÁC ĐỊNH NHIỆM VỤ CỦA ĐỀ TÀI

1.1. Khái quát chung

Những năm cuối của thế kỉ XX và đầu thế kỉ XXI chứng kiến sự lớn mạnh vượt bậc của mạng Internet cả về quy mô và chất lượng. Internet được ứng dụng rộng rãi ở mọi ngành nghề, lĩnh vực kinh tế, xã hội và an ninh. Tính phổ biến rộng rãi khiến Internet đã và đang là nền tảng cơ sở cho các giao dịch thương mại toàn cầu và các ứng dụng của giao dịch điện tử tạo thành một hình thức "xã hội ảo" với các đặc trưng riêng biệt. Trong môi trường xã hội thật, mối quan hệ giữa các đối tác thường được xác định rõ ràng bởi quá trình gặp gỡ, ký kết thường diễn ra một cách trực tiếp, không hoặc ít thông qua phương tiện truyền thông trung gian. Các tổ chức chính phủ, doanh nghiệp và các cá nhân khi tham gia giao dịch điện tử luôn đòi hỏi không những phải bảo vệ toàn vẹn thông tin lưu chuyển trên Internet mà còn phải cho họ cảm giác tin cậy giống như khi giao dịch trên giấy tờ. Họ muốn những người tham gia đúng là những người được yêu cầu, và mỗi cá nhân phải chịu trách nhiệm về hành vi liên quan của mình trong giao dịch khi có sự cố xảy ra. Tuy nhiên, môi trường mạng không phải luôn an toàn. Đặc trưng của Internet là tính "ảo" và tính tự do, mọi người đều có thể tham gia và ít để lại dấu vết cá nhân của mình. Việc xác thực mỗi cá nhân qua mạng thường là khó khăn nên nguy cơ xảy ra giả mạo định danh, bị lừa đảo trực tuyến là rất cao. Đây là vừa là điểm mạnh và cũng là điểm yếu của giao dịch điện tử qua mạng Internet. Những năm gần đây các hình thức phạm tội trong môi trường mạng và công nghệ cao tăng nhanh chóng cùng với sự phát triển của công nghệ. Mặc dù các đặc điểm trên, tính tiện lợi, phổ dụng và hiệu quả của công nghệ cao đang làm thay đổi cuộc sống và các giao dịch điện tử thương mại điện tử ngày càng phát triển nhanh chóng trên phạm vi thế giới. Vì thế nhu cầu xây dựng một hệ thống bảo mật an toàn thông tin, đảm bảo giao tiếp giữa những người dùng một cách an toàn, có định danh và chống phủ nhận trở nên hết sức cấp thiết trong phạm vi mỗi quốc gia cũng như phạm vi toàn cầu.

Hiện nay vấn đề nghiên cứu các giải pháp nhằm đảm bảo an toàn thông tin, bảo mật dữ liệu trong các giao dịch điện tử qua môi trường mạng luôn là vấn đề thời sự được tất cả các quốc gia và các tổ chức quốc tế quan tâm cả về phương diện pháp lý và phương diện kỹ thuật và công nghệ. Giải pháp an ninh dựa trên các dấu hiệu sinh trắc học là một trong các hướng nghiên cứu mới đang được thế giới quan tâm phát triển và áp dụng. Trên thực tế cũng đã có các sản phẩm quảng cáo trong các giao dịch điện tử như thẻ ngân hàng sinh trắc học, thẻ mua hàng, thẻ an ninh, hộ chiếu sinh trắc học ..., tuy nhiên hiện nay vẫn chưa có các

sản phẩm thương mại được triển khai rộng rãi có hiệu quả cao trên thực tế, hơn nữa việc nghiên cứu liên quan đến sinh trắc học con người luôn là vấn đề nhậy cảm có đặc thù của từng quốc gia. Bởi vậy giải pháp này vẫn luôn được đặc biệt quan tâm nghiên cứu và phát triển.

Đề tài nghiên cứu "Hệ thống an ninh thông tin dựa trên mã sinh trắc học Bio-PKI (Bio-PKI InfoSec System)" theo nghị định thư hợp tác với Malaysia do phía Malaysia đề nghị, được thực hiện trên cơ sở hợp tác nghiên cứu giữa trường Đại học Đa phương tiện Malaysia (MMU) và trường Đại học Bách Khoa Hà Nội (HUT). Malaysia là một nước phát triển trong khu vực Đông Nam Á, có điều kiện địa lý và môi trường tương đối gần với Việt Nam, Đại học Đa phương tiện Malaysia (MMU) là trường có uy tín của Malaysia và có điều kiện cơ sở vật chất khá hiện đại. Hợp tác với Malaysia là trong điều kiện hiện nay là phù hợp với điều kiện nước ta, cho phép chúng ta có thể tiếp cận ở mức độ phù một mặt với nền công nghệ cao, mặt khác tiếp cận về trình độ nghiên cứu khoa học để hòa nhập khu vực và tiến tới hòa nhập với thế giới.

1.2. Khảo sát về thương mại điện tử, giao dịch điện tử trên thế giới

1.2.1. Giao dịch thương mại điện tử

Ngày nay, cùng với các ứng dụng công nghệ thông tin, hình thức thương mại truyền thống đang dần thay đổi sang một hình thức khác, đó là thương mại điện tử. Thương mại điện tử bắt đầu xuất hiện từ những năm 1970 với sự ra đời của hoạt động chuyển nhượng quỹ điện tử giữa các ngân hàng thông qua các mạng an toàn tư nhân. Thập kỷ 1980, biên giới thương mại điện tử mở rộng đến các hoạt động trao đổi nội bộ dữ liệu điện tử và thư viện điện tử. Các dịch vụ trực tuyến bắt đầu xuất hiện vào giữa những năm 1980. Chỉ đến thập kỷ 1990, thương mại điện tử mới chuyển từ các hệ thống cục bộ sang mạng toàn cầu Internet. Hàng loạt các tên tuổi lớn (Amazon.com, Yahoo!, eBay.com, NTTDoMoCo, Dell, Electrolux, WallMart ...) đã khẳng định và góp phần vào sự tăng trưởng nhanh chóng giá trị giao dịch thông qua thương mại điện tử.

Ngày nay người ta hiểu khái niệm thương mại điện tử thông thường là tất cả các phương pháp tiến hành kinh doanh và các quy trình quản trị thông qua các kênh điện tử mà trong đó Internet (hay ít nhất là các kỹ thuật và giao thức được sử dụng trong Internet) đóng một vai trò cơ bản và công nghệ thông tin được coi là điều kiện tiên quyết. Thông thường có 3 đối tượng chính tham gia vào hoạt động thương mại điện tử là: Người tiêu dùng – C (Consumer) giữ vai trò quyết định sự thành công của thương mại điện tử; Doanh nghiệp – B (Business) đóng vai trò là động lực phát triển thương mại điện tử và Chính phủ - G (Government) giữ vai trò định hướng, điều tiết và quản lý các hoạt động thương mại điện tử.

Các hình thức hoạt động của giao dịch thương mại điện tử:

- Thư điện tử (e-mail): các tổ chức, cá nhân có thể gửi thư cho nhau một cách trực tuyến thông qua mạng. Đây là hình thức phổ biến nhất và dễ thực hiện nhất, hầu như mọi người ở mọi lứa tuổi đều có thể sử dụng.

- Thanh toán điện tử (e-payment): là việc thanh toán tiền thông qua hệ thống mạng (chẳng hạn như: trả lương bằng cách chuyển tiền trực tiếp vào tài khoản, trả tiền mua hàng bằng thẻ tín dụng, thẻ mua hàng...). Ngoài ra, thanh toán điện tử còn áp dụng trong các dịch vụ như: trao đổi dữ liệu điện tử tài chính (FEDI) phục vụ cho việc thanh toán điện tử giữa các công ty giao dịch với nhau bằng điện tử; tiền mặt Internet (Internet Cash) là tiền mặt được mua từ một nơi phát hành (ngân hàng hoặc tổ chức tín dụng) rồi được chuyển đổi sang các đồng tiền khác thông qua Internet; túi tiền điện tử (electronic purse) là nơi để tiền mặt Internet, chủ yếu là thẻ thông minh smart card, tiền được trả cho bất kỳ ai đọc được thẻ; giao dịch ngân hàng số hoá (digital banking), giao dịch chứng khoán số hoá (digital securities trading) phục vụ cho các hoạt động thanh toán giữa ngân hàng với khách hàng, giữa ngân hàng với các đại lý thanh toán, giữa hệ thống ngân hàng này với hệ thống ngân hàng khác hay thanh toán trong nội bộ một hệ thống ngân hàng.

- Trao đổi dữ liệu điện tử (EDI) là việc chuyển giao thông tin từ máy tính điện tử này sang máy tính điện tử khác bằng phương tiện điện tử, có sử dụng một tiêu chuẩn đã được thỏa thuận để cấu trúc thông tin, công việc trao đổi thường là giao dịch kết nối, đặt hàng giao dịch gửi hàng hoặc thanh toán.

- Truyền tải nội dung: tin tức, phim ảnh, chương trình phát thanh, truyền hình, chương trình phần mềm, vé máy bay, vé xem phim, hợp đồng bảo hiểm ... được số hoá và truyền gửi theo mạng.

- Mua bán hàng hoá hữu hình: hàng hoá hữu hình là tất cả các loại hàng hoá mà con người sử dụng được chào bán và được chọn mua thông qua mạng như: ô tô, xe máy, thực phẩm, vật dụng, thuốc, quần áo ... Người mua xem hàng, chọn hàng hoá và nhà cung cấp trên mạng, sau đó xác nhận mua và trả tiền bằng thanh toán điện tử. Người bán sau khi nhận được xác nhận mua và tiền điện tử của người mua sẽ gửi hàng hoá theo đường truyền thống đến tay người mua.

Các hình thức hoạt động của thương mại điện tử vẫn đang ngày một mở rộng và có nhiều sáng tạo. Ngày nay, rất nhiều ngành công nghiệp cũng như các lĩnh vực xã hội khác nhau cũng tham gia vào thị trường thương mại điện tử. Và như vậy, lợi ích mà thương mại điện tử đem lại cho cuộc sống của con người hiện đại cũng ngày một mở rộng hơn, nâng cao hơn.

1.2.2. Tình hình ứng dụng thương mại điện tử trên trên thế giới

Cùng với sự phát triển mạnh mẽ của Internet toàn cầu thì các dịch vụ ứng dụng giao dịch điện tử cũng phát triển một cách nhanh chóng, đặc biệt là các dịch vụ thương mại điện tử. Có nhiều các thống kê khác nhau về doanh số thương mại điện tử và những thống kê ấy có sự khác biệt đáng kể. Theo số liệu tính toán của Forrester Research - một công ty nghiên cứu Internet ở Massachusetts, Mỹ - doanh số thương mại điện tử trên toàn thế giới không ngừng tăng nhanh: năm 1997 đạt 36 tỷ USD, năm 2000 đạt hơn 700 tỷ USD và năm 2002 đạt khoảng 2.293,5 tỷ USD .... Theo một thống kê gần đây nhất của Miniwatts Marketing Group thì tính đến hết tháng 3 năm 2008, Mỹ vẫn là quốc gia đứng đầu thế giới về số lượng người sử dụng Internet (trên 218 triệu người), chiếm 71,9% dân số trong nước và 15,5%

người dùng thế giới, tốc độ tăng trưởng giai đoạn 2000-2008 là 128,9%. Xếp thứ 2 sau Mỹ là Trung Quốc chiếm 14,9% người dùng thế giới, tốc độ tăng trưởng giai đoạn 2000-2008 là 833,3%. Nhật Bản đứng thứ 3 trong bảng xếp hạng, Hàn Quốc đứng thứ 9 và Việt Nam đứng thứ 17 sau Indonesia.

Sự phát triển của thương mại điện tử dường như không có giới hạn mặc dù gặp khá nhiều trở ngại. Cụ thể là trong những năm qua, tuy có thời gian các công ty thương mại điện tử gặp phải không ít khó khăn, song tỷ lệ tăng việc làm trong các công ty này (khoảng 10%) vẫn tăng nhanh hơn tỷ lệ tăng việc làm của toàn bộ nền kinh tế. Những công việc liên quan đến mạng Internet cũng tăng khoảng 30%. Theo kết quả điều tra của Công ty Tình báo kinh tế (EIU) thuộc tạp chí The Economist, triển vọng phát triển thương mại điện tử trên thế giới rất tươi sáng, đặc biệt là khu vực Châu Á. Thương mại điện tử càng lúc càng phát triển trên thế giới và doanh thu do thương mại điện tử mang lại cũng tăng gần gấp đôi mỗi năm, đó là lý do nhiều nước đang ráo riết khuyến khích, thúc đẩy và xây dựng cơ sở cho việc phát triển thương mại điện tử. Về mặt pháp lý, hiện nay trên thế giới hầu hết các nước ứng dụng thương mại điện tử đều đã xây dựng cho mình những đạo luật và quy định riêng nhằm bảo vệ quyền lợi cho những người tham gia vào thị trường này cũng như để ổn định xã hội và phát triển kinh tế.

1.3. Tình hình phát triển các giao dịch điện tử ở Việt Nam và cơ sở pháp lý

1.3.1. Tình hình phát triển các giao dịch điện tử ở Việt Nam

Trong bảng xếp hạng của Miniwatts Marketing Group, tính đến hết tháng 3 năm 2008, Việt Nam đứng thứ 17 trong top các quốc gia có nhiều người sử dụng Internet nhất thế giới. Tính đến hết năm 2007, Việt Nam chúng ta hiện có số người sử dụng Internet nhiều thứ năm ở khu vực Châu Á, sau Trung Quốc, Nhật Bản, Ấn Độ, Hàn Quốc và Indonexia. Với tốc độ phát triển mạnh mẽ như vậy nên các ứng dụng của Internet, đặc biệt là các dịch vụ thương mại điện tử được tiếp nhận một cách nhanh chóng. Thương mại điện tử đã bắt xuất hiện tại Việt Nam từ những năm 90 và đến năm 2006 là năm có ý nghĩa đặc biệt đối với thương mại điện tử Việt Nam. Đó là năm đầu tiên thương mại điện tử được pháp luật thừa nhận chính thức khi Luật Giao dịch điện tử, Luật Thương mại (sửa đổi), Bộ luật Dân sự (sửa đổi) và Nghị định Thương mại điện tử có hiệu lực. Năm 2006 cũng là năm đầu tiên triển khai Kế hoạch tổng thể phát triển thương mại điện tử giai đoạn 2006-2010 theo Quyết định số 222/2005 /QĐ-TTg ngày 15 tháng 9 năm 2005 của Thủ tướng Chính phủ.

Theo kết quả khảo sát điều tra của Bộ Công thương năm 2007 về mức độ sẵn sàng ứng dụng thương mại điện tử trong các doanh nghiệp thuộc các ngành nghề khác nhau của Việt Nam cho thấy trung bình mỗi doanh nghiệp có 22.9 máy tính (năm 2006 là 17.6), 89% doanh nghiệp có từ 1 đến 50 máy, trong đó ngành ngân hàng, tài chính, tư vấn, bất động sản và dịch vụ công nghệ thông tin - thương mại điện tử có tỷ lệ trang bị máy tính cao nhất. Bên cạnh đó, tình hình đào tạo công nghệ thông tin và thương mại điện tử cũng có sự biến chuyển nhanh chóng và càng ngày càng được quan tâm đầu tư hơn. Năm 2004, chi phí cho đào tạo chỉ chiếm bình quân 12,3% tổng số chi phí công nghệ thông tin của doanh nghiệp thì

năm 2007, con số này đã tăng lên đến 20,5%. Hơn nữa, trong số các doanh nghiệp được khảo sát thì có đến 97% doanh nghiệp đã kết nối Internet. Điều này cho thấy độ sẵn sàng cho thương mại điện tử của các doanh nghiệp là rất cao. Kết quả điều tra trong 2 năm 2006 và 2007 cho thấy ứng dụng thương mại điện tử của doanh nghiệp ngày càng mở rộng trên mọi cấp độ và phát triển nhanh ở những ứng dụng có độ phức tạp cao. Tỷ lệ doanh nghiệp có website năm 2007 là 38%, tỷ lệ tham gia sàn giao dịch là 10%, tỷ lệ kết nối cơ sở dữ liệu với đối tác là 15% và có đến 80% doanh nghiệp được khảo sát có sử dụng hình thức ứng dụng thương mại điện tử phổ biến là e-mail trong đó có 65% doanh nghiệp nhận đặt hàng qua thư điện tử. Trong các doanh nghiệp hiện nay, tỷ lệ cán bộ chuyên trách về thương mại điện tử cũng gia tăng rõ rệt với mức trung bình là 2.7 người trong một doanh nghiệp, tăng gấp đôi so với con số 1.5 của năm 2006.

Trong năm 2006 đánh dấu sự hội nhập kinh tế quốc tế sâu sắc và toàn diện của Việt Nam. Việt Nam đã trở thành thành viên chính thức thứ 150 của Tổ chức Thương mại Thế giới (WTO). Việt Nam cũng đã thực hiện tốt vai trò nước chủ nhà của Diễn đàn Hợp tác kinh tế Châu Á Thái Bình Dương (APEC), thể hiện cam kết tiếp tục mở cửa nền kinh tế với thế giới. Tiến trình hội nhập kinh tế quốc tế đòi hỏi các doanh nghiệp phải quan tâm thực sự đến việc nâng cao khả năng cạnh tranh. Trong bối cảnh đó, thương mại điện tử là một công cụ quan trọng được nhiều doanh nghiệp quan tâm ứng dụng. Sự quan tâm của doanh nghiệp đối với thương mại điện tử được thể hiện qua các hoạt động giao dịch mua bán tại các sàn thương mại điện tử (e-Marketplace), dịch vụ kinh doanh trực tuyến, số lượng các website doanh nghiệp ... Đông đảo doanh nghiệp đã nhận thấy những lợi ích thiết thực của thương mại điện tử thông qua việc cắt giảm được chi phí giao dịch, tìm được nhiều bạn hàng mới từ thị trường trong nước và nước ngoài, số lượng khách hàng giao dịch qua thư điện tử nhiều hơn. Nhiều doanh nghiệp đã ký được hợp đồng với các đối tác thông qua sàn giao dịch thương mại điện tử.

Trên thực tế thanh toán điện tử liên tục là trở ngại lớn đối với sự phát triển của thương mại điện tử trong giai đoạn từ năm 2005 tới 2007. Tuy nhiên, năm 2007 đã đánh dấu sự phát triển nhanh chóng của lĩnh vực này. Ở tầm chính sách vĩ mô, đầu năm 2007 Chính phủ đã ra một văn bản quan trọng liên quan tới thanh toán điện tử đã có hiệu lực, đó là Quyết định số 291/2006/QĐ-TTg ngày 29 tháng 12 năm 2006 của Thủ tướng Chính phủ phê duyệt Đề án thanh toán không dùng tiền mặt giai đoạn 2006–2010 và định hướng đến năm 2020. Hiện nay hệ thống các ngân hàng thành viên của Smartlink và Banknetvn chiếm khoảng 90% thị phần thẻ cả nước và đang liên kết với nhau để từng bước thống nhất toàn thị trường thẻ. Các ngân hàng thương mại đã xây dựng lộ trình để chuyển dần từ công nghệ sử dụng thẻ từ sang công nghệ chip điện tử. Hầu hết các nghiệp vụ từ Ngân hàng Nhà nước tới các ngân hàng thương mại và các tổ chức tín dụng đã được ứng dụng công nghệ thông tin.

1.3.2. Hệ thống pháp lý cho thương mại điện tử của Việt Nam

Luật giao dịch điện tử được ban hành năm 2005 vùng với Nghị định số 57/2006/NĐ-CP về Thương mại điện tử là nghị định đầu tiên hướng dẫn Luật giao dịch điện tử, được ban hành vào ngày 9/6/2006. Tiếp theo là luật Công nghệ thông tin được ra đời năm 2006, đó là

cơ sở pháp lý quan trọng tạo ra môi trường pháp lý cho thương mại điện tử phát triển. Tiếp theo các luật đã có một loạt các văn bản quy phạm pháp luật hướng dẫn 2 luật này được ban hành trong năm 2007. Ngay trong năm 2007 Chính phủ đã ban hành liên tiếp các nghị định quan trọng, đó là:

- Nghị định số 26/2007/NĐ-CP quy định chi tiết thi hành Luật Giao dịch điện tử về Chữ ký số và Dịch vụ chứng thực chữ ký số,

- Nghị định số 27/2007/NĐ-CP về Giao dịch điện tử trong hoạt động tài chính,

- Nghị định số 35/2007/NĐ-CP về Giao dịch điện tử trong hoạt động ngân hàng,

- Nghị định số 63/2007/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực công nghệ thông tin,

- Nghị định số 64/2007/NĐ-CP về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

1.3.3. Một số vấn đề của giao dịch thương mại điện tử ở Việt Nam

Bên cạnh những thành công và thuận lợi của sự phát triển nhanh chóng, thương mại điện tử của Việt Nam cũng đang phải đối mặt với một số vấn đề lớn làm cản trở sự phát triển và mở rộng thị trường, hợp tác quốc tế. Trong các vấn đề đó, vấn đề an toàn thông tin, an ninh mạng, tội phạm liên quan đến thương mại điện tử đang là những vấn đề cấp bách cần giải quyết. Những hành vi lợi dụng công nghệ để phạm tội ngày một gia tăng; tình trạng đột nhập tài khoản, trộm thông tin thẻ thanh toán đã gây ảnh hưởng không nhỏ đến các hoạt động thương mại điện tử lành mạnh. Trên thực tế hình thức thanh toán điện tử hay giao dịch điện tử ở Việt Nam cho đến nay hầu như vẫn chưa thực sự đáp ứng được nhu cầu của người dùng do các vấn đề luật pháp, về ngân hàng và các nhà cung cấp dịch vụ thanh toán trung gian. Do vậy, người mua hàng trên mạng cuối cùng vẫn phải thanh toán bằng tiền mặt hoặc chuyển khoản cho nhà cung cấp qua 1 thiết bị trung gian khác mà không có thể thanh toán trực tiếp trên website bán hàng. Chính điều này đã gây cản trở không ít đến các hoạt động trực tuyến, gia tăng chi phí và tổn hại kinh tế của người tham gia.

1.4. Nhu cầu về an toàn bảo mật thông tin trong giao dịch điện tử

Lợi ích của thương mại điện tử và giao dịch điện tử đối với nền kinh tế quốc dân cũng như sự phát triển về mặt công nghệ và thị trường toàn cầu là vô cùng to lớn. Tuy nhiên, song hành cùng với những thuận lợi bao giờ cũng nảy sinh và tồn tại khó khăn. Vấn đề đáng lo ngại nhất hiện nay mà tất cả các quốc gia đều phải đối mặt đó là sự tấn công, phá hoại của một số phần tử xã hội, gây ảnh hưởng không nhỏ đến nền kinh tế. Một vấn đề bức xúc được đặt ra là nghiên cứu phát tiển các giải pháp an toàn thông tin cho thương mại điện tử và giao dịch điện tử qua mạng. Vấn đề đảm bảo an ninh quốc gia trong thời đại toàn cầu hoá về thông tin đã trở thành một thách thức lớn ngay cả với các quốc gia có một nền công nghệ thông tin hùng mạnh.

Tại Hà Nội, cuối tháng 3/2008 vừa qua đã diễn ra Hội thảo "Thế giới an ninh bảo mật – Security World 2008". Những báo cáo, tham luận tại Hội thảo đều cho thấy vấn đề an ninh các website, đặc biệt website của các công ty chứng khoán là những mối quan ngại lớn trong năm 2007. Với những diễn biến xảy ra, an ninh mạng Việt Nam năm 2007 thực sự là một năm bất ổn và được coi là năm "báo động đỏ". Hàng nghìn virus mới xuất hiện, những cuộc tấn công có chủ đích của giới hacker vào các website của các cơ quan, tổ chức và doanh nghiệp ... đã gây ra những hậu quả nhất định cho các đơn vị này. Nhiều hoạt động phạm pháp, lợi dụng Internet làm môi trường hoạt động, tình trạng phát tán thư rác, virus ... tăng theo cấp số nhân.

1.5. Khái quát về các giải pháp công nghệ bảo mật an toàn thông tin và an ninh mạng

Vấn đề bảo mật an toàn thông tin và an ninh mạng luôn là bài toán khó thách thức các quốc gia trên phạm vi toàn cầu. Hiện có nhiều giải pháp, nhiều sản phẩm công nghệ đã được nghiên cứu và ứng dụng, tuy nhiên vấn này vẫn luôn là vấn đề thời sự và thách thức. Trong phần dưới đây sẽ điểm qua các giải pháp công nghệ về lĩnh vực này trên cơ sở đó các chương sau sẽ tập trung trình bày giải pháp nghiên cứu của đề tài, được đặt trong bức tranh toàn cảnh chung của các giải pháp công nghệ.

1.5.1. Các công nghệ mật mã

Công nghệ mật mã là nền tảng của tất cả các công nghệ bảo vệ thông tin. Công nghệ này cung cấp 5 dịch vụ cơ bản: đảm bảo bí mật, toàn vẹn dữ liệu, chứng thực thông điệp, chứng thực người dùng và chống chối bỏ. Đối với mật mã khoá đối xứng, việc nghiên cứu được thực hiện trong lĩnh vực công nghệ ứng dụng mật mã khối. Mật mã khoá công khai, RSA và ECC đều được phát triển đồng thời. Tuy nhiên rất nhiều nghiên cứu của RSA và ECC được thực hiện nhằm giải quyết những yếu tố sai sót để tăng năng suất tính toán. Đặc biệt, một số nghiên cứu như: thuật toán modular, thuật toán trường hữu hạn, và thuật toán đường cong elíp đã được thực hiện. Ngoài ra, các nghiên cứu cũng được thực hiện một cách đồng bộ về mặt giao thức thiết lập khoá, chương trình ứng dụng mật mã, và công nghệ phân tích độ bền vững trong lĩnh vực khoá đối xứng.

1.5.2. Các công nghệ chứng thực

Các công nghệ chứng thực được chia thành 2 nhóm là công nghệ hạ tầng khóa công khai PKI (Public Key Infratruction) và công nghệ PMI. Công nghệ PKI dựa trên nền tảng hệ mật mã khóa công khai cùng với các chính sách, các kiến trúc hệ thống và cơ chế sử dụng các khoá công khai và tính toàn vẹn của chứng chỉ số tạo thành cơ sở hạ tầng an toàn cho các giao dịch điên tử trên mạng. Hiện nay hạ tầng PKI đã và đang được ứng dụng rộng rãi trên thế giới. Các công nghệ hệ thống PKI dựa trên hệ mã khoá công khai cũng đang được phát triển cùng với các sản phẩm được liên kết với lĩnh vực dịch vụ ứng dụng nhằm tăng cường chức năng VA (Validation Authority), chức năng khôi phục khoá, tăng cường sử dụng thẻ thông minh và chấp nhận các dịch vụ bảo mật, chấp nhận phương thức mật mã đường cong elip trong thuật toán chữ ký số, tích hợp công nghệ không dây vào các sản phẩm chứng

thực, xây dựng hệ thống PKI toàn cầu. Bên cạnh công nghệ PKI, công nghệ PMI được dùng trong việc quản lý các quyền của người sử dụng. PMI có thể được phân thành 2 loại: EAM (Extranet Access Management) và 3A (Authentication/ Authorization/ Administration).

1.5.3. Công nghệ sinh trắc học

Sinh trắc học là độ đo các đặc điểm về hành vi (chữ ký, dáng đi, thói quen gõ phím…) hoặc các thuộc tính vật lý mang tính duy nhất của cơ thế con người (vân tay, giọng nói, khuôn mặt, mống mắt, ADN...). Công nghệ sinh trắc học được dùng để đo các đặc điểm vật lý và đặc điểm hành vi của con người bằng các thiết bị tự động và sử dụng công cụ đo lường để xác định các cá nhân, phản chiếu thông tin nhận được từ một phần của cơ thể hoặc từ các đặc điểm hành vi cá nhân. Công nghệ này có một lợi thế là không có rủi ro khi cho thuê (nhượng) mật khẩu hoặc thẻ ID cho người khác, hoặc làm mất, chiếm đoạt hay sao chép chúng. Về mặt công nghệ hiện tại, mặt (face), vân tay và mống mắt (iris) đã được đưa vào sử dụng, một số công nghệ sinh trắc khác như: gân (vein) mu bàn tay, DNA, dáng điệu (gait), chiều cao, keystroke và mẫu tai (ear pattern) cũng đang được thúc đẩy phát triển. Hướng hiện nay là kết hợp công nghệ đa sinh trắc (multi biometrics) với các công nghệ đơn sinh trắc (single biometrics) và việc kết hợp công nghệ vào thẻ thông minh cũng đang được phát triển. Các vấn đề về tiêu chuẩn hoá quá trình xử lý, vận chuyển, và lưu trữ thông tin sinh trắc học vẫn đang được thảo luận.

Hướng nghiên cứu tích hợp phương pháp thẩm định xác thực sinh trắc học vào hạ tầng khóa công khai PKI tạo thành hệ BioPKI cho phép xác thực, thẩm định người dùng khi sử dụng khoá bí mật trong hoạt động của hệ thống PKI. Đây là một trong các giải pháp đang được quan tâm nghiên cứu nhằm đảm bảo sự ảnh hưởng lẫn nhau thông qua các tiêu chuẩn, tự động khoá và chứng thực người quản lý hợp lệ, dễ dàng áp dụng các chức năng quan trọng của chứng chỉ trong các hệ thống.

1.5.4. Công nghệ bảo vệ hệ thống và mạng

Công nghệ bảo vệ hệ thống và mạng được dùng để bảo vệ máy tính và thông tin của các tổ chức hoặc cá nhân nhằm chống lại các hành động trái phép như: giả mạo, thay thế, tiết lộ, xâm nhập vào những thông tin được truyền đi qua mạng truyền thông như internet. Các lĩnh vực chính của công nghệ này là bảo mật máy tính và máy chủ, firewall, phát hiện xâm nhập, phát hiện và quản lý xâm nhập. Việc phát triển công nghệ này bao gồm phát hiện vi rút, các tệp dữ liệu cá nhân, PC firewall, kiểm soát truy nhập dịch vụ, kiểm soát truy nhập server, công nghệ mật mã, bảo mật hệ điều hành, các công cụ phân tích nhược điểm, server firewall và tích hợp các giải pháp bảo mật. Công nghệ bảo mật máy tính là một vấn đề nóng bỏng và được quan tâm một cách đặc biệt. Công nghệ bảo mật server cũng đang được phát triển nhằm bù đắp những thiếu sót của SSH, ổn định bảo mật DHMS và cải tiến nhược điểm đối phó với xâm nhập. Trong lĩnh vực công nghệ chống xâm nhập, IDWG (Intrusion Detection Exchange Format) và INCH của IETF phát triển các tiêu chuẩn trao đổi thông tin trong việc phát hiện xâm nhập và các công cụ tính toán rủi ro; bên cạnh đó còn phát triển tiêu chuẩn bảo mật của SHSLOG.

1.5.5. Công nghệ bảo vệ mạng

Công nghệ bảo vệ mạng là công nghệ cải tiến tính ổn định của hệ thống mạng nhằm chống lại các hành động trái phép như: giả mạo, thay thế, tiết lộ, xâm nhập vào những thông tin được truyền đi qua môi trường mạng như internet. Các lĩnh vực công nghệ chính là: công nghệ bảo mật IP (IPSec) - là kiến trúc bảo mật của tầng mạng; bảo mật tầng truyền dữ liệu (TLS security) - là kiến trúc bảo mật cho tầng truyền dữ liệu Multicast, kiến trúc bảo mật cho các dịch vụ không dây, kiến trúc cho công nghệ phát hiện và ngăn chặn xâm nhập, kiến trúc quản lý bảo mật kết hợp, và kiến trúc bảo mật mạng thế hệ mới (next-generation network). Thông thường, giao thức HTTPS (HTTP/TLS) được sử dụng để đảm bảo an toàn cho các dịch vụ web thông qua các công nghệ trên. Các trình duyệt web cũng hỗ trợ SSL v2.0, SSL v3.0 và TLS v1.0 và gần đây là truyền ID và mật khẩu được mã hoá. Cũng như các công nghệ ứng dụng khác, OpenSSL, Plannet SSL và PowerTCP SSL thường sẵn sàng cung cấp đường truyền mã hoá qua Internet và Intranet, SecureNetterm hỗ trợ TLS và ws-ftp (cung cấp các dịch vụ ftp an toàn). Giao thức bảo mật IPSec - là công nghệ cốt lõi trong việc xây dựng VPN - được vận hành ở cả 2 phương thức: transport mode và tunnel mode. Tuy nhiên, tunnel mode chủ yếu được dùng để duy trì tính bí mật của các luồng truyền gói dữ liệu.

1.6. Xác định nhiệm vụ của đề tài

Hệ thống an ninh thông tin (Bio-PKI Based Information Security System) kết hợp các dấu hiệu đặc trưng sinh trắc học vân tay con người vào mã bảo mật với khóa công khai PKI, là hướng nghiên cứu mới cho phép mang lại những ưu điểm hơn các hệ thống mã khóa công khai hiện có về độ an toàn bảo mật, về tính xác thực thẩm định trong các giao dịch, các dịch vụ điện tử qua mạng máy tính.

Mục tiêu của nhiệm vụ hợp tác với Malaysia theo nghị định thư chủ yếu bao gồm:

- Nghiên cứu đề xuất phương án kết hợp các đặc trưng của vân tay với mã bảo mật khóa công PKI tạo mã sinh trắc học Bio-PKI.

- Xây dựng thử nghiệm hạ tầng cơ sở hệ thống an ninh thông tin Bio-PKI (protoptype). Thiết kế và xây dựng thử nghiệm phần mềm hệ thống an ninh thông tin dựa trên mã sinh trắc học Bio-PKI nhằm hướng tới ứng dụng trong công tác xác thực, thẩm định sinh trắc học và kiểm soát truy cập dùng trong các lĩnh vực an ninh, thương mại điện tử, ngân hàng, giao dịch điện tử, chính phủ điện tử.

Kết quả nghiên cứu phối hợp của 2 phía Việt Nam và Malaysia để thử nghiệm phát triển ứng dụng hệ thống Bio-PKI.

Chương 2.
SINH TRẮC HỌC VÀ HỆ THỐNG AN NINH BẢO MẬT THÔNG TIN DỰA TRÊN SINH TRẮC HỌC

2.1. Tổng quan về sinh trắc học

Thuật ngữ sinh trắc học (Biometric) được dùng ghép theo tiếng Hy Lạp từ 2 từ: Bio (thuộc về thực thể sinh vật sống) và metriko (kỹ thuật độ đo, đo lường), thuật ngữ này đã được hình thành trong quá trình phát triển loài người và được biết đến từ lâu để thể hiện các đặc trưng về thể chất hay về hành vi của từng cá thể con người. Có nhiều loại đặc trưng sinh trắc học: vân tay (Fingerprint), lòng bàn tay (Palm print), dạng hình học bàn tay (Hand geometry), chữ ký viết tay (Hand written Signature), khuôn mặt (Face), tiếng nói (Voice), con ngươi mắt (Iris), võng mạc (Retina), ADN… Những đặc trưng này đã được phát hiện từ rất sớm để nhận dạng, xác thực chủ thể con người và hiện nay đang được quan tâm nghiên cứu triển ứng dụng trong các lĩnh vực an ninh, quốc phòng, thương mại. Như vậy sinh trắc học được coi là độ đo các đặc điểm về hành vi (chữ ký, dáng đi, thói quen) hoặc các thuộc tính vật lý mang tính duy nhất của cơ thế con người cho phép nhận diện cá thể con người. Các đặc trưng sinh trắc học của cơ thể người được sử dụng phải đảm bảo các tiêu chuẩn sau đây:

- Tính rộng rãi: cho biết mọi người thông thường đều có đặc trưng này, tạo khả năng sử dụng hệ thống an ninh sinh trắc học cho một số lượng lớn người.
- Tính phân biệt: đặc trưng sinh trắc học giữa hai người bất kỳ phải khác nhau, đảm bảo sự duy nhất của chủ thể.
- Tính ổn định: đặc trưng phải có tính ổn định trong một thời gian tương đối dài.
- Tính dễ thu thập: để khả thi trong sử dụng, đặc trưng sinh trắc học phải dễ dàng thu nhận mẫu khi đăng ký, kiểm tra xác thực.
- Tính hiệu quả: việc xác thực sinh trắc phải chính xác, nhanh chóng và tài nguyên cần sử dụng chấp nhận được.
- Tính chấp nhận được: quá trình thu thập mẫu sinh trắc phải được sự đồng ý của người người dùng.
- Chống giả mạo: khả năng mẫu sinh trắc khó bị giả mạo…

Có nhiều đặc trưng sinh học khác nhau được sử dụng. Mỗi loại có điểm mạnh và điểm yếu riêng. Tuy nhiên không một đặc trưng nào thỏa mãn tốt đầy đủ tất cả các yêu cầu của một đặc trưng sinh trắc học nêu trên, nghĩa là không có một đặc trưng sinh trắc học hoàn toàn tối ưu [6]. Trong công trình nghiên cứu [9] một bảng dưới đây đã so sánh khái quát các tiêu chuẩn đánh giá tương ứng các đặc trưng sinh trắc học:

Đặc trưng sinh trắc học	Tính rộng rãi	Tính phân biệt	Tính ổn định	Tính dễ thu thập	Tính hiệu quả	Tính chấp nhận được	Chống giả mạo
Vân bàn tay	M	M	M	M	M	M	L
Dạng hình học bàn tay	M	M	M	H	M	M	M
Vân tay	M	H	H	M	H	M	M
Dáng đi	M	L	L	H	L	H	M
Khuôn mặt	H	L	M	H	L	H	H
Nhiệt Khuôn mặt	H	H	L	H	M	H	L
Thói quen gõ phím	L	L	L	M	L	M	M
Mùi	H	H	H	L	L	M	L
Tai	M	M	H	M	M	H	M
Võng mạc	H	H	M	L	H	L	L
Mống mắt	H	H	H	M	H	L	L
Chỉ tay	M	H	H	M	H	M	M
Giọng nói	M	L	L	M	L	H	H
Chữ ký	L	L	L	H	L	H	H
ADN	H	H	H	L	H	L	L

Bảng 2.1: So sánh các công nghệ nhận dạng sinh trắc học

Chú ý: các ký hiệu có ý nghĩa như sau: H (cao), M (trung bình) và L (thấp).

2.2. Hệ thống sinh trắc học

2.2.1. Khái quát về hệ thống sinh trắc học

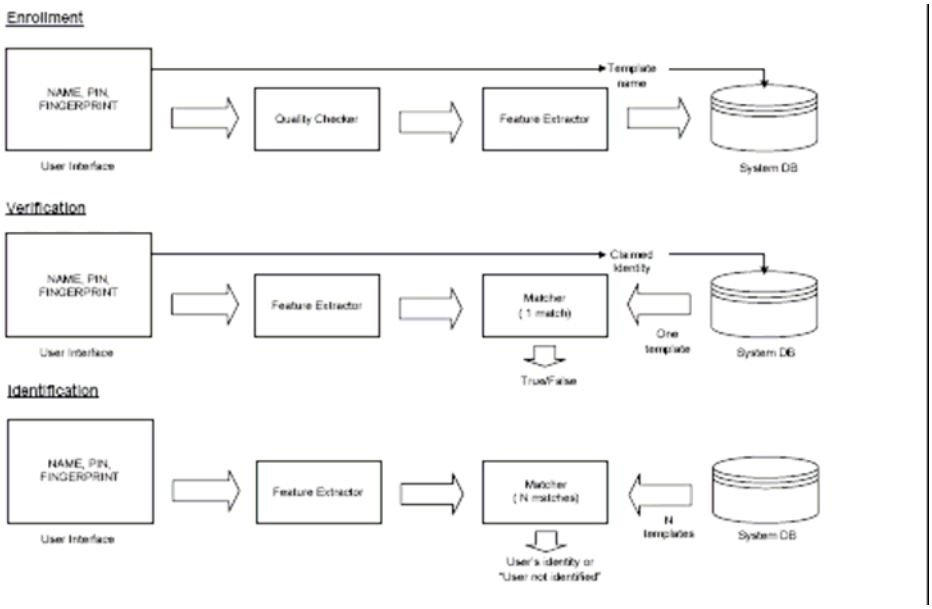
Hệ thống sinh trắc học (Biometric System) thực chất là một hệ nhận dạng dựa trên các đặc điểm về hành vi hay thuộc tính vật lý của người cần nhận dạng [9]. Hệ thống sinh trắc học được phân ra thành hai loại chính [13]:

- Hệ thẩm định (Verification): Hệ thống thực hiện đối sánh 1-1 giữa mẫu sinh trắc học thu nhận được (Biometric sample) với mẫu dạng sinh trắc học (biometric template) đã có trong hệ thống từ trước. Kết quả trả lời câu hỏi mẫu sinh trắc thu nhận có liên quan tới mẫu dạng sinh trắc hay không, thông thường trong hệ thẩm định kết hợp với thông tin định danh chủ thể thực hiện chức năng xác thực thẩm định sinh trắc (Authentication). Trong hệ xác thực thẩm định đòi hỏi cao về độ chính xác để kết quả trả lời câu hỏi "sinh trắc học sống thu nhận được (biometric sample) có phải là sinh trắc của chủ thể đã lưu trong hệ thống không?"
- Nhận dạng (Identification, Recognition): Hệ thống thực hiện chức năng tìm kiếm (1-n) từ một cơ sở dữ liệu đề tìm một mẫu sinh trắc cụ thể trong các mẫu khuôn dạng sinh trắc thu thập từ trước và sau đó thực hiện đối sánh xấp xỉ để nhận dạng phân lớp (Classification) hoặc nhận dạng đồng nhất (Identification), ví dụ như việc tìm mẫu vân tay tội phạm trong hồ sơ các vân tay, từ đó xác định danh tính của chủ sở hữu vân tay.

- Sơ đồ khối chức năng của 2 loại hệ thống sinh trắc được minh họa trong Hình 2.1. Các thành phần chức năng chủ yếu của hệ thống sinh trắc học [13]:
  - Thu nhận (Sensor, Capture): thu nhập mẫu sinh trắc học và biểu diễn dưới dạng số hóa.
  - Xử lý và trích chọn đặc trưng (Feature Extraction): Thực hiện các phép xử lý phân tích và trích chọn các đặc trưng từ mẫu sinh trắc học.

- Đối sánh (Matching): thực hiện so sánh các đặc trưng vừa trích chọn với khuôn mẫu sinh trắc đã có trước.
- Ra quyết định (Decision): dựa trên kết quả đối sánh sẽ khẳng định danh tính người dùng (với hệ nhận dạng) hoặc là một câu trả lời đúng hoặc sai về mẫu sinh trắc học so với khuôn mẫu sinh trăc có từ trước (với hệ thẩm định).

- Hoạt động của hệ thống sinh trắc bao gồm 2 giai đoạn cơ bản:
  - Đăng ký (Enrollment): Đăng ký mẫu sinh trắc vào hệ thống
  - Thẩm định hoặc nhận dạng (Verification/ Identification)



Hình 2.1. Sơ đồ khối chức năng của 2 loại hệ thống sinh trắc.

2.2.2. Các đặc điểm của hệ thống sinh trắc học

a/ Các vấn đề về thu nhận và biểu diễn mẫu sinh trắc như sau:

Xác thực bằng mật khẩu truyền thống dùng Password không cần sử dụng các phương pháp nhận dạng mẫu phức tạp, mà chỉ cần đối sánh trực tiếp mật khẩu. Cơ chế này cho phép xây dựng hệ xác thức mật khẩu đảm bảo tính chính xác, ổn định, hiệu quả đúng như thiết kế. Tuy nhiên vấn đề không an toàn và điểm yếu nhất của hệ thống là thông thường mật khẩu chỉ gồm 6-8 ký tự, mật khẩu này dễ dàng bị đánh cắp, bị quên hay bị mạo danh, khi xảy ra mất an toàn mật khẩu, toàn bộ hệ thống an toàn của hệ thống sẽ sụp đổ. Đối với sinh trắc học, mẫu sinh trắc có tính bền vững cao, khó giả mạo dịnh danh và chp phép đảm bảo an toàn cho hệ thông. Mặt khác khi thu nhận các mẫu sinh trắc sống và xử lý biểu diễn trích chọn đặc trưng, các kết quả này phụ thuộc rất nhiều vào yếu tố như phương pháp lấy mẫu, môi trường lấy mẫu, trạng thái tương tác của người lấy mẫu với thiết bị và tùy theo loại sinh trắc thu nhận [7,10].

- Thu nhận mẫu sinh trắc không ổn định

Như đã nói, tín hiệu sinh trắc học thu nhận được phụ thuộc vào đặc trưng sinh lý, hành vi tương tác của người dùng… Ví dụ như với thu nhận mẫu vân tay từ máy quét (trường hợp thu nhận mẫu được coi là lý tưởng nhất), sự khác nhau về lực ấn của ngón tay lên thiết bị quét, vị trí ấn ngón tay lên mặt phẳng quét đều ảnh hưởng tới kết quả thu nhận ảnh vân tay. Vì các ngón tay không phải là đối tượng cố định và quá trình chiếu bề mặt đầu ngón tay lên mặt phẳng quét không tuyệt đối chính xác, nên với lực ấn khác nhau, các phần khác nhau của vân tay sẽ được quét như ví dụ ở hình dưới đây:

Hình 2.2. Thu nhận mẫu sinh trắc không ổn định

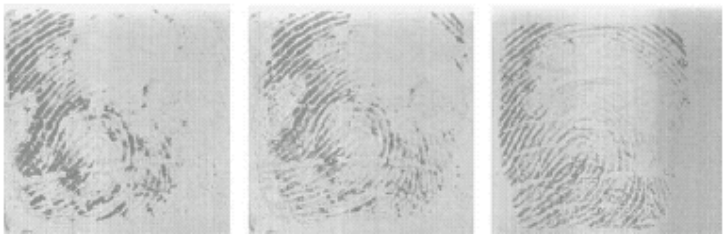
Đối với nhận dạng khuôn mặt, do góc chụp hình khuôn mặt không thể tuyệt đối giống nhau ở mọi lần lấy mẫu, nên kết quả lấy mẫu phụ thuộc vào vị trí chụp hình khuôn mặt. Vì thế các mẫu thu được đều có sự khác với nhau.

- Thay đổi của đặc trưng sinh trắc

Ngoài việc khó khăn về quá trình thu nhận, đặc sinh trắc học còn bị ảnh hưởng bởi ngoại cảnh bên ngoài. Với vân tay, các hoạt động làm việc, tai nạn lao động… đều tác động tới chất lượng hình ảnh trên đầu ngón tay. Kết quả thu nhận còn thay đổi khi người dùng có đeo đồ trang sức, ví dụ như nhẫn khi nhận dạng hình dáng bàn tay. Nhận dạng khuôn mặt có thể gặp khó khăn sau một khoảng thời gian vì độ dài và kiểu tóc, râu người dùng thay đổi, hoặc bị tai nạn ảnh hưởng tới khuôn mặt… Tất cả các tác động ngoại cảnh đều thay đổi lớn tới kết quả thu nhận mẫu.

- Tác động của môi trường

Các tác động của môi trường tại thời điểm thu nhận cũng ảnh hưởng tới kết quả mẫu sinh trắc. Ví dụ như độ ẩm, độ sạch của da, ảnh hưởng của tuổi tác, bệnh tật về da… ảnh hưởng tới mẫu vân tay (Hình 2-3).



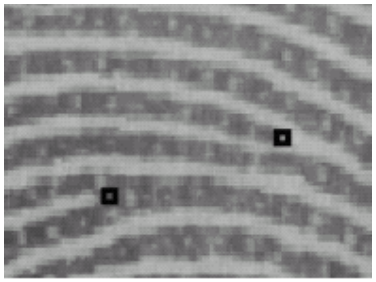
Hình 2.3. Ảnh hưởng của môi trường lên mẫu vân tay

Ngoài ra, các thuật toán phân tách đặc trưng sinh trắc học từ mẫu thu nhận cũng không hoàn hảo và có một độ lỗi nhất định. Kết quả là để đối sánh hai mẫu sinh trắc học có giống nhau hay không là quá trình nhận dạng mẫu và ra quyết định khá phức tạp

b/ Đối sánh sinh trắc học

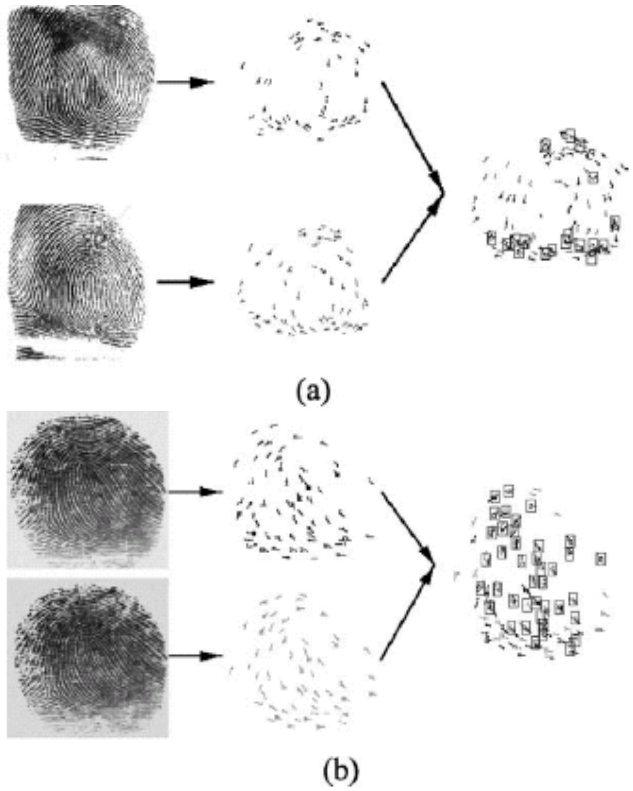
Do các nguyên nhân ảnh hưởng nêu trên, đối sánh sinh trắc học không thể thực hiện một cách tuyệt đối như với mật khẩu truyền thống. Thông thường, đối sánh sinh trắc học thường dùng cách đối sánh tương đối giữa hai mẫu, sự giống nhau của từng thành phần nhỏ được đánh giá bằng cho điểm (matching score). Khi số điểm đối sánh đủ lớn vượt ngưỡng định trước, có thể coi là hai mẫu sinh trắc gần tương tự nhau.

Ví dụ với nhận dạng vân tay, các thành phần nhỏ được so sánh là điểm kết thúc (ridge ending) và điểm rẽ nhánh (ridge bifurcation), gọi chung là điểm đặc trưng cục bộ (minutiae). Các điểm này được tách ra bằng thuật toán trích chọn đặc trưng vân tay. Các điểm đặc trưng cục bộ được định vị bằng ba tham số (x, y, θ) với (x, y) biểu diễn tọa độ tương đối của điểm và θ biểu diễn hướng của đỉnh tại điểm đó. Thông thường, một mẫu vân tay tốt có từ 20-70 điểm đặc trưng cục bộ.



Hình 2.4. Điểm đặc trưng cục bộ của vân tay

Quá trình đối sánh với một mẫu vân tay khác thực hiện bằng cách so sánh vị trí tương đối giữa các điểm đặc trưng cục bộ với nhau qua thuật toán đối sánh. Kết quả thuật toán trả về là tỷ số điểm đối sánh được chập nhận (matching score):



Hình 2.5. Đối sánh vân tay.

Kết quả minh họa trong hình 2-5(a), hai vân tay khác nhau cho ra điểm đối sánh là 4, trong hình 2-5(b), hai vân tay giống nhau cho ra điểm đối sánh là 49. Giá trị tối đa của điểm đối sánh là 100.

2.3. Đánh giá hiệu năng và chất lượng hoạt động của hệ sinh trắc học

2.3.1. Vấn đề lỗi trong hoạt động của hệ sinh trắc

Khi hoạt động một hệ sinh trắc học thường gặp hai vấn đề về lỗi sau đây:

- Lỗi khi đối sánh mẫu sinh trắc của hai người khác nhau nhưng cho kết quả là của cùng một người. Lỗi này được gọi là loại bỏ sai (false reject hay false match).
- Lỗi khi đối sánh hai mẫu sinh trắc của cùng một người nhưng cho kết quả sai, vì cho rằng là của hai người khác nhau. Lỗi này được gọi là chấp nhận sai (false accept hay false nonmatch).

2.3.2. Các tham số đánh giá chất lượng.

Để đo lường mức độ lỗi của hệ thông, các độ đo thường dùng được định nghĩa như sau

- FMR *(False Match Rate*): còn gọi là FAR (*False Accept Ratio*)- Tỷ số chấp nhận sai : cho biết tỉ lệ trả lời là đúng đối với dữ liệu vào là sai
- FNMR *(False Nonmatch Rate*): còn gọi là FRR (*False Rejection Ratio*) - Tỷ số từ chối sai: cho biết tỉ lệ trả lời là sai đối với dữ liệu vào là đúng.

Hai độ đo này có ràng buộc với nhau: nếu FMR cao thì FNMR sẽ giảm tương đối và ngược lại. Mức độ chấp nhận được của FMR và FNMR tùy thuộc vào từng hệ xác thực sinh trắc cụ thể. Với hệ yêu cầu tính bảo mật cao, và đặt nặng vấn đề an toàn của xác thực hơn sự tiện dụng của người dùng, thì FMR sẽ nhỏ và FNMR sẽ cao. Ngoài hai độ đo trên, người ta còn sử dụng độ đo FTC (*Failure To Capture* - thu nhận mẫu thất bại) và FTE (*Failure to Enroll* - chấp nhận mẫu thất bại) để đánh giá hiệu năng của hệ xác thực sinh trắc học.

2.4. Hệ thống an ninh bảo mật dựa trên trắc học

Hệ sinh trắc học có những ưu điểm mà hệ bảo mật thông thường không có, nghiên cứu hệ thống an ninh, bảo mật sinh dựa trên sinh trắc học (Biometric Security System) đã được quan tâm nghiên cứu và ứng dụng. Hướng nghiên xây dựng hệ thống trên cơ sở kết hợp hệ thống sinh trắc học với hệ mật mã (Biometric Cryptosystem) đang là vấn đề thời sự được quan tâm nghiên cứu phát triển. Sự kết hợp này nhằm mục tiêu nâng cao tính an toàn của hệ mật mã dựa trên các ưu điểm của hệ thống sinh trắc học. Hệ thống an ninh, bảo mật sinh trắc học (Biometric based Security System) dựa trên sự nhận biết hoặc thẩm định các đặc trưng về thể chất hay về hành vi con người để nhận dạng, xác thực từng chủ thể [1,3,7,8]. Cùng với sự phát triển nhanh chóng của CNTT và truyền thông, hệ thống an ninh dựa trên nhận dạng, thẩm định xác thực sinh trắc học đã và đang được quan tâm nghiên cứu và có nhiều triển khai ứng dụng trong những năm gần đây trên thế giới. Đối với các giao dịch điện tử và truyền thông, đây là một trong các hướng tiếp cận mới về an ninh thông tin và mạng, an toàn dữ liệu. Phương pháp này mở ra triển vọng lớn về an toàn trong các giao dịch điển tử, chính phủ điển tử, thương mại điện tử…

- Các lĩnh vực nghiên cứu về hệ thống an ninh sinh trắc học (Biometric Security Systems)
  - Các các nghiên cứu cơ bản về các loại sinh trắc học, về phương pháp trích chọn đặc trưng sinh trắc và về nhận dạng, thẩm định xác thực chủ thể con người.
  - Các hệ nhận dạng, thẩm định xác thực sinh trắc học chủ thể trong hệ thống
  - Hệ thống an ninh sinh trắc học trên cơ sở hạ tầng khóa công khai PKI (gọi là hệ thống BioPKI)
  - Mật mã sinh trắc học (Biometric Cryptography)

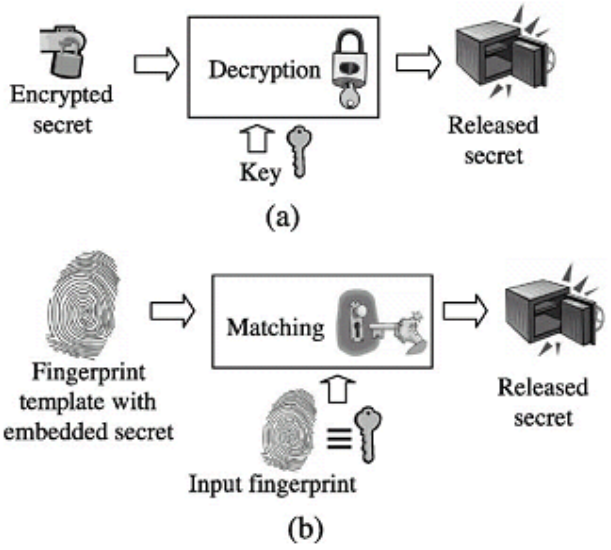
Trong hệ mật mã thông thường, điểm yếu thường ở quá trình bảo vệ, quản lý và phân phối khóa. Nguy cơ này đe dọa các mục tiêu về xác thực và chống phủ nhận. Hệ sinh trắc học được ứng dụng giải quyết vấn đề đó. Hiện nay có hai hướng tiếp cận để kết hợp sinh trắc học và mật mã học như sau [9]:

- Dùng sinh trắc học quản lý khóa (biometric-based key release)
- Dùng sinh trắc học để tạo khóa (biometric-based key generation).

2.4.1. Dùng sinh trắc học quản lý và bảo vệ khóa

Nguyên tắc của phương pháp này là quá trình đối sánh sinh trắc học tách riêng với quá trình mã hóa của mật mã học. Đối sánh thực hiện theo kịch bản: nếu mẫu sinh trắc đối sánh

chấp nhận được so với mẫu khuôn dạng sinh trắc đã lưu trữ, hệ sẽ giải phóng khóa mã từ nơi lưu trữ an toàn, như smart-card hay cơ sở dữ liệu trên máy chủ.



Hình 2.6. Hai mô hình bảo vệ khóa trong hệ bảo mật

Hình 2.6 minh họa hai mô hình bảo vệ khóa trong hệ bảo mật: mô hình thứ nhất (hình a) sử dụng mật khẩu truyền thống để bảo vệ khóa mã, đây là mô hình bảo vệ khóa truyền thống và thông dụng; mô hình thứ hai (hình b) dùng vân tay để bảo vệ khóa mã, đây là dạng kết hợp sinh trắc học với mật mã học.

Đặc điểm của hướng tiếp cận này như sau:

- Cần phải truy cập tới mẫu khuôn dạng sinh trắc học để thực hiện đối sánh mẫu.
- Quá trình xác thực người dùng và quá trình giải phóng khóa khỏi nơi lưu trữ hoàn toàn tách rời nhau (offline).
- Quá trình thẩm định xác thực chủ thể không liên quan trực tiếp các giao dịch trên mạng

Hướng giải pháp

- Giải pháp dùng sinh trắc tại các thiết bị đầu cuối (End-User dùng công nghệ nhúng). Thường là giải pháp theo các dòng thiết bị theo công nghệ nhúng.
- Kỹ thuật chủ yếu: KT nhận dạng, đối sánh thẩm định sinh trắc học từ CSDL lưu trữ tại thiết bị nhúng, đạt độ chính xác cao.
- Ứng dụng: Thường dùng các giải pháp khóa sinh trắc tại thiết bị đầu cuối, chất lượng phụ thuộc vào dòng thiết bị.

Một số vấn đề an toàn với mô hình tiếp cận trên:

- Khả năng mẫu khuôn dạng sinh trắc học bị mất hay sử dụng lại: Mẫu khuôn dạng sinh trắc học được dùng khi xác thực, vì thế đặt ra vấn đề về an toàn lưu trữ mẫu định dạng. Cách giải quyết có thể là chuyển đổi mẫu khuôn dạng sinh trắc sang một miền biểu diễn khác: H(X) với X là mẫu khuôn dạng sinh trắc và H là hàm chuyển đổi một chiều không thể đảo ngược, đặc trưng cho từng hệ mật khác nhau. Nhưng cách giải quyết này sinh ra khó khăn khi thực hiện đối sánh sinh trắc trên miền không gian xử lý khác.

• Chống sử dụng lại mẫu sinh trắc học: Một mẫu sinh trắc học thu nhận được ở hệ mật này có thể bị sử dụng lại tại một hệ mật khác. Để tránh nguy cơ trên, có thể thiết kế sao cho mẫu sinh trắc học chỉ được dùng cho riêng biệt từng hệ mật khác nhau. Điều này thực hiện khi cho thêm một vài thành phần dữ liệu bổ sung vào mẫu định dạng, tương tự như trong hệ xác thực mật mã truyền thống. Thành phần bổ sung này gọi là salt, có tính chất đặc thù cho từng hệ mật.

• Tách rời giữa xác thực và giải phóng khóa: Do hai quá trình tách rời nhau, nên kết quả của xác thực có nguy cơ bị tấn công sửa đổi từ "sai" thành "đúng" khi truyền tải kết quả, dẫn tới phá vỡ an toàn xác thực của hệ thống.

2.4.2. Dùng sinh trắc học để sinh khóa

Nghiên cứu kết hợp kỹ thuật sinh trắc với kỹ thuật mật mã, mật mã sinh trắc (Biometric Encryption) nhằm nghiên cứu "tạo" ra khóa mã từ mẫu khuôn dạng và mẫu sinh trắc trong hệ thống. Hướng tiếp cận "Biometric Cryptosystem" cho phép kết hợp chặt chẽ sinh trắc học với mật mã học nhằm khắc phục các điểm yếu của phương pháp bảo vệ khóa và cho phép thực hiện quá trình thẩm định xác thực chủ thể tích hợp trực tiếp vào trong các giao dịch trên mạng. Đây là hướng nghiên cứu chủ yếu hiện nay.

Tuy nhiên phương pháp tạo khóa từ mẫu sinh trắc học gặp phải các khó khăn chính sau [7,9]:

- Khó khăn khi cần phải sinh ra chuỗi bit chính xác từ các mẫu sinh trắc thu nhận. Các mẫu sinh trắc học thu nhận được từ quá trình không ổn định, chịu nhiều tác động của những yếu tố ngẫu nhiên khác nhau. Về nguyên tắc không thể thu được các chuỗi bít đồng nhất tuyệt đối từ các mẫu sinh trắc sống của cùng một chủ thể. Do vậy chuỗi bit đặc trưng sinh trắc thường không đủ độ chính xác để dùng làm khóa. Đây là khó khăn chủ yếu của phương pháp này.

- Vấn đề sử dụng mẫu sinh trắc học với nhiều hệ: Do khả năng chỉ sinh được một khóa từ một loại mẫu sinh trắc học, điều này ảnh hưởng tới độ an toàn của các hệ mật còn lại khi một hệ mật bị tấn công. Giải pháp của vấn đề này là thêm một phần dữ liệu đặc trưng có vai trò làm tham số cho khóa sinh ra, nhằm tăng độ đa dạng của khóa đối với từng hệ mật.

- Tính toán phức tạp. Các giải thuật tính toán hiện nay để sinh ra khóa từ mẫu sinh trắc yêu cầu lượng tính toán lớn.

Những vấn đề khó nêu trên là mục tiêu định hướng nghiên cứu của đề tài. Trong chương này đã trình bày tổng quan về hệ thống sinh trắc học và hệ thống an ninh bảo mật dựa trên sinh trắc học: khái niệm, các thành phần, hoạt động; các yêu cầu đối với hệ thống. Trong các chương tiếp sau sẽ trình bày nghiên cứu về giải pháp kết hợp hệ bảo mật sinh trắc học vào hạ tầng cơ sở khóa công khai PKI. Chương 4 tiếp theo sẽ tập trung trình bày hạ tầng PKI, hạ tầng cơ sơ cho các giao dịch điện tử hiện nay và các vấn đề an toàn trong hệ PKI.

Chương 3.
CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI PKI VÀ VẤN ĐỀ AN TOÀN TRONG HỆ THỐNG

3.1. Hệ mật mã khóa công khai

Mật mã là một công cụ bao gồm các nguyên tắc, phương tiện và phương thức chuyển đổi dữ liệu nhằm ấn dấu nội dung thông tin, củng cố tính xác thực của thông tin, ngăn chặn sự thay đổi, tính từ chối, và việc sử dụng trái phép thông tin. Đây là một trong các phương tiện mang tính công nghệ được dùng để đảm bảo an toàn cho dữ liệu của các hệ thống thông tin và truyền thông. Mật mã cũng có thể được dùng để bảo vệ tính bí mật của những dữ liệu như tài chính hoặc cá nhân kể cả khi dữ liệu được lưu trữ hay vận chuyển. Ngoài ra, nó cũng có thể dùng để kiểm tra tính toàn vẹn của dữ liệu bằng việc phát hiện dữ liệu đã bị thay thế hay chưa và xác định người hoặc thiết bị đã gửi nó. Những kỹ thuật này là rất quan trọng đối với việc phát triển và sử dụng các mạng thông tin truyền thông toàn cầu và những công nghệ khác, như phát triển thương mại điện tử.

Mật mã bao gồm hai quy trình hoạt động trái ngược nhau: mã hoá và giải mã. Đứng trên góc độ sử dụng máy tính trong việc bảo mật thông tin, mã hoá là quá trình áp dụng một thuật toán vào một bản tin rõ để sinh ra một bản tin mã. Bản tin mã sẽ xuất hiện như là những thứ vô nghĩa đối với mọi người vô tình có được nó, nhưng có thể biến đổi ngược lại thành bản tin rõ đối với những người có được thuật toán phù hợp. Quá trình biến đổi bản tin mã thành bản tin rõ gọi là quá trình giải mã .

Quá trình mã hoá thường được điều khiển bởi một “khoá”, thực chất là một chuỗi các bít số dùng để làm các tham số cho thuật toán mã hoá. Quá trình giải mã cũng được điều khiển bởi một “khoá” để làm tham số cho thuật toán giải mã, và có thể là giống hoặc khác với khoá đã dùng để mã hoá [2].

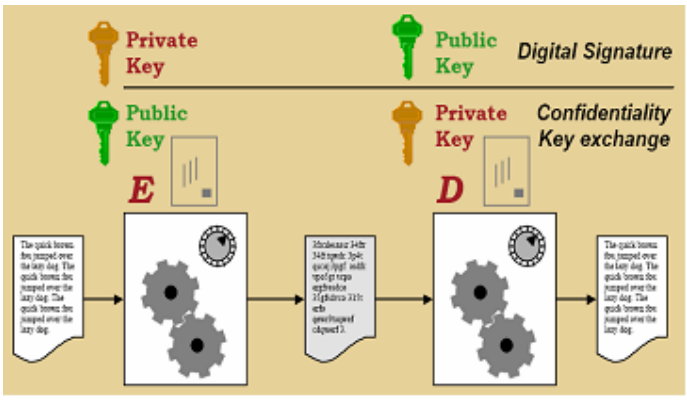
Hiện nay, trên thế giới thường sử dụng 2 hệ mật cơ bản là Mật mã khoá bí mật (Secret Key Cryptography) và Mật mã khoá công khai (Public Key Cryptography).

3.1.1. Khái quát về hệ mật mã khóa công khai

Hệ mật mã khoá công khai, còn gọi là hệ mật mã không đối xứng (asymmetric Cryptography), sử dụng hai khoá khác nhau cho quá trình mã hóa và giải mã: một khoá (khoá công khai – public key) để mã hoá, và khoá kia (khoá riêng – private key) để giải mã. Hai khoá này có quan hệ với nhau về mặt toán học, nhưng từ khoá công khai không thể tìm ra được khoá riêng. Trông hệ mật này, nếu A muốn gửi cho B một bản tin mật, A trước tiên sẽ lấy khoá công khai của B từ cơ sở dữ liệu công cộng về khoá công khai. Sau đó A sẽ sử dụng khoá công khai của B để mã hoá bản tin, rồi gửi cho B. Phía B sẽ sử dụng khoá riêng của mình để giải mã bản tin mã. Như vậy là, chỉ B mới có thể giải được bản tin mã mà A đã tạo ra.

Hệ mật này được thực hiện nhờ vào đặc tính rất quan trọng của cặp khoá là không thể xác định được khoá giải mã nếu chỉ căn cứ vào các thông tin về thuật toán và khoá mã hoá.

Nguyên tắc chủ yếu của hệ mã PKI là dùng có 1 cặp khóa cho mỗi giao dịch khi dùng một khóa khóa này để mã hóa thì sẽ khóa kia dùng để giải mã và ngược lại.



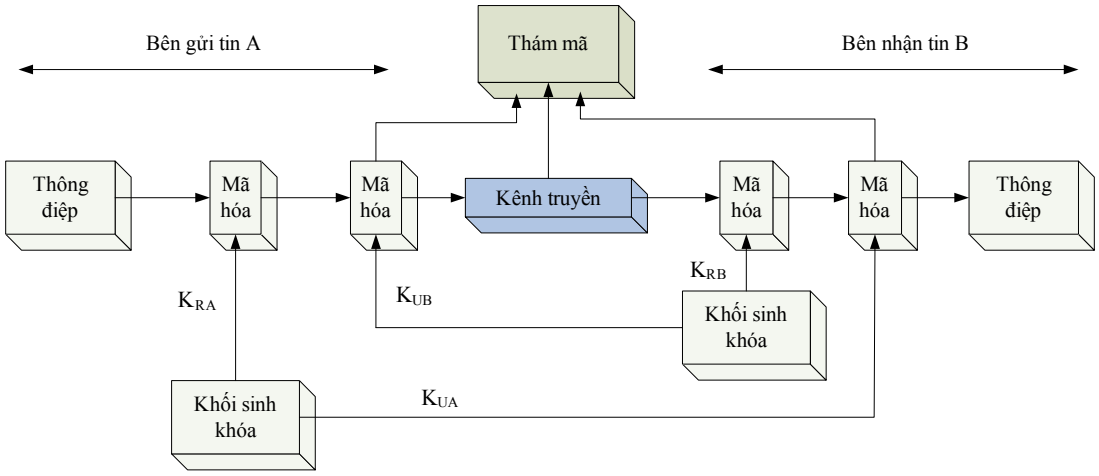
Hình 3.1. Hoạt động trao đổi thông tin bảo mật trong hệ khóa không đối xứng

Trong hoạt động trao đổi thông tin bảo mật thông điệp trong hệ khóa không đối xứng, thường dùng khóa công khai để mã hóa và dùng khóa riêng – khóa cá nhân để giải mã, như vậy chỉ người nào là chủ sở hữu khóa cá nhân thì mới có thể giải mã được bản tin đã mã hóa. Khác với hệ mật mã khóa đối xứng sử dụng một khóa bí mật duy nhất để vừa mã hóa và giải mã, phương pháp mật mã dùng cặp khóa công khai và khóa riêng để mã hóa và giải mã thông tin. Cặp khóa này tuy vẫn liên quan đến nhau theo kiểu tương ứng 1-1, nhưng nếu biết khóa này thì không thể suy ra khóa kia được, do đó, phương pháp mã hóa này có tên mã hóa bất đối xứng.

Yêu cầu cơ bản với một hệ mật mã hóa công khai [2]:

- Không thể tìm ra được khóa giải mã nếu biết thuật toán và khóa mã hóa.
- Cả 2 khóa trong cặp khóa này đều có thể dùng để mã hóa, khóa còn lại sẽ giải mã thông điệp do khóa thứ nhất mã hóa. (Đây là yêu cầu không bắt buộc nhưng hầu hết các thuật toán thông dụng trong công nghệ mã hóa công khai đều có đặc điểm này).
- Trong cặp khóa này, khóa công khai được công bố rộng rãi, khóa riêng được giữ bí mật cho chủ nhân của nó.

Vấn đề bảo vệ bí mật an toàn khóa cá nhân của chủ sở hữu là điểm mấu chốt của hệ thống khóa công khai.



Hình 3.2. Sơ đồ hoạt động hệ mật khóa công khai Đảm bảo tính xác thực và tính mật

Công việc mã hóa và giải mã có thể mô tả tóm tắt như sau:

- Mỗi đầu cuối trong hệ thống mạng sinh một cặp khóa dùng cho việc mã hóa và giải mã các thông điệp mà nó nhận được.
- Mỗi đầu cuối này công khai hóa một khóa dùng để mã hóa của nó. Khóa còn lại được đầu cuối này giữ cho riêng mình.
- Nếu A muốn gửi một thông điệp cho B, A dùng khóa công khai của B để mã hóa.
- Khi nhận được thông điệp này, B dùng khóa riêng của mình để giải mã. Chỉ B có khóa riêng này nên ngoài B ra, không ai có thể giải mã thông điệp đó.

3.1.2. Chữ ký số

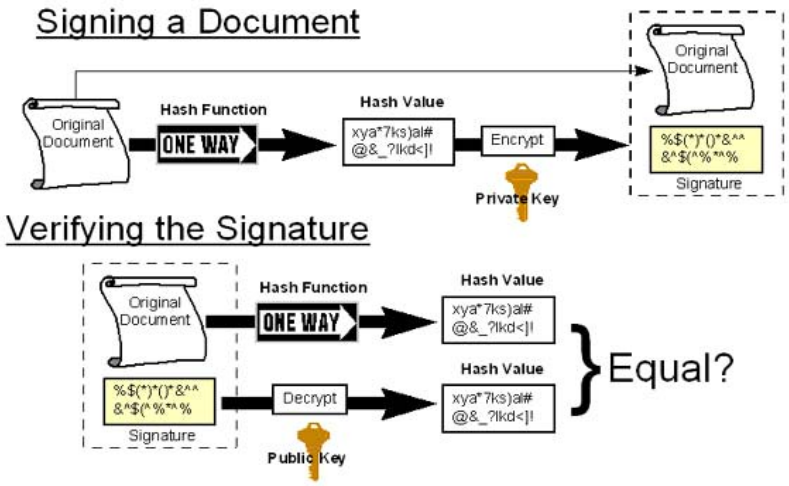
Ý tưởng về chữ ký điện tử cũng tương tự như chữ ký viết tay mà chúng ta vẫn dùng. Nó dùng để "ký" lên các thông tin cần gửi đi nhằm mục đích xác nhận tính trung thực của thông tin và của người gửi tin. Người nhận có thể biết được chữ ký này có đúng hay không và có phải của người gửi thực sự hay không. Ngoài ra, cũng như chữ ký viết tay, chữ ký điện tử đặc trưng cho chủ nhân của nó, kẻ khác không thể bắt chước được.

Chữ ký điện tử được biểu diễn trong máy tính bởi một xâu các số nhị phân. Nó được tạo ra bởi một tập luật, một tập tham số đặc trưng của người ký, cùng toàn bộ dữ liệu mà nó được dùng để ký lên. Có một thuật toán có khả năng tạo ra chữ ký bằng khóa riêng và xác minh chữ ký bằng khóa công khai tương ứng. Mỗi người dùng sở hữu một cặp khóa riêng / khóa công khai. Khóa công khai được công bố đại chúng, tuy nhiên khóa riêng thì chỉ có chủ nhân của nó biết. Do vậy, bất kì ai cũng có thể xác minh chữ ký của người khác bằng khóa công khai tương ứng, nhưng việc tạo ra chữ ký đó thì chỉ người sở hữu cặp khóa này mới làm được.

Một *hàm băm* được dùng trong quá trình tạo chữ ký. Mục đích của nó là nén dữ liệu, biến một mẩu tin thành mẩu tin tóm lược. Sau đó, mẩu tin tóm lược này được áp dụng thuật toán sinh chữ ký. Chữ ký được chuyển đi cho phía nhận cùng với dữ liệu đã ký [2].

Phía nhận làm nhiệm vụ kiểm tra xác minh mẩu tin vừa nhận được cùng chữ ký đi kèm bằng cách dùng khóa công khai của người nhận. Phía nhận cũng dùng một hàm băm

như trên để thực hiện trên dữ liệu được ký, thu được bản băm thứ nhất. Song song với việc đó, nó dùng khóa công khai của người gửi, giải mã chữ ký để thu được bản dữ liệu băm thứ hai. Nếu 2 bản băm này giống nhau, chữ ký được xác thực, ngược lại thì không.



Hình 3.3. Mô hình sử dụng chữ ký số

Thuật toán về chữ ký điện tử xác minh tính toàn vẹn của dữ liệu và nhân dạng của người ký. Thuật toán này được dùng cho thư điện tử, hay một số hoạt động qua mạng khác như chuyển tiền, trao đổi dữ liệu, phân phối phần mềm, lưu trữ dữ liệu và một số ứng dụng khác mà trong đó có yêu cầu về an toàn và toàn vẹn dữ liệu.

3.2. Hạ tầng khóa công khai PKI

3.2.1. Khái quát chung về PKI

Sáng kiến hạ tầng khóa công khai PKI (**P**ublic **K**ey **I**nfrastructure, viết tắt là PKI) ra đời năm 1995, khi mà các tổ chức công nghiệp và các chính phủ xây dựng các tiêu chuẩn chung dựa trên phương pháp mã hoá để hỗ trợ một hạ tầng bảo mật trên mạng Internet. Tại thời điểm đó, mục tiêu được đặt ra là xây dựng một bộ tiêu chuẩn bảo mật tổng hợp cùng các công cụ và lý thuyết cho phép người sử dụng cũng như các tổ chức (doanh nghiệp hoặc phi lợi nhuận) có thể tạo lập, lưu trữ và trao đổi các thông tin một cách an toàn trong phạm vi cá nhân và công cộng. PKI bản chất là một hệ thống công nghệ vừa mang tính tiêu chuẩn, chính sách, vừa mang tính ứng dụng được sử dụng để khởi tạo, lưu trữ và quản lý các chứng thực điện tử (digital certificate) cũng như các mã khoá công cộng và cá nhân. Hiện nay có rất nhiều cách định nghĩa khác nhau về PKI tuỳ theo góc độ nghiên cứu hoặc ứng dụng cơ sở hạ tầng này. Tuy nhiên, một cách cơ bản nhất có thể định nghĩa cơ sở hạ tầng khoá công khai là một hệ thống công nghệ, chuẩn, cấu trúc và các chính sách phối hợp với nhau nhằm bảo đảm tính bí mật và an toàn thông tin trên Internet sử dụng mật mã khoá công khai [2].

Cơ sở hạ tầng khóa công khai PKI là khung làm việc bao gồm cấu trúc tổ chức các thành phần hoạt động cả phần cứng và phần mềm hệ thống, cùng với các chính sách, các

thủ tục để quản lý và phân phối khóa, quản lý, cấp phát các chứng chỉ số (digital certificate) và chứng thực các chứng chỉ số. Nền tảng mật mã của PKI chính là hệ thống mật mã khóa công khai. Như vậy PKI là một cơ sở hạ tầng hệ thống vừa mang tính mô hình vừa mang tính công nghệ và các chuẩn, vừa là mô hình kiến trúc vừa là hệ thống các giao dịch và ứng dụng cho phép thực hiện khởi tạo, lưu trữ, quản lý các chứng chỉ số (Digital certificate), quản lý và phân phối các khoá công khai, khóa cá nhân và cơ chế chứng thực chứng chỉ số [11,12]. Hiện nay trên thế giới PKI được xây dựng và triển khai thành các kiến trúc hệ thống cụ thể bao gồm tổ chức phần cứng, phần mềm, các chính sách quy tắc, các thủ tục, các giao dịch trong hệ thống và các chuẩn. Công nghệ làm nền tảng cho các hoạt động chứng thực là công nghệ mật mã khoá công khai. Các thành phần cơ bản nhất trong công nghệ mật mã khoá công khai bao gồm các thuật toán để tạo cặp khoá công khai/ khoá riêng, các thuật toán bảo mật, cơ chế mã hoá và giải mã thông tin, phương pháp tạo ra chữ ký điện tử và cấu trúc của chứng chỉ số.

- ***Các thành phần chủ yếu của PKI bao gồm [11]***:

- CA (Certificate Authority): Bộ phận thẩm quyền phát hành chứng chỉ và chứng thực
- RA (Registration Authority): Bộ phận thẩm quyền đăng ký chứng chỉ,
- Certificate Holder- User: người sử dụng trong hệ thống PKI, chủ thể chứng chỉ,
- Digital Certificate Distribution System: Hệ thống phân phối chứng chỉ số, kho chứa
- Relying Party: Các thực thể liên quan sử dụng chứng chỉ.

Các hoạt động giao dịch cơ sở trong hệ PKI bao gồm: Tạo yêu cầu chứng chỉ số; Phát hành chứng chỉ số; công bố chứng chỉ số; sử dụng/ hủy bỏ chứng chỉ số; chứng thực chứng chỉ số, bảo vệ khóa cá nhân của người dùng chứng chỉ số.

Sơ lược về công nghệ và kỹ thuật, có các chuẩn hệ thống PKI với các định dạng chứng chỉ số khác nhau [12]:

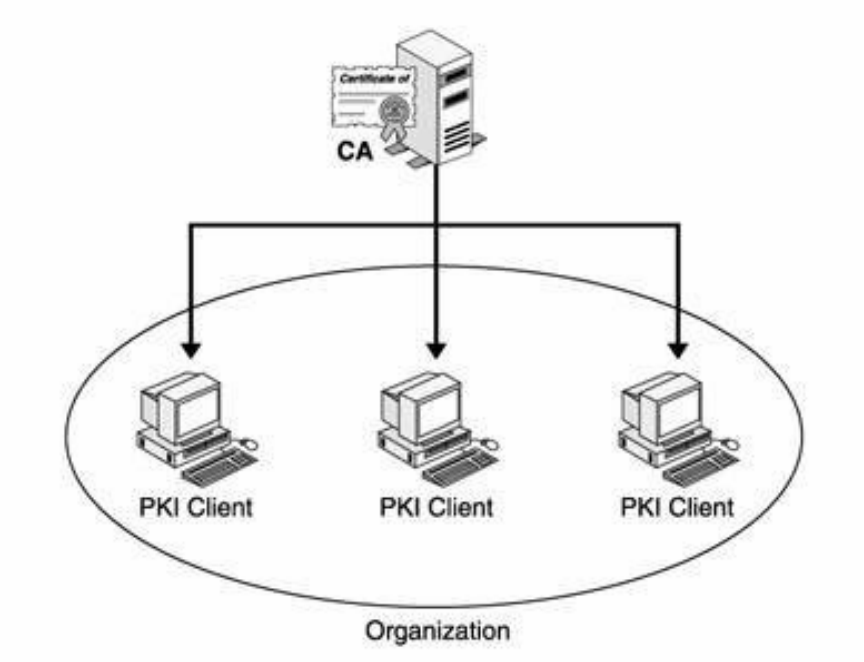
- Chứng thực số theo chuẩn X.509: Do nhóm PKIX của IETF xây dựng, dùng giao thức bảo mật SSL, IPSec…, sử dụng cho mô hình kiến trúc PKI phân cấp.
- Chứng thực số SPKI - Simple Public Key Infrastructure.
- Chứng thực số PGP - Pretty Good Privacy: Do Phil Zimmermann thiết kế vào năm 1991, chuẩn mã hóa thư điện tử và chứng thực chữ ký số bằng chứng nhận PGP, sử dụng mô hình PKI lưới – Web of Trust.

3.2.2. Các mô hình kiến trúc của PKI

Về mặt lý thuyết thì có nhiều kiểu mô hình PKI. Mỗi mô hình có các thuộc tính về tổ chức và sự tin cậy riêng như số lượng các CA trong một PKI, điểm tin cậy của người dùng cuối trong một PKI, và quan hệ tin cậy giữa các CA trong một PKI có nhiều CA [2,11,12] .

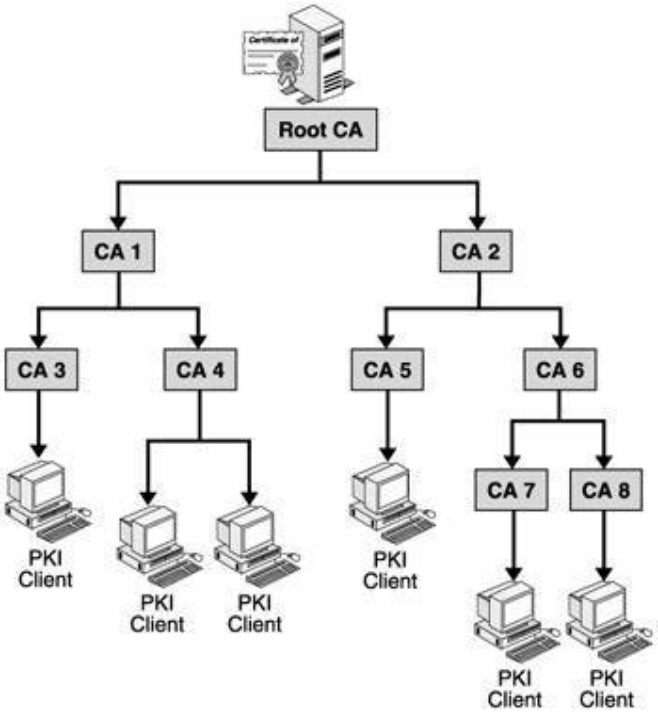
Tuy nhiên, thực tế chỉ có một số mô hình PKI sau đây là được triển khai:

- Kiến trúc một CA đơn - Single CA architecture



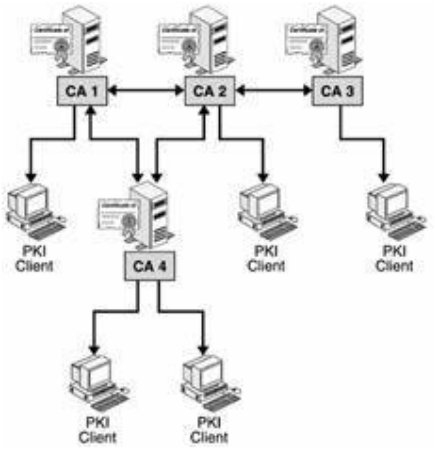
Hình 3.4. Kiến trúc CA đơn

- Kiến trúc cây phân cấp - Hierarchical architecture



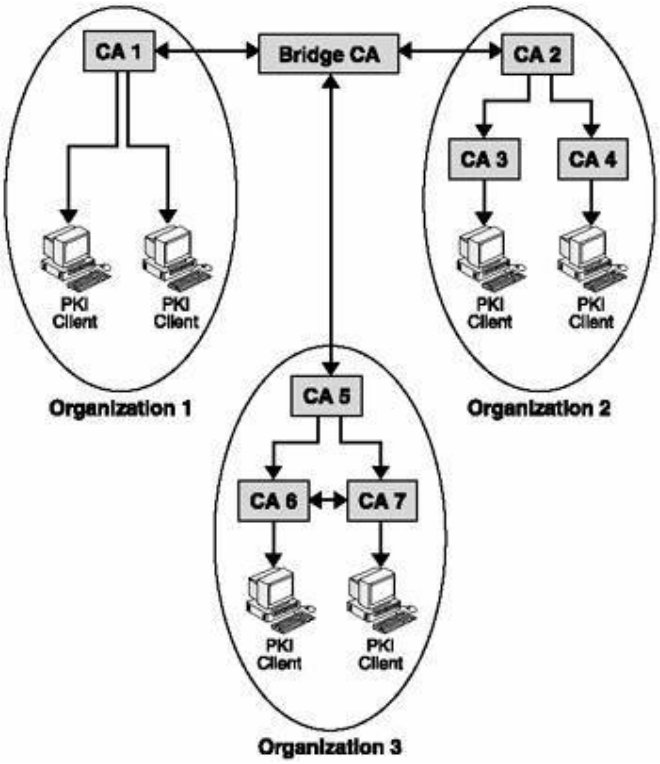
Hình 3.5. Kiến trúc CA phân cấp

- Kiến trúc mắt lưới - Mesh architecture



Hình 3.6. Cấu trúc CA dạng lưới

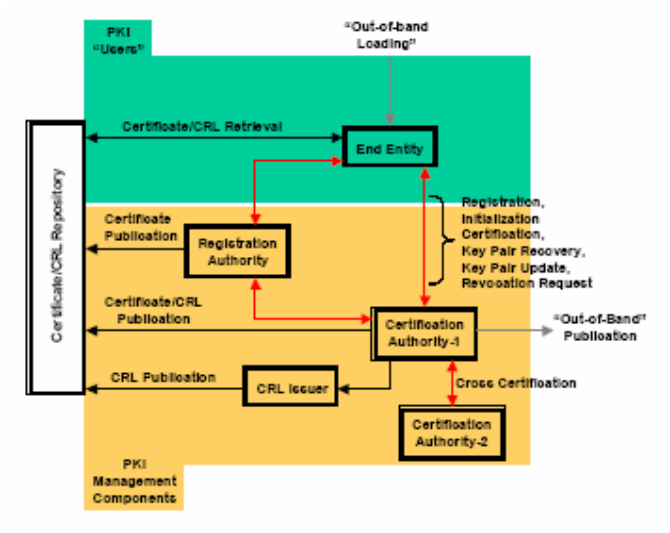
- Kiến trúc hỗn hợp - Hybrid architecture



Hình 3.7. Kiến trúc PKI dạng hỗn hợp

3.2.3. Kiến trúc các thành phần trong hoạt động PKI

Có thể thấy trên hình vẽ dưới đây sự phối hợp hoạt động của 5 thành phần cơ bản trong kiến trúc của PKI [11]:



Hình 3.8. Kiến trúc các thành phần PKI

- Các thực thể đầu cuối (End Entities – EE)

Trên thực tế, một EE có thể là người dùng cuối, hoặc một thiết bị như router, máy chủ, một xử lý, hay bất kì thứ gì có thể được gán là đối tượng của hệ thống chứng chỉ khóa công khai. Tóm lại, EE có thể được hiểu là khách hàng của các dịch vụ PKI. Thậm chí, một nhà cung cấp các dịch vụ PKI cũng đôi khi được coi là EE, ví dụ một RA có thể coi là EE của CA (CA và RA sẽ được giải thích cụ thể sau). Các EE bị ràng buộc bởi các chứng chỉ. Ví dụ như các server và các người dùng đầu cuối phải được kết nạp vào PKI trước khi có thể tham gia như một thành viên của PKI.

- Bộ phận thẩm quyền phát hành chứng chỉ (Certificate Authority – CA)

Các khóa công khai được phân tán theo các chứng chỉ. Bởi thế, CA là một phần vô cùng quan trọng trong kiến trúc PKI vì nó là đơn vị duy nhất ký và phát hành các chứng chỉ khóa công khai (CA sử dụng khóa riêng của mình để ký các chứng chỉ). Thực chất của công việc là liên kết tên đối tượng với khóa công khai, công nhận rằng đối tượng đó sở hữu khóa công khai tương ứng. CA cũng đồng thời chịu trách nhiệm phát hành các danh sách chứng chỉ bị hủy (CRL) nếu nó không ủy quyền cho một đơn vị chuyên trách làm việc này (CRL Issuer). CA cũng thực hiện một số tác vụ quản trị như đăng ký cho người dùng, tuy nhiên việc này thường được ủy thác cho RA (Registration Authority) (RA sẽ được giải thích rõ ràng sau). Trong quá trình hoạt động, CA còn kiêm nhiệm cả việc lưu và khôi phục khóa mặc dù công việc này cũng có thể được ủy thác cho một bộ phận chuyên trách.

Trong kiến trúc PKI, thông thường, các EE được định cấu hình với một hay nhiều mốc tin cậy nào đó. Những mốc này được coi là điểm xuất phát cho các quá trình xác minh tiếp theo. Chính CA đóng vai trò làm cơ sở cho sự an toàn và tin cậy này.

- Bộ phận thẩm quyền đăng ký (Registration Authority – RA)

RA là một thành phần không bắt buộc phải có trong kiến trúc PKI. Tuy nhiên sự xuất hiện của nó là rất hữu ích vì sẽ giảm nhẹ số lượng công việc mà CA phải làm. Như chúng ta đã nói ở trên, RA thường tham gia vào quá trình đăng kí cho các EE. Công việc này bao gồm cả việc xác minh các thông tin mà EE dùng để đăng ký với PKI. Ngoài ra, RA còn đảm nhiệm một số công việc khác, gồm:

- Thiết lập và xác nhận thông tin cá nhân của một thực thể.

- Phát tán thông tin chia sẻ tới các người dùng, để phục vụ việc xác thực trong một tiến trình khởi tạo trực tuyến.

- Khởi tạo tiến trình chứng nhận bởi một CA. Lúc này, RA đóng vai trò một EE.

- Cung cấp các thông tin cần thiết với tư cách một người dùng cuối.

- Thực hiện việc quản lý vòng đời của các khóa, chứng chỉ.

Mặc dù RA có thể gánh vác rất nhiều công việc giúp CA, nhưng nó không bao giờ được giao quyền phát hành chứng chỉ khóa công khai, đây luôn là độc quyền của CA. Tóm lại, việc xuất hiện của RA mang lại 2 lợi ích chính:

- Giảm chi phí, đặc biệt là đối với các tổ chức phân tán trên diện rộng, có thể phân tán các RA để quản lý giúp CA.

- Việc giảm nhẹ công việc cho CA giúp CA có thể nghỉ ngơi nhiều hơn. Do đó sẽ giảm thiểu được các cơ hội tấn công nhằm vào CA đó.

- Chứng chỉ và hệ thống kho lưu trữ các chứng chỉ

Trong việc dùng khóa công khai, chứng chỉ là một văn bản điện tử được CA ký cho các EE, công nhận tính đúng đắn và xác thực của các thông tin mà EE dùng để giao tiếp. Kho lưu trữ các chứng chỉ thường là một thư mục. Tuy nhiên, trong kiến trúc PKI, kho này thực chất là một cách nào đó để lưu các thông tin liên quan của PKI, ví dụ như các chứng chỉ khóa công khai, các CRL.

Trong chuẩn X.500, kho lưu trữ này là một thư mục máy chủ mà máy khách có thể truy cập qua giao thức LDAP (Lightweight Directory Access Protocol), hoặc lấy file trên máy chủ qua giao thức FTP (File Transfer Protocol), giao thức HTTP (Hyper Text Transfer Protocol).

Ngoài ra, kho này còn đáp ứng được một số yêu cầu từ phía hệ thống máy khách. Ví dụ có thể trả lời cho máy khách về tình trạng của các chứng chỉ, xem chúng đã bị hủy chưa. Tuy nhiên, lợi ích cơ bản của các kho lưu trữ này chính là việc các EE có nơi để tìm các chứng chỉ và các CRL. Ví dụ khi A muốn giao tiếp với B, A phải biết được khóa công khai của B, và khóa đó có thể tìm thấy trong kho lưu trữ này. Danh sách các chứng chỉ bị hủy

(CRL - Certificate Revocation List) và bộ phận phát hành (CRL Issuers). CRL chứa danh sách các chứng chỉ bị hủy, kèm theo chữ kí điện tử để đảm bảo sự toàn vẹn và xác thực của nó. Chữ kí trong CRL thường chính là của thực thể đã kí và phát hành các chứng chỉ trong CRL này. Các CRL thường được lưu để có thể dễ dàng thực hiện xác minh các chứng chỉ khi làm việc off-line.

Thông thường, CA phát hành các chứng chỉ số nào thì sẽ đồng thời chịu trách nhiệm phát các thông tin về các chứng chỉ bị hủy trong số đó. Tuy nhiên, CA cũng có thể ủy thác cho một bộ phận khác chuyên phát hành các thông tin này, đó chính là bộ phận phát hành CRL (CRL Issuer). Trong trường hợp đó, các CRL được phát hành gọi là các CRL gián tiếp.

3.3. Các giao dịch điện tử với hạ tầng khóa công khai

3.3.1. Các dịch vụ của PKI

- Đảm bảo quá trình truyền thông an toàn. Cung cấp một kênh truyền thông tin cậy giữa PKI và khách hàng. Tư vấn khách hàng các giải pháp, cũng như thực hiện truyền thông tin cậy giữa các khách hàng. Ta có thể kể đến một số các dịch vụ ứng dụng PKI:
- Secure e-mail (sử dụng giao thức, ví dụ như Secure Multipurpose Internet Mail Extensions Version 2, S/MIMEv2, [RFC2311, RFC2312] hoặc S/MIMEv3 [RFC2632, RFC2633])
- Secure Web server access (sử dụng giao thức, ví dụ như Transport Layer Security, or TLS, [RFC2246])
- A secure Virtual Private Network, or VPN (sử dụng giao thức, ví dụ như IPsec/IKE [RFC2401, RFC2411])
- Ví dụ như với secure-email, có thể thực thi bởi dịch vụ của PKI như sau: Khách hàng sẽ sử dụng gói phần mềm đi kèm của PKI để mã hóa email rồi truyền email đó qua các vùng mạng không an toàn sử dụng cú pháp chuẩn S/MIME mà không còn phải lo lắng về “tính toàn vẹn”, “tính xác thực”, “tính mật” của email đó.
- Chống phủ nhận: bất kỳ tài liệu tài phát tán trên mạn “bắt đầu” từ một nhà phân phối “hợp lệ” thì đều bị PKI tìm ra ai là chủ thể của nó, giúp đảm bảo quyền lợi của khách hàng. Các PKI cũng có thể “hợp tác” với nhau để tạo ra một môi trường truyền thông khá “lý tưởng” cho khách hàng.
- PKI cũng cung cấp luôn cả các dịch vụ về phân quyền, đối với một tài liệu, căn cứ vào nội dung chứng chỉ có thể cho biết khách hàng những quyền gì đối với loại tài liệu đó.

3.3.2. Xác thực an toàn trong giao dịch điện tử

- Dưới góc nhìn về bảo mật thông tin phải đảm bảo các yêu cầu sau:

- Yêu cầu về bảo mật thông tin: trong giao dịch điện tử xuất hiện rất nhiều thông tin riêng tư cần được giữ mật ở từng mức độ khác nhau. Đó là các thông tin về cá nhân khách hàng (danh tính, địa chỉ, địa chỉ thư điện tử, các thông tin về tài khoản ngân hàng…); các thông tin về tài khoản của doanh nghiệp tại các ngân hàng….

- Yêu cầu về tính toàn vẹn thông tin: thông tin giao dịch được mã hóa dưới dạng chuỗi bit/byte và được truyền qua môi trường mạng Internet. Như chúng ta đã biết, mạng Internet hoàn toàn là một hệ thống "mở", rất dễ bị tấn công và xâm nhập. Các thông tin giao dịch không những bị lộ mà hoàn toàn có thể bị thay đổi với mục đích xấu.

- Yêu cầu về chứng thực nguồn gốc thông tin: các thông tin trong giao dịch điện tử đều có chủ thể của nó (khách hàng, doanh nghiệp, trung tâm xử lý dữ liệu, ngân hàng …).

- Yêu cầu về chứng thực nguồn gốc thông tin gồm có 2 khía cạnh:

  - Ai là chủ thể của thông tin?

  - Chống từ chối nguồn gốc thông tin?

- Các yêu cầu về an toàn hệ thống khác: chống tấn công và xâm nhập vào website, trung tâm dữ liệu…, chống ăn cắp thông tin khách hàng.

Xác thực trở thành một yêu cầu cấp thiết và tối quan trọng ngay từ khi các ý tưởng về thương mại điện tử mới ra đời. Trong quá trình phát triển và giải quyết vấn đề xác thực thì chứng chỉ số tạo bởi hạ tầng khóa công khai PKI (Public Key Infrastructure) nổi lên như một giải pháp ưu việt hàng đầu. Tuy nhiên, một trong những vấn đề nổi cộm đó là bảo vệ các chứng chỉ số và các khóa riêng tư (khóa bí mật).

3.3.3. Đặc điểm khi triển khai PKI

- Những lợi ích có thể nhận thấy khi triển khai PKI là [12]:

  - Tiết kiệm thời gian làm việc, ví dụ như thư từ, báo cáo, hợp đồng có thể gửi theo con đường điện tử thay vì dùng con đường vật lý như truyền thống.

  - Người dùng có thể dành thời gian vào các công việc phải làm tay, thay vì luẩn quẩn với các công việc của cơ sở hạ tầng bảo mật.

  - Sự quản lý tập trung, thống nhất sẽ giảm bớt lượng tài nguyên cho công việc quản trị.

  - Giá vật liệu thấp hơn, cần ít không gian lưu trữ hơn, ít dư thừa hơn.

  - Giảm tổn thất do mất mát thông tin.

  - Khả năng tạo mạng riêng ảo (Virtual Private Network – VPN) qua một mạng công cộng như Internet có thể làm giảm chi phí so với việc thuê một đường dây riêng.

  - Có thể tạo ra lợi nhuận từ việc kinh doanh một số dịch vụ, ví dụ như việc kiểm tra tính hợp lệ của các giao dịch tài chính bằng chữ kí điện tử và chứng chỉ số.

- Nhược điểm và khó khăn khi triển khai PKI

Tuy nhiên bên cạnh các điểm mạnh, cũng có một số điểm đáng cân nhắc khi có ý định triển khai PKI:

- Hệ thống phức tạp, kiến trúc còn phụ thuộc các chính sách
- Tính pháp lý của chứng chỉ số.

3.4. Vấn đề an toàn trong hệ thống PKI

Mặc dù hệ thống PKI được coi là giải pháp cho vấn đề an ninh và xác thực hiện nay, nhưng bản thân hệ thống cũng như cơ chế, mô hình hoạt động của nó vẫn còn sơ hở. Các sơ hở này không nhất thiết đến từ cơ chế mật mã học, vốn đã được cộng đồng mật mã kiểm nghiệm, mà đến từ nhiều nhân tố chủ quan và khách quan khác nhau, trong đó phải kể tới yếu tố con người. Một hệ PKI về cơ bản vẫn tồn tại một số rủi ro về bảo mật sau: Mất khóa cá nhân, giả mạo khóa công khai, giả mạo định danh chủ thể [3,18].

- ***An toàn khóa cá nhân***

Trong hệ thống PKI hiện nay, khóa cá nhân được lưu trữ trên phương tiện truyền thống như trên máy tính của người dùng, hoặc smartcard và phương tiện này được bảo vệ truy cập bằng một mật khẩu được bảo vệ truy cập bằng một mật khẩu độ dài 6 đến 8 ký tự, độ an toàn của người dùng phụ thuộc cả vào mật khẩu này. Cơ chế đảm bảo an toàn cho khóa cá nhân bằng mật khẩu không thể hiện được tính chống phủ nhận trong mật mã học. Bản thân mật khẩu có nhiều nguy cơ dễ bị lộ, hoặc bị mất bởi virus, bị đánh cắp bởi các chương trình mã độc hại. Khi khóa cá nhân để mất sẽ rất nguy hiểm, thì bất cứ ai cũng có thể giả mạo người đó và không chỉ là mất thông tin mà còn có thể dẫn đến đổ vỡ cả hệ thống. Như vậy độ an toàn bảo mật khi dùng cặp khóa trong hệ thống phụ thuộc vào mật khẩu. Bảo mật khóa cá nhân là vấn quan trọng trong hệ thống cơ sở hạ tầng PKI và cũng là điểm yếu trong hoạt động của các hệ PKI truyền thống.

- ***Giả mạo khóa công khai***: Trường hợp khóa này được bảo vệ bằng chữ ký của CA, tức là kiểm tra được bằng khóa công khai của CA, có nguy cơ kẻ tấn công thay thế khóa của CA trên máy người dùng, sau đó tiến hành thay thế khóa công khai của người dùng bằng khóa giả. Giả mạo khóa công khai dẫn đến lộ thông tin trong hệ thống.

- ***Định danh đối tượng***: Chứng chỉ số có chứa tên của đối tượng và phải có thêm các thông tin bổ sung đủ để tránh trường hợp định danh sai do các thông tin cá nhân của người dùng trùng nhau

Trong các nguy cơ về bảo mật kể trên ta thấy nguy cơ lớn nhất trong PKI là bị mất khóa cá nhân. Vấn đề này có thể được giải quyết bằng một cơ chế xác thực định danh mạnh hơn mật khẩu truyền thống. Đó là sinh trắc học. Do sinh trắc học mang bản chất chống phủ nhận, khả năng giả mạo, mất trộm đặc trưng sinh trắc học thấp hơn nhiều so với mật khẩu, nên đây là giải pháp tương đối hoàn thiện cho vấn đề an toàn và sử dụng khóa cá nhân.

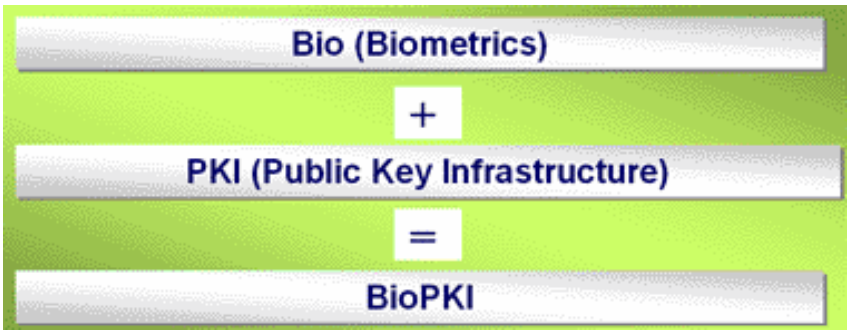
Phần III. BÁO CÁO KẾT QUẢ NGHIÊN CỨU CỦA ĐỀ TÀI

Chương 4.
NGHIÊN CỨU PHÂN TÍCH VÀ XÂY DỰNG MÔ HÌNH GIẢI PHÁP HỆ THỐNG BioPKI

4.1. Vấn đề kết hợp sinh trắc vào hạ tầng khóa công khai PKI

Như đã trình bày ở các chương trên, ngày nay hạ tầng khóa công khai PKI là nền tảng cho nhiều ứng dụng bảo mật phát triển cho các giao dịch điện tử qua mạng Internet. Tuy nhiên, trong hệ thống PKI vẫn tồn tại vấn đề về an toàn trong việc quản lý và bảo vệ khóa cá nhân. Vấn đề này đã được nghiên cứu từ lâu, đã có rất nhiều các giải pháp khác nhau được đưa ra để giải quyết vấn đề. Một trong những giải pháp đang được quan tâm nghiên cứu là kết hợp sinh trắc học với PKI để tăng cường khả năng an toàn cho hệ thống PKI nhằm loại bỏ nguy cơ sử dụng trái phép khóa cá nhân.

Khái quát về một hệ thống BioPKI được minh họa trong Hình 4.1.



Hình 4.1. Hướng tiếp cận hệ thống BioPKI

Tuy nhiên hệ thống BioPKI không phải chỉ là một phép cộng đơn giản giữa hạ tầng khóa công khai PKI với một hệ sinh trắc học nào đó. Việc nghiên cứu xây dựng hệ thống BioPKI cần giải quyết các vấn đề chủ yếu sau:

- Hệ thống xác thực thẩm định sinh trắc (Biometric Verification-Authentication System) với các vấn đề về độ khó thẩm định sinh trắc sống và về các loại sinh trắc (đã trình bày ở chương 2)
- Hạ tầng khóa công khai PKI: Kiến trúc, chính sách, công nghệ và các vấn kỹ thuật (đã trình bày ở chương 3)
- Mô hình kết hợp hai hệ thống: Biometric security system và PKI system

Hơn nữa, nghiên cứu xây dựng hệ BioPKI liên quan đến nhiều vấn đề từ cơ sở pháp lý, chính sách, mô hình kiến trúc, mô hình tích hợp đến phân tích thiết kế hệ thống, thiết kế các giải thuật và các giải pháp kỹ thuật thực thi. Các phần tiếp theo của chương này sẽ trình bày phân tích các hướng tiếp cận BioPKI trên cơ sở đó xây dựng giải pháp về hệ thống Bio-PKI.

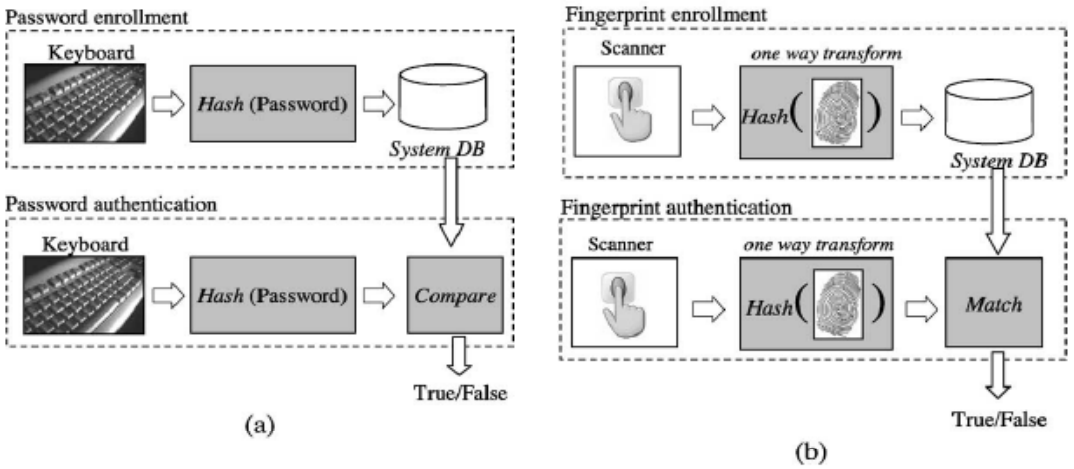
4.2. Phân tích các hướng tiếp cận nghiên cứu hệ thống BioPKI

Hiện nay có 3 hướng tiếp cận chủ yếu nghiên cứu về giải pháp hệ BioPKI [3,5,7]:

- Giải pháp 1: Đối sánh đặc trưng sinh trắc thay mật khẩu (password) xác thực chủ thể
- Giải pháp 2: Tích hợp kỹ thuật nhận dạng sinh trắc vào quá trình mã hóa bảo mật, mật mã sinh trắc bảo vệ khóa cá nhân
- Giải pháp 3: Sinh khóa cá nhân trực tiếp từ các đặc trưng sinh trắc học

4.2.1. Giải pháp 1: đối sánh đặc trưng sinh trắc thay mật khẩu để xác thực chủ thể

Mô hình nguyên tắc hoạt động của hệ thống xác thực dùng thẩm định sinh trắc vân tay thay mật khẩu được minh họa trong hình 4.2.



Hình 4.2. Hệ thống xác thực mật khẩu và xác thực thẩm định sinh trắc vân tay

Theo giải pháp này, người dùng mỗi khi sử dụng hệ thống PKI cần gửi kèm theo thông tin sinh trắc học để chứng minh bản thân. Hệ thống PKI sẽ thực hiện các các thủ tục xác thực thông thường và thực hiện đối sánh thông tin sinh trắc của người dùng kèm theo tại thời điểm đó với mẫu sinh trắc đã lưu trong quá trình đăng ký.

Giải pháp 1 cho phép làm tăng tính tin cậy của hệ thống PKI, nhưng cần phải lưu ý một số đặc điểm sau:

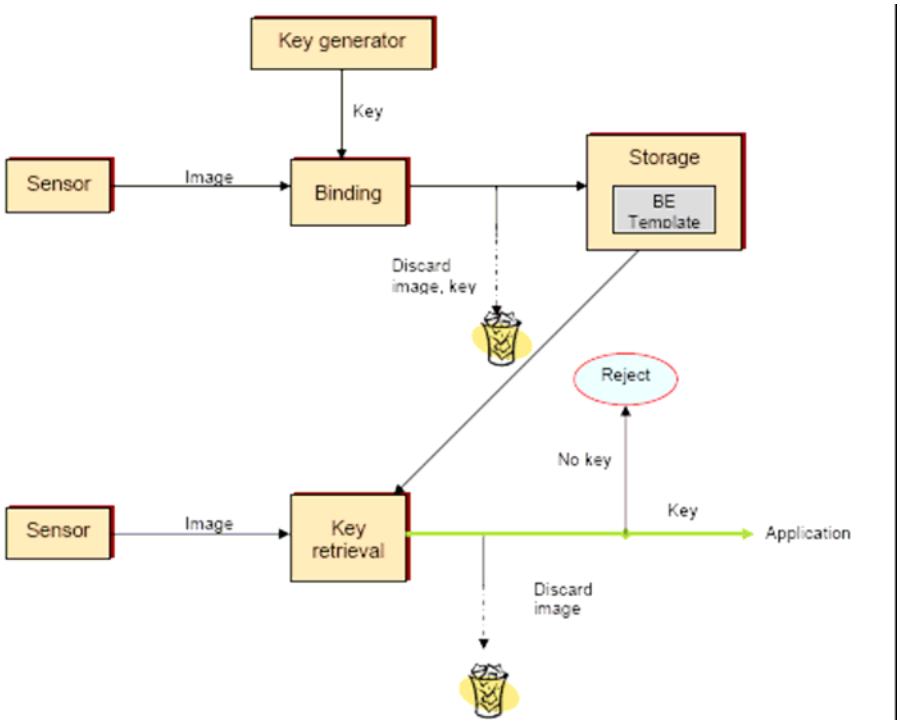
- Hệ thẩm định xác thực sinh trắc dựa trên kỹ thuật đối sánh mẫu thông thường của kỹ thuật nhận dạng, dễ khả thi.
- Khi các mẫu sinh trắc được lưu trữ tập trung tại Server, đặt ra vấn đề bảo đảm an toàn cho máy chủ lưu trữ và quá trình truyền các đặc trưng sinh trắc từ nơi lưu trữ đến nơi sử dụng đối sánh.

- Quá trình đối sánh đặc trưng thẩm định sinh trắc tách rời quá trình hoạt động mật mã trong hệ PKI. Kết quả đối sánh đặc trưng sinh trắc là điều kiện để hệ thống tiếp tục thực hiện các hoạt động khác, hơn nữa các kết quả thường được gửi qua môi trường mạng truyền thông, do vậy có nảy sinh nguy cơ bị tấn công vào kênh truyền thông nhằm làm sai lệch kết quả trả lời.
- Đặc trưng sinh trắc học được gửi từ người dùng tới máy chủ để đối sánh nên có thể bị mất trộm và dẫn đến tấn công giả mạo.
- Ưu điểm là tận dụng các kỹ thuật về đối sánh sinh trắc học hiện có, dễ thực hiện trên thiết bị nhúng. Khi kết hợp với giải pháp công nghệ nhúng có thể tổ chức lưu tại thiết bị nhúng cá nhân, tuy nhiên độ an toàn bảo mật còn phụ thuộc vào độ an toàn của dòng thiết bị lưu trữ mẫu và giao thức truyền thông bảo mật từ nơi lưu trữ đến nơi sử dụng.

4.2.2. Giải pháp 2: kết hợp kỹ thuật nhận dạng sinh trắc với kỹ thuật mật mã, mã hóa bảo mật khóa cá nhân

Theo hướng tiếp cận này, nhiều phương pháp đang được quan tâm nghiên cứu, nổi bật là phương pháp mã hóa bảo mật sinh trắc BE (Biometric Encryption) [1,7]. Quá trình mã hóa bảo mật mã sinh trắc học là quá trình mã hóa gắn kết số PIN hay khóa mã sinh trắc với đặc trưng sinh trắc sao cho sau đó cả khóa mã và đặc trưng sinh trắc gốc đều không cần lưu trữ và khôi phục chính xác. Tuy nhiên khóa sinh trắc chỉ được tạo lại đúng khi mẫu sinh trắc học sống của chủ thể xuất hiện trong quá trình thẩm định.

Sơ đồ khối mô hình hệ thống dựa trên kỹ thuật BE được trình bày trong hình 4.3



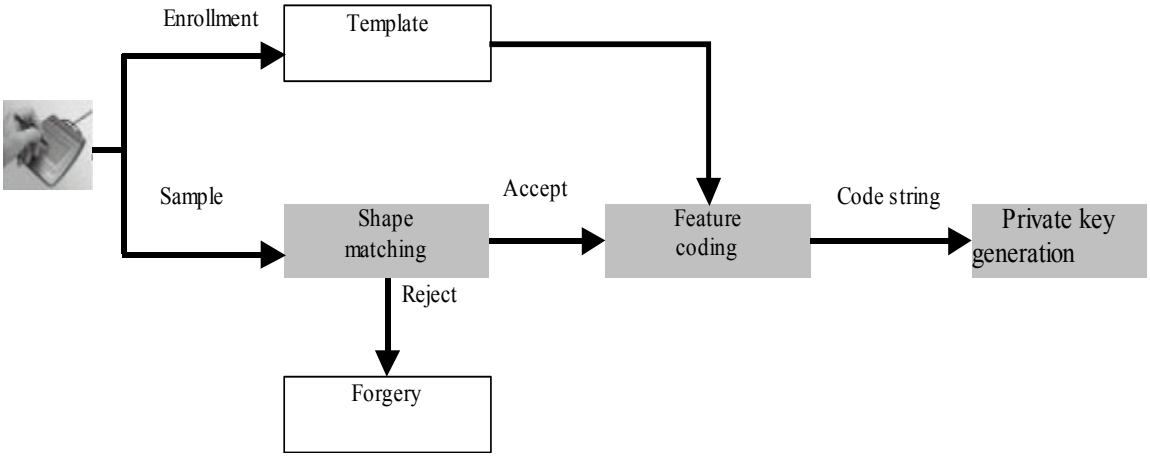
Hình 4.3. Hệ thống BioPKI xác thực thẩm định sinh trắc theo phương pháp mật mã sinh trắc học (Biometric Encryption- BE)

Đây là hướng nghiên cứu mới đang được nhiều người quan tâm nghiên cứu hiện nay, các đặc điểm của phương pháp này như sau:

- Hệ thẩm định xác thực sinh trắc dựa trên khóa mã sinh trắc tránh phải đối sánh mẫu sinh trắc trực tiếp, cho phép chấp nhận độ không ổn định khi thu nhận các dấu sinh trắc sống trực tuyến, giải quyết một vấn đề khó mấu chốt của các hệ thống thẩm định sinh trắc.
- Lưu các khóa mã sinh trắc thay cho lưu trực tiếp các mẫu sinh trắc, cho phép tổ chức lưu trữ phân tán và an toàn
- Quá trình đối sánh sinh trắc được tích hợp vào quá trình hoạt động mật mã trong các giao dịch sử dụng chứng chỉ số của hệ PKI. Quá trình thẩm định chủ thể gắn liền với cơ chế trao đổi khóa trong các hoạt động giao dịch làm tăng độ an toàn lưu trữ và bảo vệ truy cập khóa cá nhân.
- Độ khó và độ phức tạp của các thuật toán mật mã sinh trắc (Biometric Encyption), đòi hỏi nhiều nghiên cứu về mô hình và thuật toán.

4.2.3. Giải pháp 3: dùng sinh trắc học để sinh khóa cá nhân

Ý tưởng chính của hướng này là khóa cá nhân được sinh trực tiếp dựa trên đặc trưng sinh trắc học và được dùng để ký các dữ liệu. Ưu điểm lớn nhất của giải pháp này là nó không cần nơi để lưu trữ, do vậy loại bỏ nguy cơ tấn công khóa cá nhân. Mặt khác, hệ thống rất thuận tiện khi bản thân người dùng đã "mang" theo khóa cá nhân để sử dụng ở bất kỳ đâu, không cần thiết phải có đĩa lưu trữ hoặc smartcard [13]. Khóa công khai sẽ được sinh tương ứng với khóa cá nhân này theo thuật toán RSA.

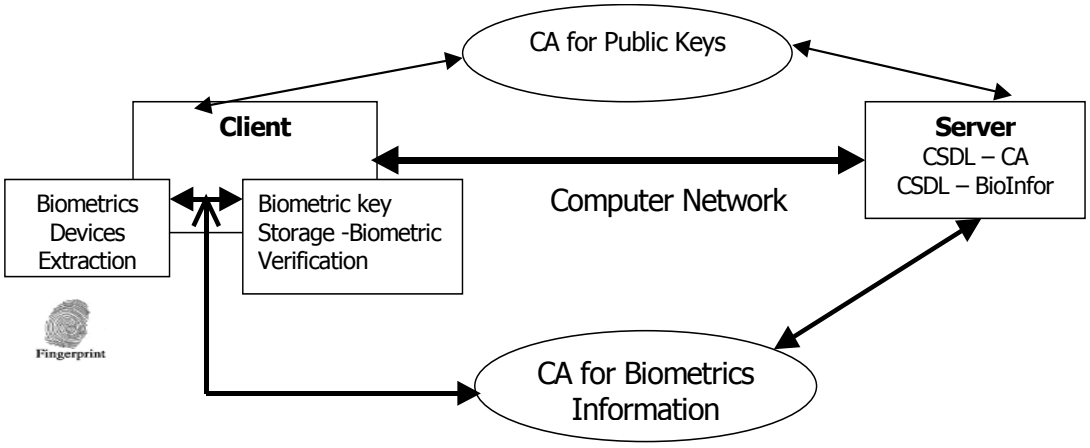


Hình 4.4. Hệ thống BioPKI dùng khóa cá nhân sinh trắc học

Trên thực tế giải pháp 3 khó khả thi, khó triển khai ứng dụng và có những giới hạn về lý thuyết. Định hướng nghiên cứu về hệ thống BioPKI sẽ nghiên cứu hai giải pháp 1 và 2 và tập trung nghiên cứu giải pháp 2.

4.3. Đề xuất mô hình giải pháp hệ thống BK-BioPKI của đề tài

Theo hướng nghiên cứu BioPKI [5], khung làm việc của hệ thống BioPKI trong môi trường mạng được trình bày trong hình 4.5 dưới đây.



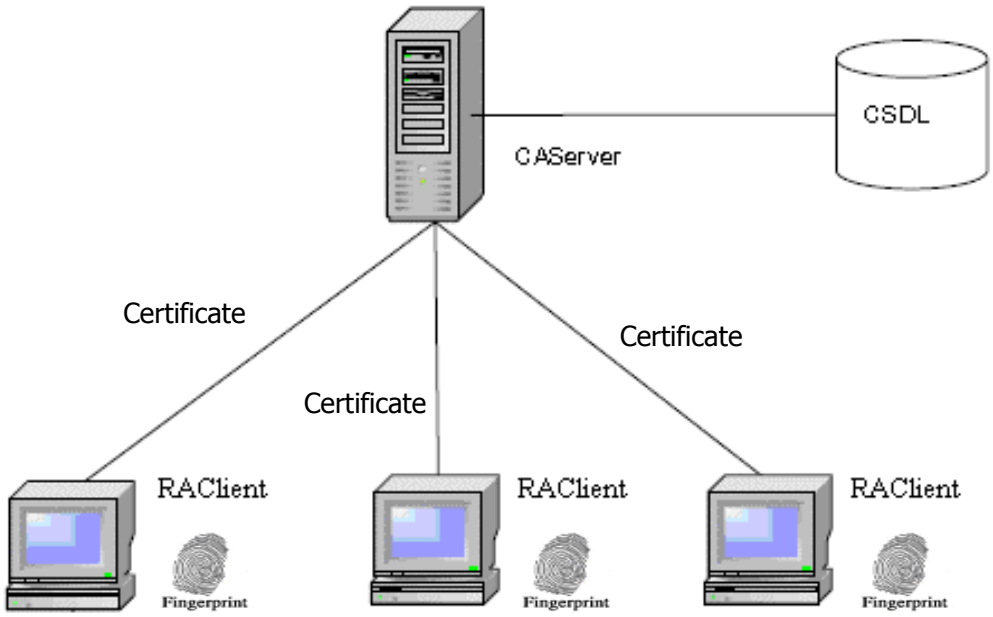
Hình 4.5. Khung làm việc của hệ thống trong môi trường mạng

Để đạt được các kết quả nghiên cứu theo các yêu cầu nhiệm vụ, nội dung nghiên cứu của nhiệm vụ đề tài được xác định bao gồm từ nghiên cứu về phương diện lý thuyết xây dựng mô hình giải pháp hệ thống an ninh dựa trên sinh trắc học vân tay kết hợp với hạ tầng khóa công khai BioPKI đến nghiên cứu về phương diện kỹ thuật phân tích thiết kế toàn bộ hệ thống BioPKI và lựa chọn giải pháp công nghệ thực thi cài đặt triển khai hệ thống trong môi trường mạng phòng thí nghiệm. Trên cơ sở đó xây dựng và thử nghiệm một số ứng dụng về chữ ký số và bảo mật thông điệp trong hệ thống BioPKI.

Đề xuất mô hình hệ thống an ninh thông tin dựa trên sinh trắc học BioPKI bao gồm các thành phần hệ thống sau:

- Hệ thống lõi hạ tầng khóa công khai PKI
- Hệ thống sinh trắc thẩm định xác thực sinh trắc vân tay trực tuyến (Fingerprint Biometric System)
- Mô hình tích hợp hệ sinh trắc vào hạ tầng khóa công khai và xây dựng hệ thống tích hợp BioPKI (gọi tên là BK-BioPKI)

Mô hình mức khung cảnh hệ thống BK-BioPKI được trình bày trong Hình 4.6.



Hình 4.6. Mô hình mức khung cảnh hệ thống BioPKI

4.3.1. Hệ thống lõi hạ tầng khóa công khai PKI.

Như đã trình bày ở phần trên, nhiệm vụ chủ yếu của đề tài tập trung vào vấn đề tăng cường bảo mật khóa cá nhân trong hoạt động hệ thống PKI, đề tài lựa chọn giải pháp xây dựng hệ thống PKI dựa trên mô hình kiến trúc CA đơn làm hệ thống lõi để nghiên cứu giải pháp tích hợp hệ thống sinh xác thực thẩm định sinh trắc vào hệ PKI để xác thực sinh trắc người dùng.

• Hệ thống hạ tầng cơ sở PKI của đề tài được xây dựng đảm bảo đầy đủ các thành phần chủ yếu của mô hình PKI, bao gồm:

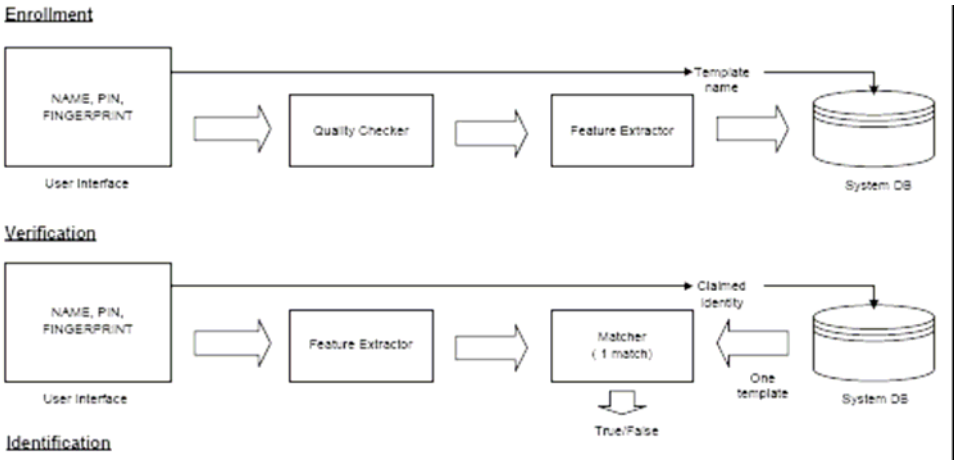
- Bộ phận thẩm quyền xác thực và cấp chứng chỉ (CA)
- Bộ phận thẩm quyền đăng ký (RA)
- Hệ thống phân phối, quản lý chứng chỉ số - chứng thư số (Certificate)
- Lưu trữ chứng chỉ số (CR)
- Người dùng trong hệ thống (user)

• Các hoạt giao dịch cơ sở trong hệ thống PKI bao gồm:

- Đăng ký người dùng
- Xin cấp chứng chỉ
- Cấp phát và quản lý chứng chỉ số
- Gia hạn hay hủy bỏ chứng chỉ số
- Thực hiện cơ chế sử dùng chứng chỉ số, xác thực chữ ký số

4.3.2. Hệ thẩm định xác thực sinh trắc vân tay trực tuyến

Hệ thống thẩm định xác thực sinh trắc dựa trên mô hình cơ bản dưới đây:



Hình 4.7. Mô hình hệ thống thẩm định xác thực sinh trắc

Theo mô hình này hệ thống sinh trắc của hệ BioPKI dùng sinh trắc vân tay sống được lấy trực tuyến từ thiết bị scanner. Hoạt động của hệ thống sinh trắc gồm 2 phân hệ chức năng hoạt động bao gồm:

- Pha đăng ký sinh trắc (Enrollment):
  - Đăng ký người dùng
  - Lấy dấu vân tay sống trực tuyến từ thiết bị
  - Xử lý ảnh trích chọn đặc trưng
  - Mã hóa
  - Lưu trữ đặc trưng
- Pha xác thực và thẩm định (Verification and Authentication):
  - Lấy dấu vân tay sống trực tuyến từ thiết bị
  - Xử lý ảnh trích chọn đặc trưng
  - Đối sánh thẩm định trực tuyến (online) xác thực vân tay của chủ thể người dùng

4.3.3. Mô hình tích hợp hệ sinh trắc vào hạ tầng khóa công khai thành hệ BK-BioPKI

Trên cơ sở nghiên cứu các hướng tiếp cận BioPKI như đã phân tích trong phần 4.2, đề tài nghiên cứu đề xuất mô hình tích hợp hệ thống kết hợp giải pháp 1 và giải pháp 2. Mô hình mức khung cảnh được trình bày trong hình 4.6, bao gồm:

- Hệ thống lõi PKI trên cơ sở kiến trúc CA đơn được xây dựng trên cơ sở bộ thư viện mở OpenSSL và ngôn ngữ C++ với Windows 2003. Trung tâm xác thực CA server đảm nhiệm các chức năng cơ bản của CA hệ PKI. Trong giai đoạn hiện tại trong hệ thống RA có vai trò quản lý người dùng, lưu trữ khóa cá nhân được bảo mật bằng sinh trắc vân tay. Toàn bộ các giao thức của các giao dịch cơ sở gữa RA và CA được thiết kế và cài đặt làm cơ sở để tích hợp hệ sinh trắc tạo thành hệ BioPKI.

- Hệ sinh thẩm định sinh trắc vân tay sống trực tuyến bao gồm 2 phân hệ sinh trắc: Phân hệ sinh trắc thẩm định trực tuyến vân tay người dùng (theo hướng tiếp cận giải pháp 1, gọi là *Phân hệ sinh trắc 1*); Phân hệ sinh trắc sinh khóa sinh trắc vân tay để bảo mật khóa cá nhân của người dùng trong hệ thống (theo hướng tiếp giải pháp 2 gọi là *Phân hệ sinh trắc 2*). Hệ sinh trắc được tích hợp vào hệ BioPKI tại máy user và được quản lý bởi RA và xác thực bởi CA, chi tiết của mô hình tích hợp sẽ được trình bày trong chương 5 và chương 7.

4.4. Giải pháp công nghệ thiết kế và triển khai hệ thống BK-BioPKI

4.4.1. Cấu hình mạng hệ thống và thiết bị

- Cấu hình mạng cục bộ cho hệ thống BK-BioPKI trong giai đoạn này bao gồm một máy Server và các máy Client (users) kết nối hoạt động trong môi trường mạng tác nghiệp tại phòng thí nghiệm khoa CNTT – ĐHBK HN

- Thiết bị quét vân tay: Scaner Futronic model 9880, Futronic's FS82 USB 2.0 Fingerprint scanner with scanning window size is 16x24mm; Image resolution is 480x320 pixel, 500 DPI; Raw fingerprint image file size is 150K byte; with Live Finger Detection (LFD).

- Hệ thống lõi PKI được thiết kế trên cơ sơ bộ thư viện mã nguồn mở OpenSSL, theo chuẩn X509.

- Tất cả các máy trong phòng thí nghiệm được cài đặt môi trường lập trình Windows XP SP1, bộ công cụ lập trình Microsoft visual studio 2003, hệ quản trị cơ sở dữ liệu MySQL.

4.4.2. Nội dung xây dựng và triển khai toàn bộ các thành phần hệ thống BK-BioPKI

Toàn bộ hệ thống BK-BioPKI được thiết kế xây dựng trên cấu hình hệ thống phần cứng và lập trình toàn bộ bao gồm các thành phần hệ thống:
- Hệ thống phần mềm cơ sở BK-PKI: sẽ trình chi tiết trong chương 6
- Hệ thống phần mềm sinh trắc Fingerprint Biometric Verification: sẽ trình chi tiết trong chương 5.
- Hệ thống phần mềm tích hợp BK-BioPKI: sẽ trình chi tiết trong chương 7
- Hệ thống phần mềm các ứng dụng trong hệ thống BK-BioPKI: sẽ trình bày chi tiết trong chương 8.

4.4.3. Phương án phân tích thiết kế xây dựng hệ thống BK-BioPKI

- Mặc dù hiện tại có các phần mềm mở về hệ PKI như OpenCA, trong giai đoạn này đề tài chọn phương án: Phân tích thiết kế và xây dựng hệ thống lõi hạ tầng khóa công khai PKI theo chuẩn trên cơ sở dùng bộ thư viện OpenSSL triển khai các hoạt động giao dịch trong môi trường mạng phòng tại thí nghiệm. Với phương án này cho phép làm chủ toàn bộ hệ thống PKI đề thử nghiệm mô hình giải pháp tích hợp BioPKI.
- Phân tích thiết kế hệ thống sinh trắc của hệ BioPKI

- Đề tài đã lựa chọn dùng sinh trắc vân tay sống và xây dựng hệ thống trên cơ sở kết hợp 2 hướng tiếp cận BioPKI: giải pháp 1 và giải pháp 2 (Hệ thống sinh trắc vân tay gồm 2 phân hệ sinh trắc 1 và phân hệ sinh trắc 2 được trình bày chi tiết trong chương 5).

- Dùng thiết bị scanner USB quét vân tay thông dụng, giá thành rẻ.

- Ngôn ngữ lập trình: C++, Matlab

Các nội dung phân tích thiết kế xây dựng và cài đặt hệ thống BK-BioPKI sẽ được trình bày chi tiết trong các chương 5, 6, 7 và 8 tiếp theo đây.

Chương 5.
PHÂN TÍCH THIẾT KẾ VÀ XÂY DỰNG PHẦN MỀM HỆ THẨM ĐỊNH XÁC THỰC SINH TRẮC VÂN TAY

5.1. Hệ thẩm định sinh trắc vân tay trong hệ thống BK-BioPKI.

Về mô hình hệ thống PKI cùng với cơ chế xác thực chứng chỉ số trên cơ sở hệ mật mã khóa công khai về nguyên tắc và lý thuyết là đã đảm bảo an toàn nhờ các phương pháp mã hóa và giải mã cùng với kênh truyền thông bảo mật dùng giao thức SSL. Tuy nhiên, lỗ hổng của trong hoạt động của hệ thống PKI lại liên quan đến chính yếu tố người dùng. Thật vậy chúng ta có thể thấy được tác hại nghiêm trọng khi một người dùng đánh mất khóa cá nhân hoặc quên mật khẩu hoặc bị lộ mật khẩu để giải mã khóa cá nhân, từ đó, người dùng sẽ mất hết độ an toàn các thông tin, dữ liệu đã được mã hóa, hoặc nguy hiểm hơn, nếu họ bị kẻ xấu sử dụng trái phép khóa cá nhân để làm các bất cứ việc gì hắn muốn (sử dụng chữ ký số), và sau đó người dùng không thể từ chối được những thông tin đã được ký bằng khóa cá nhân của họ đã bị mất.

Một trong các hướng nghiên cứu để giải quyết vấn đề đó là xây dựng các giải pháp an ninh thông tin dựa trên sinh trắc học trên cơ sở kết hợp hệ xác thực sinh trắc vào hạ tầng khóa công khai PKI tạo thành hệ BioPKI. Đề tài đã nghiên cứu đề xuất giải pháp.

Hệ thẩm định xác thực sinh trắc vân tay trong hệ thống BK-BioPKI bao gồm 2 phân hệ:

- Phân hệ sinh trắc thẩm định trực tuyến vân tay người dùng (theo hướng tiếp cận giải pháp 1 về BioPKI, gọi là *Phân hệ sinh trắc 1*).
- Phân hệ sinh trắc sinh khóa sinh trắc vân tay để bảo mật khóa cá nhân của người dùng trong hệ thống (theo hướng tiếp giải pháp 2 về BioPKI, gọi là *Phân hệ sinh trắc 2*)

Mỗi phân hệ sinh trắc bản thân nó là một hệ thống thẩm định xác thực sinh trắc vân tay sống trực tuyến, bao gồm 2 quá trình hoạt động chủ yếu:

- Đăng ký (Enrollment)
- Thẩm định xác thực (Verification – Authentication)

Sau đây sẽ trình bày đặc tả hoạt động từng phân hệ sinh trắc:

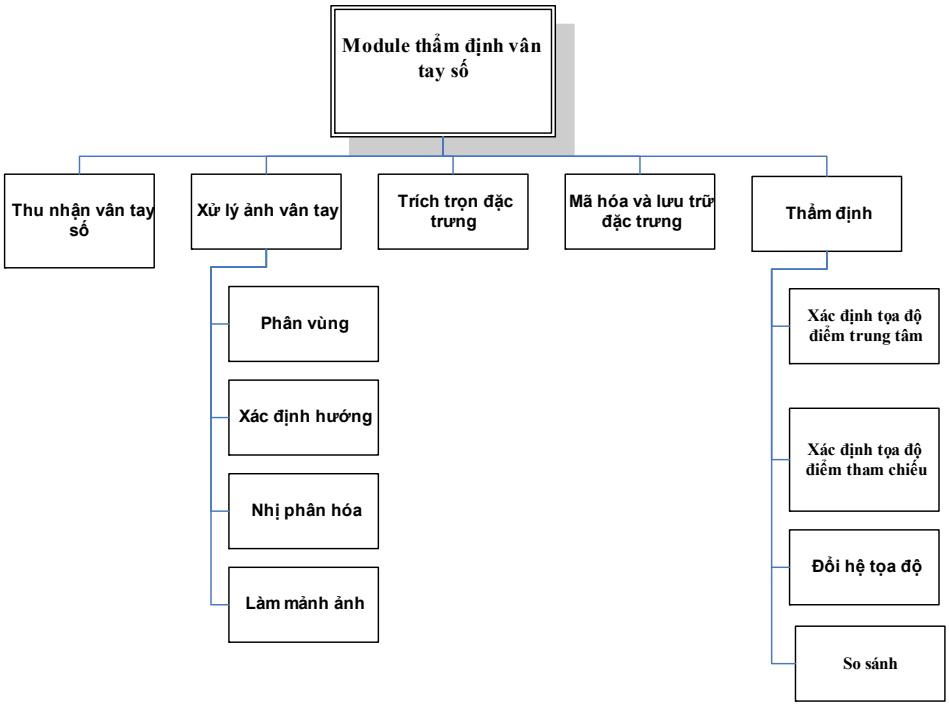
- Phân hệ sinh trắc thẩm định vân tay người dùng (*Phân hệ sinh trắc 1*): Đầu vào là vân tay sống của người dùng, người dùng cho vân tay vào thiết bị quét vân tay, ảnh vân tay được thu nhận và xử lý, sau đó đặc trưng vân tay của người dùng sẽ được trích chọn. Trong quá trình kí mã (enrollment), đặc trưng vân tay được lưu vào cơ sở dữ liệu. Còn trong quá trình thẩm định, đặc trưng vân tay sẽ được đối sánh với đặc trưng đã được giải mã từ cơ sở dữ liệu, từ đó đưa ra kết quả thẩm định.
- Phân hệ sinh trắc sinh khóa sinh trắc vân tay để bảo mật khóa cá nhân của người dùng trong hệ thống (*Phân hệ sinh trắc 2*): Đầu vào là vân tay sống của người dùng,

người dùng đưa vân tay vào thiết bị quét vân tay, ảnh vân tay được thu nhận và xử lý, sau đó đặc trưng vân tay của người dùng sẽ được trích chọn. Từ đặc trưng vân tay, một tập khóa sẽ được sinh ra và tập khóa được sử dụng để mã hóa khóa cá nhân của người dùng. Khi muốn lấy khóa cá nhân ra sử dụng, người dùng cũng lại thực hiện quét vân tay, các đặc trưng sinh trắc trích chọn được sẽ được dùng để sinh ra tập khóa. Tập khóa đó sẽ được dùng để giải mã khóa cá nhân.

5.2. Phân tích thiết kế và xây dựng Phân hệ sinh trắc 1: Hệ thẩm định đặc trưng vân tay sống, trực tuyến trong hệ thống BK-BioPKI

5.2.1. Phân tích thiết kế chức năng

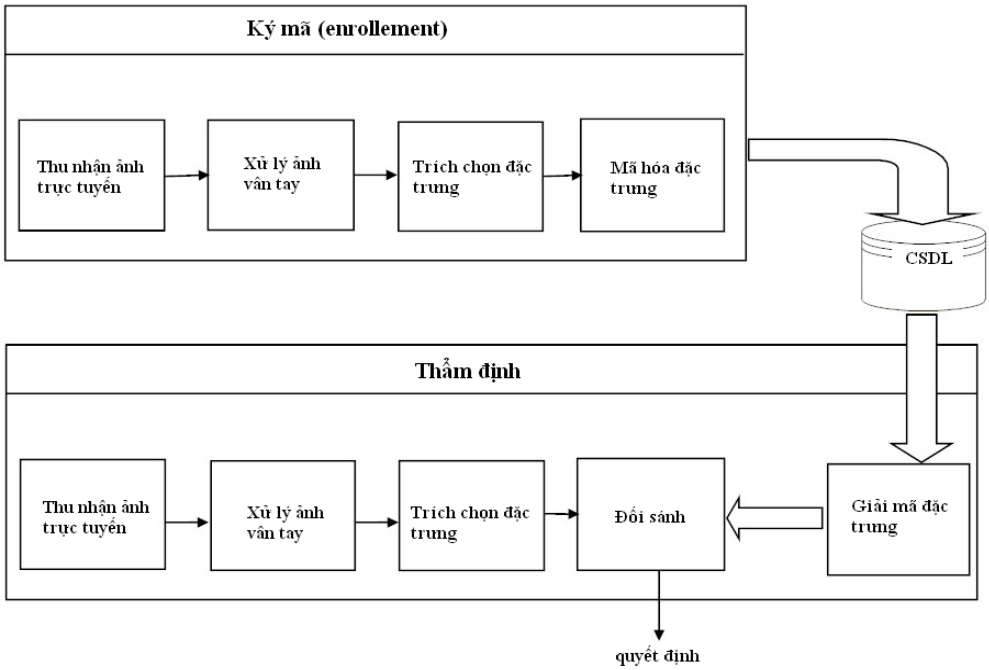
Các chức năng của Phân hệ sinh trắc 1 được biểu diễn như sau:



Hình 5.1. Biểu đồ phân cấp các chức năng của Phân hệ sinh trắc 1.

Hoạt động Phân hệ sinh trắc 1 gồm 2 quá trình:

- Đăng ký sinh trắc (Enrollment): Trong chức năng này, người dùng thực hiện quá trình đăng ký vào hệ thống, cùng với các thông tin cá nhân, vân tay số được quét trực tuyến thành ảnh, quá trình xử lý ảnh và trích trọn đặc trưng được thực hiện, đặc trưng vân tay được mã hóa và được lưu trữ lại trong CSDL tại máy người dùng.
- Thẩm định xác thực (Verification-Authentication) sinh trắc: Người sử dụng thực hiện đăng nhập vào hệ thống và quét vân tay sống trực tuyến đưa vào hệ thống. Các giai đoạn xử lý và trích chọn đặc trưng vân tay được thực hiện tương tự trong giai đoạn đăng ký (Enrollment). Việc đối sánh 2 tập đặc trưng vân tay được thực hiện trên cơ sở, một tập được trích chọn từ vân tay thu nhận trực tuyến của người dùng, tập kia được lấy trong CSDL.



Hình 5.2. Hai quá trình hoạt động chức năng của Phân hệ sinh trắc 1

Phân hệ sinh trắc 1 được tích hợp vào hệ thống BK-BioPKI ở 2 tiến trình:

- Tiến trình đăng ký người dùng:

Khi người dùng muốn đăng ký một tài khoản trong hệ thống, sau khi nhập những thông tin cá nhân cần thiết, người dùng sẽ phải thực hiện quá trình quét vân tay để hệ thống có thể lưu trữ được các đặc trưng của người dùng đó (ứng với tài khoản của người dùng vừa được tạo).

- Tiến trình đăng nhập hệ thống

Khi đăng nhập vào hệ thống, người dùng sau khi nhập username và password, sẽ phải thực hiện quét vân tay. Hệ thống sẽ thực hiện quá trình thẩm định vân tay để đưa ra quyết định có cho người dùng đăng nhập vào hệ thống hay không.

5.2.2. Phân tích chức năng và các thuật toán

5.2.2.1. Chức năng thu nhận ảnh vân tay

Chức năng này thực hiện thu nhận lấy ảnh vân tay sống từ Thiết bị quét vân tay: Scaner Futronic model 9880, Futronic's FS82 USB 2.0 Fingerprint scanner và lưu vào máy dưới dạng file ảnh Bitmap. Futronic's FS80 USB2.0 Fingerprint Scanner sử dụng công nghệ cảm biến CMOS hệ thống quang học chính xác để thu nhận ảnh vân tay, tốc độ quét của nó là 100ms. Ảnh bitmap vân tay thu được từ máy quét với các thông số kỹ thuật cụ thể như sau: “scanning window size is 16x24mm; Image resolution is 480x320 pixel, 500 DPI; Raw fingerprint image file size is 150K byte; with Live Finger Detection (LFD)”

Sau khi thiết bị được kích hoạt, chương trình sẽ tạo ra một tiến trình chạy liên tục kiểm tra tín hiệu thu nhận được từ USB, nếu tín hợp lệ sẽ bắt đầu thu nhận dữ liệu do thiết bị trả về

bằng cách gọi các hàm API trong thư viện. Kiểm tra dữ liệu lấy về và đưa ra thành định dạng file Bitmap hiển thị lên màn hình. Tiến trình này liên tục quét dữ liệu nhận được từ USB, do đó khi thực hiện thu mẫu hay thẩm định thì phải tạm dừng tiến trình để đảm bảo dữ liệu không bị sai lệch

Hình 5.3. Thiết bị scaner Futronic's FS80 USB 2.0

Hình 5.4. Ảnh vân tay thu được từ thiết bị (*.bmp)

5.2.2.2. Chức năng xử lý ảnh vân tay và trích chọn đặc trưng

Đây là chức năng quan trọng nhất, nó quyết định sự chính xác của chương trình. Chức năng này nhận ảnh vân tay từ đầu vào và có nhiệm vụ xử lý để có thể trích chọn được đặc trưng. Toàn bộ công cụ phần mềm xử lý ảnh vân tay của chức năng được phân tích thiết kế và lập trình cài đặt bằng ngôn ngữ C++ trong môi trường Windows 2003. Trong phần dưới đây sẽ trình bày chi tiết về phân tích và xây dựng bộ công cụ phần mềm xử lý ảnh vân tay.

Khối chức năng xử lý ảnh vân tay gồm các chức năng [10,15]:

- Phân vùng ảnh vân tay: phân ra vùng quan tâm và vùng không quan tâm trong xử lý
- Xác định hướng cho mỗi điểm ảnh: tính hướng cho mỗi điểm ảnh sau đó tính hướng cho khối chứa điểm ảnh và đặt lại hướng mỗi điểm ảnh thành hướng của khối.
- Nhị phân hóa dựa theo hướng thu được.
- Làm mảnh ảnh nhị phân

a) Phân vùng ảnh

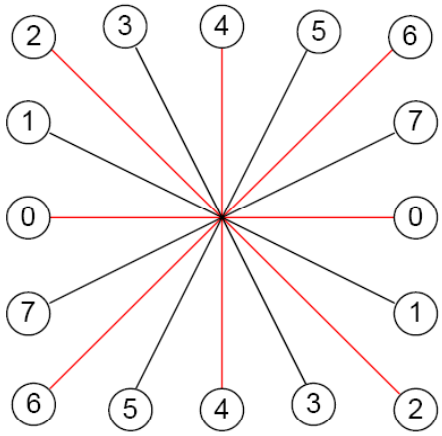
Giai đoạn này thực hiện việc phân vùng ảnh vân tay sao cho có thể loại đi những vùng không quan tâm. Chương trình sử dụng một thuật toán khá hiệu quả. Ý tưởng phân vùng như sau:

- Chia ảnh thành các khối điểm ảnh (bigPoint). Khối này có kích thước 3x3 với ảnh kích thước nhỏ và 7x7 với ảnh kích thước lớn.
- Xét xem mỗi khối điểm ảnh có thuộc vùng quan tâm hay không theo điều kiện: nếu khối 3x3 thì nó sẽ thuộc vùng quan tâm nếu có ít nhất 1 điểm ảnh trong khối là đen. Nếu khối 7x7 phải có ít nhất 6 điểm ảnh là điểm đen 15%).
- Việc xét các khối điểm ảnh được xuất phát từ tâm của ảnh (phần lớn cũng là tâm của vùng chứa vân), loang ra biên của vùng đó để đánh dấu những điểm thuộc vùng chứa vân.

Hình 5.5. Ảnh vân tay ban đầu và ảnh đã phân vùng

b) Xác định hướng của các điểm ảnh.

Có nhiều phương pháp tính hướng của điểm ảnh. Một trong số những phương pháp quen thuộc hay được sử dụng là phương pháp của Lin Hong [20] dựa trên tính các đạo hàm gradient bậc một theo hai hướng ngang, dọc của ảnh. Tuy nhiên phương pháp này có khối lượng tính toán khá lớn. Ở đây áp dụng một phương pháp được đề nghị trong bài báo [14] cho phép ước lượng hướng đơn giản với khối lượng tính toán nhỏ hơn nhiều mà độ chính xác cũng tương đương. Chương trình thực hiện thuật toán này sử dụng các trình bày như hình vẽ sau, vị trí một điểm ảnh được ước lượng rơi vào một trong 8 hướng chia bởi các đường thẳng cách đều nhau một góc 22.50



Hình 5.6. ***Hướng của các điểm ảnh***

Thủ tục xác định hướng của điểm ảnh:

```
void SetOrient()
{
        Orient[0].dong=0;Orient[0].cot=1;
        Orient[1].dong=-1;Orient[1].cot=1;
        Orient[2].dong=-1;Orient[2].cot=0;
        Orient[3].dong=-1;Orient[3].cot=-1;
        Orient[4].dong=0;Orient[4].cot=-1;
        Orient[5].dong=1;Orient[5].cot=-1;
        Orient[6].dong=1;Orient[6].cot=0;
        Orient[7].dong=1;Orient[7].cot=1;
}
```

Một điểm ảnh có thể nằm trên một đường vân, hoặc nằm trên một rãnh nào đó. Do vậy, ta quy ước hướng của điểm ảnh là hướng của đường vân (nếu nó nằm trên đường vân) hoặc hướng của rãnh trong trường hợp ngược lại. Để xác định hướng của mỗi pixel, trước hết ta tính giá trị xám trung bình G[i] của mỗi hướng i (i = 0,1,..,7) trong cửa sổ 9×9 với tâm là điểm đang xét theo công thức:

- G[0] = (G[4,0] + G[4,2] +G[4,6] +G[4,8]) / 4;
- G[1] = (G[2,0] + G[3,2] +G[5,6] +G[6,8]) / 4;
- G[2] = (G[0,0] + G[2,2] +G[6,6] +G[8,8]) / 4;
- ..

với G[i,j] là giá trị mức xám tại điểm có tọa độ (i,j) ứng với mỗi cửa sổ.

Tám hướng này được chia thành 4 nhóm, mỗi nhóm 2 hướng vuông góc nhau: nhóm j (j = 0,1,2,3) chứa hướng j và j + 4. Giá trị tuyệt đối của sự khác của mức xám trung bình trong mỗi nhóm được tính như sau:

$G_d[j] = | G[j] - G[j+4]|$ (j = 0,1,2,3)

Sau đó ta chọn nhóm có giá trị khác nhau lớn nhất, nếu:

$$i_{Max} = \arg\{ \underset{i = 0,1,2,3}{\text{Max}} (G_d[i]) \}$$

(trong đó $\arg (G[i]) = i$)

thì cả hai hướng i_{Max} và i_{Max}+4 đều được xem xét. Hướng của pixel được tính bởi:

$$D_i = \begin{cases} i_{Max} \text{ nếu } (|Grey - G[i_{Max}] < Grey - G[i_{Max+4}]) \\ i_{Max} + 4 \text{ ngược lại} \end{cases}$$

(trong đó Grey là mức xám tại pixel đang xét).

c) Nhị phân hóa ảnh.

Phần này trình bày thuật toán nhị phân hóa ảnh dựa trên hướng của các điểm ảnh. Nhị phân hóa được thực hiện dựa trên hướng được đánh giá là hiệu quả nhất.

Quá trình nhị phân hóa được thực hiện như sau:

Với pixel có hướng i đã xác định được ở trên, ta tính giá trị xám trung bình theo hướng i và hướng i + 4, giả sử chúng là G[i] và G[i + 4]. Ta nhị phân hóa pixel đó băng việc lấy trung bình độ xám đó rồi so sánh với ngưỡng, nếu hơn thì ta cho mức xám đó nhận giá trị 255 còn nhỏ hơn thì nhận là 0.

Hình 5.7. Ảnh hướng và ảnh vân tay đã nhị phân hóa

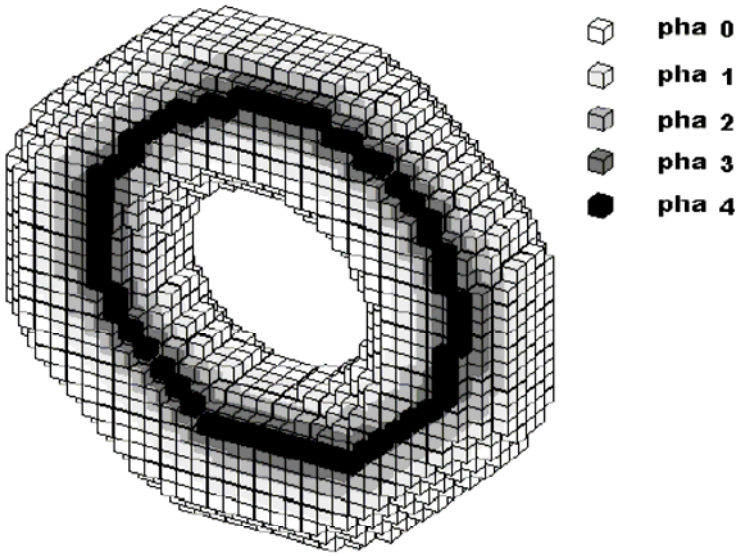
d) Giải thuật làm mảnh ảnh

Khái niệm làm mảnh được hiểu là với mỗi đường vân trích chọn được ta sẽ thu mảnh nó lại đến khi nó chỉ có độ dày là 1 pixel. Đường vân đã được làm mảnh gọi là xương. Giải thuật làm mảnh thực chất là giải thuật tìm xương đối tượng được trình bày ở phần 3.3.6 chương 3. Ta sẽ thực hiện bằng cách dựa trên biên của đối tượng, theo đó ta sẽ bóc dần các

lớp biên từ ngoài vào trong cho đến khi không còn bóc thêm được nữa thì dừng. Phần còn lại của quá trình này là xương của đối tượng.

Các giải thuật xử lý ảnh nhị phân và lam mảnh ảnh vân tay được áp dụng và lập trình trên cơ sở các giải thuật cơ bản đã trình bày trong các tài liệu đã đăng tải [10].

Tiến trình làm mảnh ảnh được minh họa như sau:



Hình 5.8. Quá trình làm mảnh ảnh

Thuật toán làm mảnh ảnh tổng quát: Tiến hành dò biên một đối tượng, với mỗi điểm biên tìm được, kiểm tra điều kiện xóa của điểm này. Cứ thế tiếp tục cho tới khi không còn điểm nào được xóa cả, điều kiện kiểm tra một điểm có bị xóa hay không sẽ tương ứng với một thuật toán. Một số qui ước và ký hiệu: cặp 4 (8) – láng giềng đối xứng; điểm xương. P là một điểm ảnh, đánh dấu với 8 điểm lân cận P theo thứ tự P0 đến P7.

P_3	P_2	P_1
P_4	P	P_0
P_5	P_6	P_7

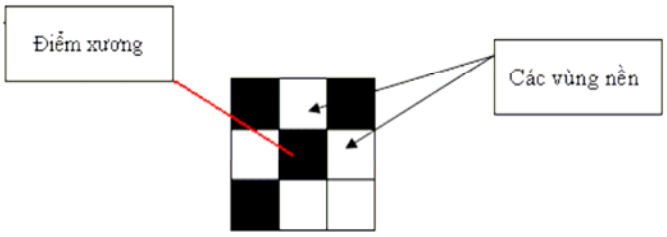
Hình 5.9. Các điểm lân cận (kề) của điểm ảnh P

Cặp 4 lân cận: N2 = {(P0, P4); (P2, P6)}

Cặp 8 lân cận: là N4 = N2 U {(P1, P5),(P3, P7)}

Điểm biên**:** một điểm được gọi là điểm biên nếu ở đó có sự thay đổi đột ngột về mức xám. Trong ảnh nhị phân vân tay, điểm biên đen mà trong 8 láng giềng của nó có ít nhất một điểm trắng.

***Điểm xương*:** Một điểm ảnh là điểm xương khi nó là điểm có nhiều hơn hai vùng - nền không gần nhau trong 8 – láng giềng. Như vậy tại một điểm biên chúng ta chỉ cần quét xung quanh các điểm láng giềng và đếm số lần thay đổi màu nền của các điểm láng giềng này so với màu nền. Nếu số lần thay đổi này lớn hơn 2 thì điểm biên đang xét là điểm xương.



Hình 5.10. Điểm xương và vùng nền.

Các bước của thuật toán làm mảnh được tiến hành như sau:

- Bước 1: Dò biên theo thuật toán dò biên chuẩn.
- Bước 2: Với mỗi đường biên, kiểm tra điểm biến có là điểm xương không? Nếu không là điểm xương thì đánh dấu điểm đó để xóa về sau.
- Bước 3: Xóa những điểm đã được đánh dấu
- Bước 4: Kiểm tra điều kiện dừng. Nếu không còn điểm biên nào được đánh dấu xóa thì dừng, ngược lại thì quay lại bước 1.

Theo thuật toán này thì các đối tượng ảnh lần lượt bị bóc dần các lớp biên, cuối cùng thu được dạng biểu diễn cấu trúc của đối tượng.

e/ Trích chọn đặc trưng.

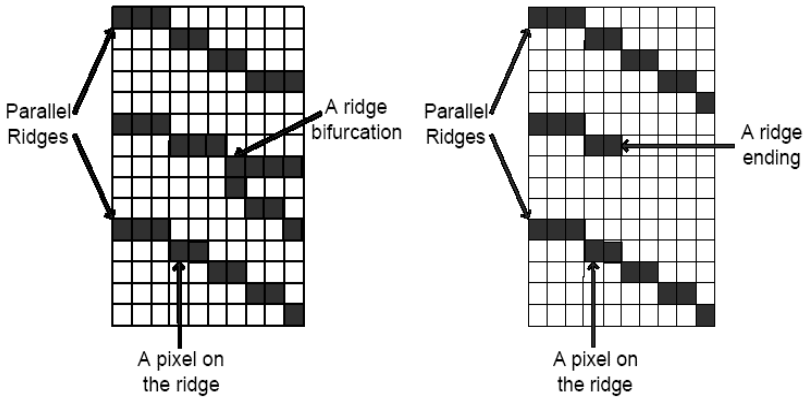
Sau khi xử lý ảnh vân tay và làm mảnh ảnh chúng ta thu được ảnh vân tay ở dạng ảnh xương, dựa vào đó, có thể trích chọn một cách dễ dàng các điểm đặc trưng mà chúng sẽ làm cơ sở cho chức năng thẩm định.

Các điểm đặc trưng được xác định nhờ các thuộc tính sau [4]:

- Điểm kết thúc: số điểm đen lân cận là 1
- Điểm rẽ nhánh: số điểm đen lân cận là 3,

Thông tin về mỗi điểm đặc trưng bao gồm:

- Tọa độ của điểm đặc trưng (x, y)
- Hướng của điểm đặc trưng
- Kiểu của điểm đặc trưng (điểm kết thúc hay rẽ nhánh)



Hình 5.11. Điểm rẽ nhánh và điểm dừng

Các bước thuật toán trích chọn đặc trưng và đối sánh [4]*:*

Bước 1: Tìm tọa độ điểm trung tâm vân tay.

Với mỗi tập điểm minutiae trích chọn được ta tính khoảng cách trung bình từ một điểm minutiae tới tất cả các điểm còn lại và chọn ra điểm minutiae có giá trị nhỏ nhất trong số đó

Khoảng cách trung bình từ điểm minutiae (x_i , y_j) đến tất cả các điểm minutiae còn lại được tính là:

$$d_j = \frac{1}{n-1} \cdot \sum_{k=\{1,2,..,n\}\setminus j} \sqrt{|x_j - x_k|^2 + |y_j - y_k|^2}$$

Trong đó n là số điểm minutiae của tập, (x_j , y_j) là tọa độ của điểm minutiae thứ j trong tập. Sau đó ta sẽ chọn ra điểm có khoảng cách trung bình nhỏ nhất.

δ = min *(d1, d2, … , dn)*

Điểm này là trung tâm vân tay. Trong trường hợp có từ hai khoảng cách nhỏ nhất trùng nhau trở lên thì điểm được chọn sẽ là điểm đầu tiên theo thứ tự duyệt. Thử nghiệm cho thấy nếu số điểm minutiae giả ít thì trung tâm vân tay tính được là ổn định.

Bước 2: Xác định điểm đặc trưng tham chiếu.

Điểm minutiae tham chiếu ký hiệu là μR. Đây là điểm có vị trí gần trung tâm vân tay nhất. (chính là điểm trung tâm vân tay nếu tính theo cách 1). Điểm này được xác định theo phương trình [4]:

$$\mu_R = \left(\mu_m \middle| m \longleftarrow \min\left(\sqrt{|C_x - x_i|^2 + |C_y - y_i|^2} \right), i = 1...n_\mu \right)$$

Với [C_x, C_y] là tọa độ điểm trung tâm vân tay. Tọa độ của điểm minutiae tham chiếu này là [X_R, Y_R]

Bước 3: Chuyển hệ tọa độ.

Đầu tiên ta chuyển hệ tọa độ cực. Ta gọi hệ tọa độ cũ là CSold. Gốc tọa độ của CSold là góc trên bên trái của ảnh, điểm [0,0]. Hệ tọa độ mới gọi là CSnew có gốc tọa độ tại điểm minutiae tham chiếu μR. Phép chuyển đổi giữa hai hệ trục tọa độ này có thể được thể hiện như sau [4]:

$$T: Cs_{old} \longrightarrow Cs_{new} \mid \; O^x_{new} = O^x_{old} + x_R \;\&\; O^y_{new} = O^y_{old} + y_R$$

Gốc tọa độ của hệ tọa độ mới sẽ là [X_R, Y_R]. μT là tập điểm minutiae, tọa độ của các điểm minutiae được tính lại như sau:

$$\mu^T = \left\{ \mu_i \middle| \mu_i = \left(x_i - x_R, y_i - y_R\right), i = 1...n \right\}$$

Tiếp theo sắp lại trật tự các điểm minutiae còn lại. Khoảng cách giữa gốc tọa độ và các điểm minutiae khác được tính trước:

$$d_t^T = \sqrt{\left|x_R - x_i^T\right|^2 + \left|y_R - y_i^T\right|^2}, i = 2...n_\mu$$

Các điểm minutiae μ_i được sắp lại dựa trên khoảng cách tới gốc tọa độ và sẽ được đặt chỉ số mới:

$$\mu^{T'} = \left\{ \mu_i^{T'} \middle| d_i \le d_{i+1}, i = 2....n_\mu \right\}$$

Như vậy: điểm minutiae đầu tiên là điểm minutiae tham chiếu, điểm thứ hai là điểm minutiae gần nhất với điểm minutiae tham chiếu, cứ tiếp tục như vậy,.. Tiếp theo là hiệu chỉnh xoay cho trong UT. Góc quay được tính như sau:

$$\alpha = \frac{\pi}{2} - \arccos\left\{ \frac{\left|x_2^{T'}\right|}{\sqrt{\left|x_2^{T'}\right|^2 + \left|y_2^{T'}\right|^2}} \right\}$$

Góc α là góc giữa trục x và hệ tọa độ từ điểm minutiae tham chiếu đến điểm minutiae thứ hai. Dùng góc α, ta có thể quay toàn bộ các điểm minutiae:

$$\mu_i^{T''} = \left\{ \mu_i^{T''} \middle| \mu_i^{T''} = (x_i^{T''}, y_i^{T''}, \phi_i^{T''}, t_i), i = 2...n_\mu \right\}, \text{ với}$$

$$x_i^{T''} = x_i^{T'}.\cos(\alpha) - y_i^{T'}.\sin(\alpha)$$

$$y_i^{T''} = x_i^{T'}.\sin(\alpha) + y_i^{T'}.\cos(\alpha)$$

$$\phi_i^{T''} = (\alpha + \phi_i) \bmod 2\pi$$

Như vậy, toàn bộ các điểm minutiae đã được sắp xếp lại và quay để tạo thành một tập điểm minutiae có tọa độ mới.

Bước 4: So sánh hai tập điểm đặc trưng. Sau khi chuyển đổi hệ tọa độ ta được 2 tập điểm minutiae là tập mẫu và tập so sánh [4]

$$\mathbf{T}=\{\mathbf{m}_1,\mathbf{m}_2,...,\mathbf{m}_m\},\quad \mathbf{m}_i=\{x_i,y_i,\theta_i\},\quad i=1..m$$
$$\mathbf{I}=\{\mathbf{m}'_1,\mathbf{m}'_2,...,\mathbf{m}'_n\},\quad \mathbf{m}'_j=\{x'_j,y'_j,\theta'_j\},\quad j=1..n,$$

Lần lượt đọc 2 tập điểm đó và tính độ lệch về khoản cách và góc, nếu nhỏ hơn ngưỡng cho phép thì chấp nhận.

$$sd(\mathbf{m}'_j,\mathbf{m}_i)=\sqrt{(x'_j-x_i)^2+(y'_j-y_i)^2}\ \le r_0,$$
$$dd(\mathbf{m}'_j,\mathbf{m}_i)=\min\left(\left|\theta'_j-\theta_i\right|,360^\circ-\left|\theta'_j-\theta_i\right|\right)\ \le\theta_0$$

Cuối cùng là tính tổng số điểm hợp lệ trên tổng số điểm đã duyệt, nếu lên hơn ngưỡng thì cho phép. Ngưỡng ở đây là tự đặt phụ thuộc và mức độ chính xác của thuật toán và chất lượng ảnh vân tay, ngưỡng càng lớn thì càng bảo mật nhưng khả năng từ chối lại cao, còn nếu nhỏ quả thì khả năng nhận nhầm tăng lên.

g/ Mã hóa lưu trữ đặc trưng và thẩm định

Sau khi đã trích chọn đặc trưng, sẽ thực hiện mã hóa các đặc trưng đó bằng thuật toán Blowfish mã hóa với khóa đối xứng và được lưu giữ và bảo mật cá nhân. Người dùng được quyền chọn lựa khóa mã để mã hóa, một giải pháp đơn giản là khóa đối xứng được chọn chính là password của người dùng.

Khi xác thực, các đặc trưng sinh trắc sống lấy trực tiếp từ thiết bị quét vân tay, qua quá trình xử lý như đã trình bày ở trên, các đặc trưng vân tay sống sẽ được xác thực bởi quá trình đối sánh với mẫu đã lấy trong quá trình đăng ký. Tuy nhiên trên thực tế không thể lấy được 2 ảnh vân tay hoàn toàn đồng nhất của cùng một người, đây là vấn đề khó chủ yếu của quá trình xác thực thẩm định sinh trắc. Khó khăn này luôn tồn tại thực tế bởi các nguyên nhân sau:

- Sự dịch chuyển: Cùng một ngón tay nhưng người sử dụng lại đặt vào các vị trí khác nhau trên máy quét dẫn đến các kết quả khác nhau. Với máy scaner USB thì chỉ cần dịch chuyển 2mm cũng đã dẫn đến lệch khoản 30 pixel trên ảnh vân tay
- Quay: Cùng một ngón tay, một vị trí nhưng lại xoay theo nhiều hướng khác nhau và do đó ảnh vân tay cũng bị quay một góc tương tự
- Méo do phép chuyển đổi phi tuyến: Như ta đã biết, ngón tay là vật thể 3 chiều khi máy scaner quét, nó phải chuyển thành ảnh 2 chiều thông qua một phép biến đổi phi tuyến, do đó sẽ dẫn đến việc cùng một ngón tay và vị trí nhưng độ nghiêng cũng như vị trí cao thấp của ngón tay so với bề mặt quét dẫn đến ảnh thu được lại khác nhau.
- Sức đè và điều kiện của da: Ảnh thu được hoàn toàn chịu ảnh hưởng của việc ấn tay vào máy quét mạnh hay nhẹ và quan trọng hơn và điều kiện của da. Da ẩm, khô hay sạch, bẩn đều gây ra các kết quả khác nhau
- Nhiễu: Đây là điều mà bất kỳ hệ thống thu nhận ảnh cũng gặp phải, nó tùy thuộc và chất lượng của máy quét.

Chính vì các nguyên nhân trên đây mà nhiều các công trình đã quan tâm nghiên cứu và đề xuất, mô hình giải pháp theo hướng tiếp cận 2 cũng nhằm giải quyết vấn đề này.

5.2.3. Xây dựng và lập trình các khối chức năng Phân hệ sinh trắc 1

Trong phần này sẽ trình bày thiết kế triển khai và cài đặt lập trình Phân hệ sinh trắc 1 như đã phân tích ở trên

a/ Giao diện của phân hệ sinh trắc 1: là cửa sổ hiển thị ảnh vân tay quét trực tuyến (Hình 5.12). Với 3 nút ấn: Save, Scan và Stop, việc sử dụng phân hệ rất đơn giản, gồm:

Phím Scan: Khi người dùng ấn phím Scan, chương trình sẽ hiển thị ảnh vân tay lên cửa sổ giao diện để người dùng có thể tự đánh giá chất lượng ảnh quét.

Phím Stop: Dừng quá trình quét ảnh.

Phím Save: Chương trình sẽ thực hiện các chức năng ẩn bên trong để cuối cùng đưa ra file chứa thông tin của các điểm đặc trưng trích chọn được có tên là minutiae.txt.

b/ Cài đặt lập trình các hàm chức năng

- ***Chức năng thu nhận và lưu trữ ảnh***

Phân hệ có chức năng lưu trữ ảnh vào file trong bộ nhớ và biểu diễn ảnh lên màn hình. Phân hệ có sử dụng thư viện mã nguồn mở FreeImage (http://sourceforge.net).

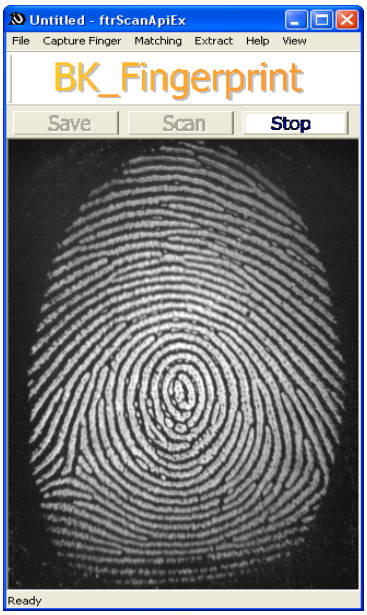
- ***Chức năng trích chọn đặc trưng***

Chức năng này bao gồm các công việc sau: phân vùng ảnh, xác định hướng, nhị phân hóa, làm mảnh ảnh và trích chọn đặc trưng.

- Phân vùng ảnh: void doSegmentImage(fipWinImage &doneImage);
- Xác định hướng các điểm ảnh: void getDirPixels(fipWinImage &doneImage);
- Nhị phân hóa: void doBinazi(fipWinImage &doneImage);
- Làm mảnh ảnh: fipWinImage doThinning(fipWinImage imageInput);
- Trích chọn đặc trưng: void takeAllMinutiaePoints(Minutiae *pt);

- ***Chức năng đối sánh ảnh:***

Chức năng này có nhiệm xác định xem 2 tập điểm đặc trưng có tương đương không: void OnVerification();



Hình 5.12. Giao diện phân hệ sinh trắc 1

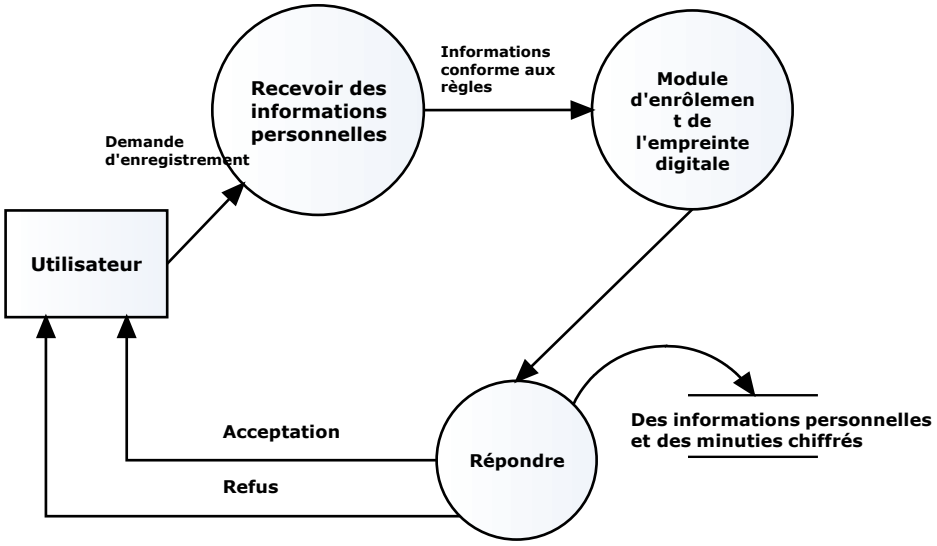
5.2.4. Thử nghiệm và kết quả.

5.2.4.1. Kịch bản thử nghiệm tích hợp phân hệ vào hệ thống

Phân hệ này được tích hợp trong tiến trình đăng ký và đăng nhập của người dùng của chương trình RA_Client. Phân hệ cũng được sử dụng trong ứng dụng bảo vệ truy cập từ xa.

- ***Tiến trình đăng ký.***

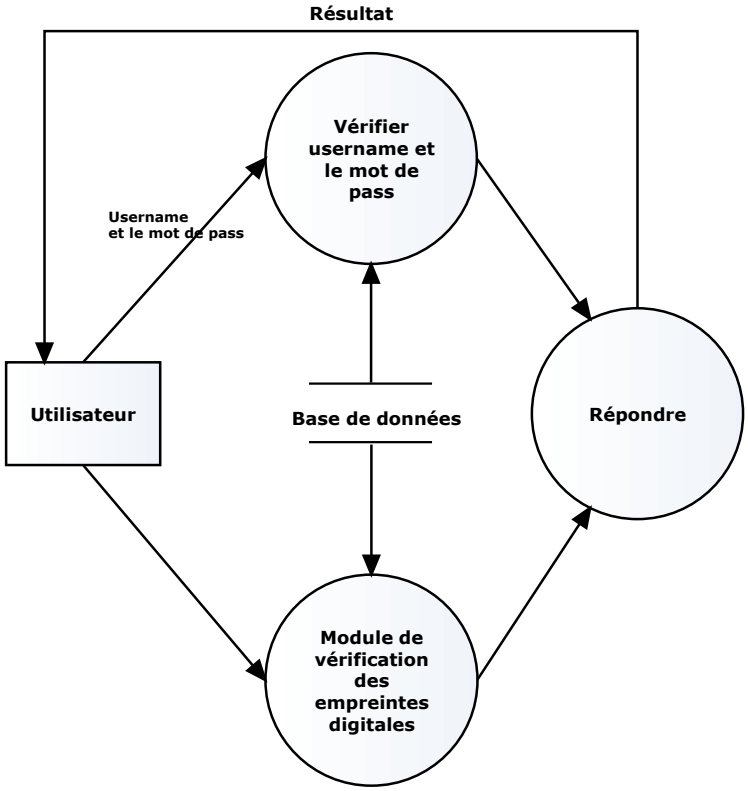
Sau khi đã điền đầy đủ thông tin cá nhân, người dùng phải quét vân tay trực tuyến. Phân hệ sẽ gọi chức năng ký mã vân tay số. Cuối cùng, thông tin về vân tay người dùng sẽ được mã hóa và lưu trữ trong CSDL của RA. Thuật toán mã hóa sử dụng là Blowfish, và khóa sử dụng để mã là password của người dùng.



Hình 5.13. Tiến trình đăng ký người dùng vào hệ thống

- ***Tiến trình đăng nhập.***

Để đăng nhập vào hệ thống, người dùng phải nhập thông tin về username, password, và phải quét vân tay sống.



Hình 5.14. Tiến trình đăng nhập hệ thống dùng vân tay

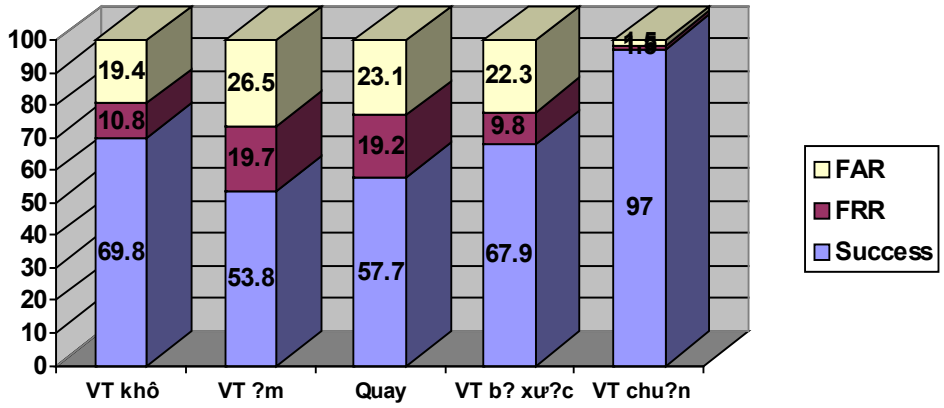
5.2.4.2. Kết quả thử nghiệm.

Để đánh giá hiệu năng cũng như độ chính xác của phân hệ, 2 quá trình thử nghiệm đã được tiến hành thử nghiệm. Đầu tiên, đó là thí nghiệm trên những mẫu ảnh vân tay có sẵn trong CSDL«Fingerprint Verification Competition 2004» từ trang web: ***http://bias.csr.unibo.it/fvc2004***. Sau đó là thí nghiệm với các vân tay sống được quét trực tuyến bởi thiết bị scanner, các vân tay của những người trong PTN của khoa CNTT- ĐH BKHN.

Mục đích của thí nghiệm là để tính ra được 3 tỷ lệ theo 3 công thức sau:

- Tỷ lệ thành công: $T_{success} = \frac{n_s}{N} \times 100\%$
- Tỷ lệ từ chối sai: $T_{FRR} = \frac{n_{FR}}{N} \times 100\%$
- Tỷ lệ chấp nhận sai: $T_{FAR} = \frac{n_{FA}}{N} \times 100\%$

Từ đó thu được biểu đồ kết quả thực nghiệm sau với các điều kiện khác nhau của vân tay:



Hình 5.15. Biểu đồ kết quả thử nghiệm thuật toán

- Nhận xét:

Qua thử nghiệm với CSDL vân tay cho thấy: vây tay ẩm đưa lại kết quả tồi nhất, vân tay khô và bị xước có kết quả chấp nhận được. Vân tay chuẩn cho kết quả tốt nhất. Yếu tố quyết định đến kết quả nhiều nhất đó là phải chọn được tập minutiae chính xác, đầy đủ.

Tồn tại những sự không chính xác này là do các lý do sau:

- Thiết bị quét vân tay hoạt động chưa thật sự hiệu quả, thiết bị khá nhạy cảm với vân tay ẩm.
- Mỗi lần quét mới chỉ thực hiện quét một lần, do vậy ứng với một người dùng, chỉ có một mẫu vân tay để đối sánh.

5.3. Phân tích thiết kế và xây dựng Phân hệ sinh trắc 2: Hệ sinh khóa sinh trắc bảo mật khóa cá nhân trong hệ BK-BioPKI.

5.3.1. Phân tích các chức năng

Vấn đề bảo vệ khóa cá nhân luôn được chú trọng vì khóa cá nhân đóng vai trò bảo mật tập trung cho toàn bộ hoạt động khác. Nếu khóa cá nhân của người dùng bị mất trộm thì đương nhiên những tài liệu mật gửi cho người dùng đó sẽ không còn an toàn. Trong trường hợp khóa cá nhân của một CA bị mất thì toàn bộ các CA và người dùng cấp dưới của nó sẽ không đảm bảo độ tin cậy, vì người lấy được khóa cá nhân đó có thể cấp chứng chỉ số cho bất kỳ một CA hay người dùng giả mạo nào đó nhân danh CA này. Nếu CA gốc bị mất khóa cá nhân thì toàn bộ hệ thống PKI trở nên vô nghĩa và sụp đổ. Có thể thấy, vấn đề bảo vệ khóa cá nhân mang ý nghĩa rất lớn.

Vấn đề xác thực và thẩm định chủ thể, điểm yếu của PKI, lại là điểm mạnh của sinh trắc học. Do đó xu thế kết hợp sinh trắc học với PKI thành BioPKI là xu thế tất yếu. Hệ thống BioPKI được xây dựng sẽ đảm bảo định danh chính xác người dùng, bảo vệ an toàn tuyệt đối khóa cá nhân, đồng thời mang lại sự tiện lợi cho người sử dụng.

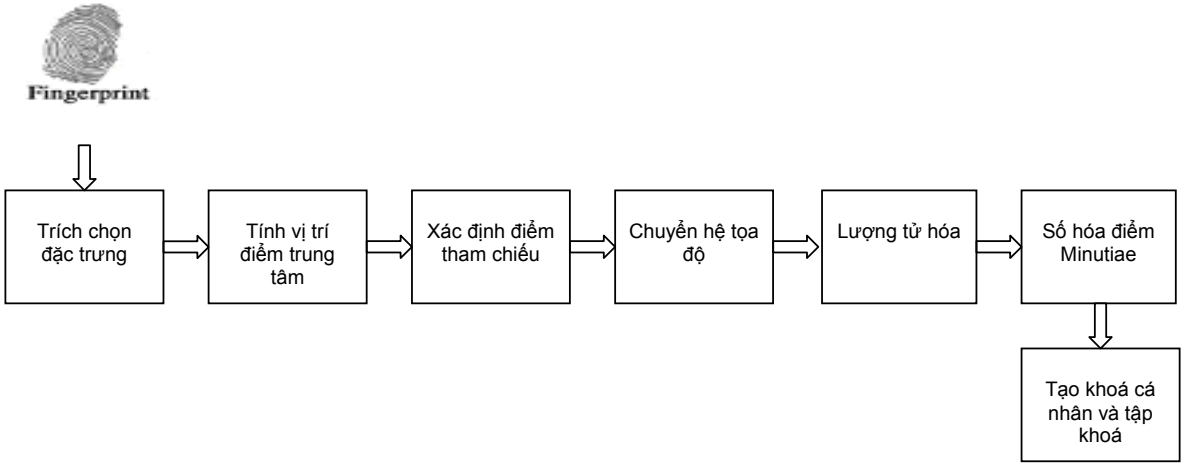
Cũng theo xu hướng đó, trong hệ thống BKBioPKI có thiết kế phân hệ sinh trắc với mục đích là thẩm định người dùng trực tuyến và bảo vệ khóa cá nhân.

Phân hệ sinh trắc 2 gồm các chức năng chính:

- Chức năng đăng ký mã: Sinh trắc học vân tay được dùng để sinh tập khóa sinh trắc, tiếp đó, tập khóa sinh trắc được dùng để mã hóa bảo vệ khóa cá nhân.
- Chức năng thẩm định xác thực sinh trắc và truy xuất khóa cá nhân: Tập khóa sinh trắc được sinh ra từ vân tay sống để giải mã khóa cá nhân.

5.3.2. Thuật toán sinh khóa từ sinh trắc vân tay

Hệ thống BK-BioPKI sử dụng thuật toán sinh khóa dựa trên thuật toán trích chọn các đặc trưng sinh trắc học vân tay gồm các điểm minutiae. Điểm minutiae là các điểm kết thúc hoặc rẽ nhánh của đường vân. Thuật toán này được xây dựng và thiết kế dựa trên tư tưởng của một luận án tiến sĩ [4] gồm các bước chính được trình bày trong sơ đồ sau:



Hình 5.16. Thuật toán sinh khóa từ sinh trắc vân tay

a/ Trích chọn tập điểm đặc trưng

Áp dụng cùng thuật toán trích chọn đặc trưng đã trình bày trong phần 5.2.2 để thu được tập điểm đặc trưng ở đây là tập điểm minutiae. Tuy nhiên để tăng cường độ ổn định đặc trưng, trong giải pháp này đã bổ sung 1 số xử lý sau:

- Người dùng N sẽ phải lấy mẫu khoảng K lần (ví dụ thực tế chọn K=5), mỗi lần một tập điểm đặc trưng – minutiae được trích chọn, sau 5 lần, chọn ra các điểm minutiae có xác suất xuất hiện cao nhất trong 5 tập đó, tập điểm minutiae cuối cùng tương đối ổn định và có độ chính xác cao với khoảng μ_{min} điểm minutiae. Quá trình chọn điểm minutiae diễn ra như sau

  - ✓ Chọn các điểm minutiae mà cùng vị trí, hướng và loại trong cả năm mẫu. Chọn các điểm gần điểm trung tâm trước.
  - ✓ Xét các điểm minutiae có vị trí trong 5 mẫu giống nhau nhưng gradient và loại lại khác nhau. Điểm minutiae sẽ được lấy khi có từ 3 trong số 5 mẫu đó giống nhau. Thứ tự chọn là chọn từ các điểm gần trung tâm chọn ra.
  - ✓ Xét các điểm minutiae có cùng gradient và loại nhưng lại có vị trí sai khác trong khoảng dung sai. Khoảng dung sai ở đây là một hình chữ nhật kích thước chọn trước. Nếu các điểm minutiae ở các mẫu có thể được đặt trong khoảng dung sai

đó thì có thể coi chúng là một và được chấp nhận. Thứ tự chọn là điểm càng gần trung tâm thì càng được ưu tiên.

- ✓ Xét các điểm minutiae giống nhau ở ít nhất 3 mẫu về vị trí hoặc hướng hoặc loại. Điểm minutiae nằm càng gần trung tâm của ảnh vân tay càng được ưu tiên.

Quá trình chọn sẽ kết thúc khi đảm bảo số điểm minutiae được trích chọn thỏa mãn μ_{min}:

$$12 < \mu_{min} \leq 70$$

Mỗi điểm minutiae được đặc trưng bởi 3 thông số quan trọng gồm vị trí, hướng và loại điểm.

$$\mu_i^j = \left(x_i^j, y_i^j, \phi_i^j, t_i^j\right)$$

Trong đó:

i là chỉ số của điểm minutiae trong lần lấy mẫu thứ i (i = 1..5),

j là chỉ số điểm minutiae thứ j trong một lần lấy mẫu với các tọa độ (x_i^j, y_i^j) hướng ϕ_i^j

loại điểm minutiae t_i^j.

Tính vị trí điểm trung tâm của vân tay dựa trên Thuật toán đếm số đường vân (Ridge Count Method) được trình bày trong [4]. Ý tưởng của phương pháp là: các đường vân có thể coi như các đường tròn đồng tâm. Điểm càng gần trung tâm thì số đường vân bao quanh nó càng nhiều. Do đó, điểm trung tâm sẽ là điểm có số đường vân bao quanh nó lớn nhất. Qua thống kê thì giao điểm của hàng cắt số đường vân lớn nhất với cột cắt số đường vân lớn nhất sẽ là điểm trung tâm. Phương pháp này tính đối với ảnh vân tay đã được làm mảnh.

Gọi RC_i là số đường vân mà một đường ngang thứ i cắt, lần lượt tính số đường vân bị cắt cho mỗi hàng ta có tập:

$$RC_{V,All} = \{RC_i \mid i = 0,\ldots, Height\}$$

Trong đó Height là số điểm của ảnh vân tay theo chiều thẳng đứng. Xét từ trái qua phải, tăng giá trị của RC_i nếu có sự chuyển tiếp từ điểm đen (giá trị mức xám là 0) sang điểm trắng (giá trị mức xám là 255)

Chọn hàng ngang chứa hoành độ của trung tâm vân có RC_V lớn nhất theo công thức:

$$RC_V = \max(RC_{V,All})$$

Một cách tương tự chọn ra hàng dọc có chứa tung độ của trung tâm vân RC_H

$$RC_{H,All} = \{RC_i \mid i = 0\ldots Width\}$$
$$\text{và } RC_H = \max(RC_{H,All})$$

Sau khi chọn được hai đường ngang và đường dọc như trên, lấy giao điểm của hai đường đó. Điểm đó chính là điểm trung tâm vân tay và có tọa độ $[C_X; C_Y]$, gọi là tọa độ trung tâm. Trên hình 5.17 minh họa một vân tay được tính số đường vân theo cách này. Điểm trung tâm là điểm giao bởi hàng dọc cắt 34 vân và hàng ngang cắt 24 vân.

Hình 5.17. Cách tính số đường vân của một vân tay

Các bước xử lý dưới đây được thực hiện như đã trình bày trong phần 5.2.2.2, bao gồm:

- Xác định điểm tham chiếu

Điểm minutiae tham chiếu được định nghĩa là điểm minutiae gần điểm trung tâm vân tay nhất Điểm minutiae tham chiếu ký hiệu là μ_R. Khoảng cách từ điểm trung tâm đến tất cả các điểm còn lại:

$$d_i = \sqrt{\left|C_x - x_i\right|^2 + \left|C_y - y_i\right|^2}, \text{với } i = \overline{1,N}$$

Trong đó:

N là số điểm minutiae trong ảnh đang xét.

x_i, y_i là tọa độ của điểm minutiae

Điểm tham chiếu là điểm có giá trị d_i min:

$$\mu_R = \left(\mu_m \middle| m \leftarrow \min\left(\sqrt{\left|C_x - x_i\right|^2 + \left|C_y - y_i\right|^2} \right), i = \overline{1,N} \right)$$

Tọa độ điểm tham chiếu là [x_R, y_R].

- Chuyển hệ tọa độ

Sau khi tính toán được điểm tham chiếu ta đã có thể dựng được hệ tọa độ mong muốn lên ảnh vân tay đang xét. Công việc tiếp theo là chuyển từ hệ tọa độ cũ sang hệ tọa độ mới này. Hệ tọa độ cũ chính là hệ tọa độ do bộ nhớ quy định: gốc [0, 0] nằm ở góc trên bên trái. Hệ tọa độ mới có gốc tại điểm minutiae tham chiếu. Sở dĩ ta chuyển sang hệ tọa độ mới này (còn được gọi là hệ tọa độ cực) là để sử dụng thuộc tính vị trí tương đối giữa các điểm minutiae ở gần điểm gốc, thuộc tính này không thay đổi nhiều với mỗi lần lấy mẫu nên có thể sử dụng để tính toán. Ta có công thức chuyển hệ tọa độ như sau:

$$T : Cs_{old} \rightarrow Cs_{new} \left| \left\{ O^x_{new} = O^x_{old} + x_R, O^y_{new} = O^y_{old} + y_R \right\} \right.$$

Gốc tọa độ của hệ tọa độ mới sẽ là [X_R, Y_R]. μ^T là tập điểm minutiae, tọa độ của các điểm minutiae được tính lại như sau:

$$\mu^T = \left\{ \mu_i \left| \mu_i = \left(x_i - x_R, y_i - y_R \right), i - \overline{1, N} \right. \right\}$$

Tiếp theo sắp lại trật tự các điểm minutiae còn lại. Khoảng cách giữa gốc tọa độ và các điểm minutiae khác được tính trước:

$$d^T = \sqrt{\left| x_R - x_i^T \right|^2 + \left| y_R - y_i^T \right|^2}, i = \overline{2, N}$$

Các điểm minutiae μ_i được sắp lại dựa trên khoảng cách tới gốc tọa độ và sẽ được đặt chỉ số mới:

$$\mu^T = \left\{ \mu^{T'} \left| d_i \le d_{i+1}, i = \overline{2, N} \right. \right\}$$

Như vậy điểm minutiae đầu tiên là điểm minutiae tham chiếu, điểm thứ hai là điểm minutiae gần nhất với điểm minutiae tham chiếu, cứ tiếp tục như vậy.

Tiếp theo, ta quay hệ tọa độ đó sao cho trục hoành đi qua điểm minutiae thứ hai. Mục đích của bước này là giảm độ ảnh hưởng của sự quay của ảnh đầu vào đến độ chính xác của thuật toán. Góc quay được tính là:

$$\alpha = \frac{\pi}{2} - \arccos\left\{ \frac{\left| x_2^{T'} \right|}{\sqrt{\left| x_2^T \right|^2 + \left| y_2^T \right|^2}} \right\}$$

Với $(x_2^{T'}, y_2^{T'})$ là tọa độ của các điểm minutiae thứ hai. Góc α là góc giữa trục x và trục hoành mới là đường thẳng nối từ điểm minutiae tham chiếu đến điểm minutiae thứ hai μ_2. Dùng góc α, ta có thể quay toàn bộ các điểm minutiae:

$$\mu_i^{T''} = \left\{ \mu_i^{T''} \left| \mu_i^{T''} = \left(x_i^{T''}, y_i^{T''}, \phi_i^{T''}, t_i \right), i = \overline{2, N} \right. \right\} \text{ với}$$

$$x_i^{T''} = x_i^{T'} \cos(\alpha) - y_i^{T'} \sin(\alpha)$$

$$y_i^{T''} = y_i^{T'} \sin(\alpha) + y_i^{T'} \cos(\alpha)$$

$$\phi_i^{T''} = \left(\alpha + \phi_i \right) \bmod 2\pi$$

Như vậy, toàn bộ các điểm minutiae đã được sắp xếp lại và quay để tạo thành một tập điểm minutiae có tọa độ mới.

b/ Sinh tập khoá sinh trắc

Thuật toán sinh trắc vân tay từ tập điểm đặc trưng đã trích chọn được xây dựng trong Phân hệ sinh trắc 2 cần thực hiện các bước các xử lý đây:

- ***Lượng tử hoá***

Để giảm yêu cầu chính xác quá cao của ảnh đầu vào và vẫn đảm bảo an toàn cho thuật toán bảo vệ khóa cá nhân, ảnh vân tay cần được chia thành các ô có kích thước bằng nhau và tọa độ của điểm minutiae sẽ được tính là vị trí của ô chứa nó [4].

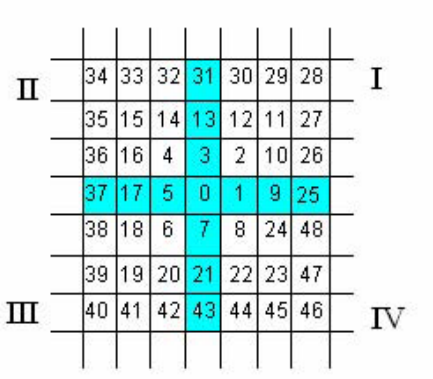
Ta chia ảnh vân tay thành các ô kích thước K_x x K_y. Số ô trên ảnh chỉ còn lại là:

$$p_k = \frac{\text{Width}}{K_x} x \frac{\text{Height}}{K_y}$$

Theo thực nghiệm cho thấy trong một hình vuông 7x7 không tồn tại hai điểm minutiae. Như vậy giá trị lớn nhất có thể lấy cho Kx và Ky là 7. Với kích thước ảnh là 512 x 512 thì số ô lượng tử tối thiểu sẽ là 16.000 ô.

Trong hệ trục tọa độ mới, đặt ký hiệu các ô quay quanh gốc tọa độ theo hình xoắn ốc. Các ô lượng tử được đánh dấu ngược theo chiều kim đồng hồ, xuất phát từ gốc là ô có số 0, tiếp theo các ô từ 1 đến 8 xếp trên hình vuông bao quanh ô gốc. Ô 9 lại tiếp tục được xếp bên phải ô 1 và việc sinh ô cứ được thực hiện tiếp tục đến khi gặp ô chứa điểm minutiae cuối cùng trong tập thì dừng lại.

Mỗi điểm minutiae sẽ rơi vào một trong các ô lượng tử trong hình xoắn ốc đó. Mỗi điểm minutiae sẽ được số hóa theo ô lượng tử tương ứng.



Hình 5.18. Hệ tọa độ các ô

- ***Số hoá điểm minutiae***

Điểm minutiae rơi vào ô lượng tử nào sẽ được thay bằng số thứ tự của ô đó. Ta giả thiết không có hai điểm minutiae nào rơi vào cùng một ô. Sau quá trình này, tập điểm minutiae trích chọn được sẽ được chuyển thành tập số.

Giả sử điểm ảnh có tọa độ đã lượng tử hoá là (k,l) thì giá trị số hoá của điểm đó là: numCoor

					(m)					
					4					
					3					
			II		2		**I**			
					1					
-5	-4	-3	-2	-1	0	1	2	3	4	(k)
					-1					
			III		-2		**IV**			
					-3					
					-4					
					-5					

Hình 5.19. Số hóa tọa đồ cực

Quá trình xác định giá trị số hoá căn cứ vào điểm đó nằm trên ô vuông bao nào, trên hình vẽ là hình vuông có cạnh 4 được tô nhạt. Điểm đầu của ô là điểm thuộc trục k có tọa độ số hoá là: *(2*chiều_dài_cạnh_ô_vuông -1)*^{2}

Tọa độ số hoá của các điểm khác ở trên ô vuông này được tính bằng cách xác định độ lệch với điểm đầu này. Sau đây là biểu thức chi tiết cho từng trường hợp.
Giá trị của numCoor được tính tuỳ thuộc vào giá trị của k và m:

- ✓ $k > m >= 0 \rightarrow numCoor = (2k-1)^2+m$
- ✓ $m >= k > 0 \rightarrow numCoor = (2m-1)^2+m + m -k$
- ✓ $m > -k >= 0 \rightarrow numCoor = (2m-1)^2+2m-k$
- ✓ $-k >= m > 0 \rightarrow numCoor = (-2k-1)^2+ 3(-k) +(-k) + (-m)$
- ✓ $-k > -m >= 0 \rightarrow numCoor = (-2k-1)^2+ 4(-k) + (-m)$
- ✓ $-m >= -k > 0 \rightarrow numCoor = (-2m-1)^2+ 5(-m) + (-m) – (-k)$
- ✓ $- m > k >= 0 \rightarrow numCoor = (-2m-1)^2+ 6(-m) + k$
- ✓ $k >= -m > 0 \rightarrow numCoor = (2k-1)^2+ 7k + k – (-m)$

- ***Tạo tập khóa sinh trắc***

Trong các điểm minutiae tìm được ta chọn ra k điểm minutiae ổn định nhất và lấy k số tương ứng trong quá trình số hóa.
Ví dụ một khoá gồm 10 điểm minutiae là:

17 27 35 50 83 99 128 142 173 193

Nếu muốn tạo ra một tập khoá thì ta sinh tổ hợp chập m của k số được Nrcombiantion phần tử. Mỗi khóa sinh trắc là m giá trị số hóa đứng cạnh nhau (theo thứ tự tăng dần) theo kiểu ghép xâu. Số khóa sinh trắc của tập là:

$$Nr_{combination} = C_k^m$$

Trong chương trình, chọn m = 5. Như vậy mỗi khoá con là một chuỗi gồm 5 số tự nhiên ghép với nhau.

5.3.3. Thiết kế phần mềm sinh khóa sinh trắc bảo vệ khóa cá nhân

5.3.3.1. Thiết kế sơ đồ khối

Sơ đồ khối các chức năng phần mềm sinh khóa sinh trắc được trình bày trong hình 5.20.

5.3.3.2. Các thuật toán

Các thuật toán thực hiện trong sơ đồ (hình 5.21) bao gồm:

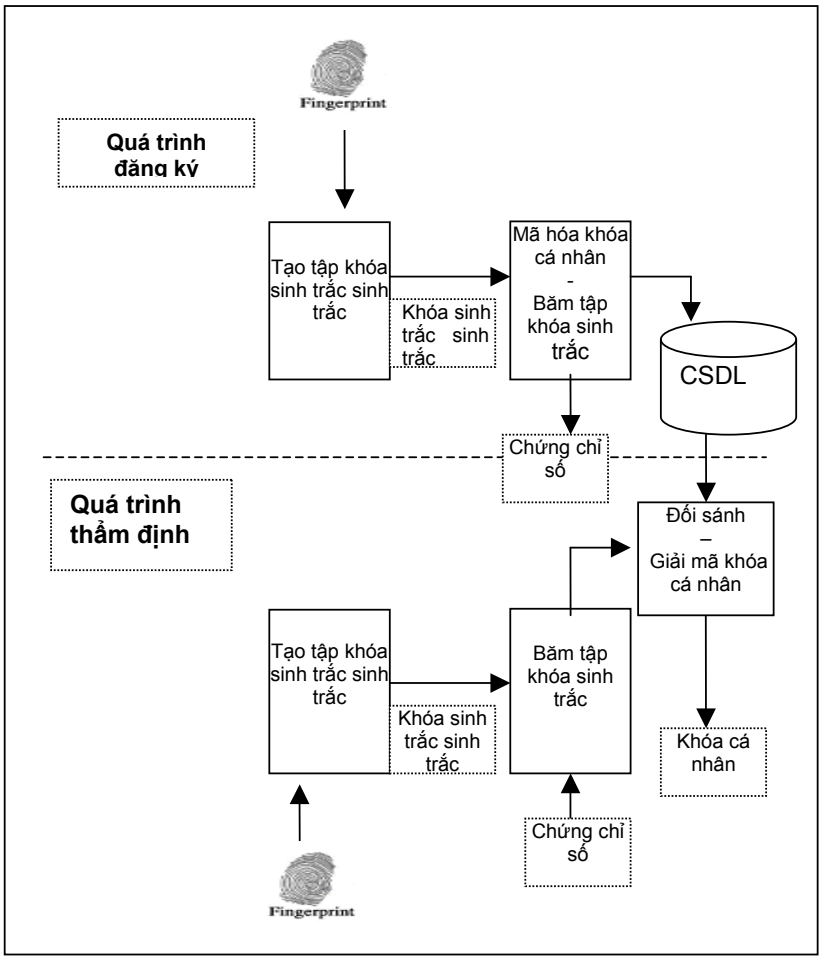
- Mã hoá khoá cá nhân bằng khóa sinh trắc
- Mỗi khóa K_r thuộc tập K dùng để mã hóa khóa cá nhân thành bản mã C

$$g : P \xrightarrow{K_r} C, C = g_{K_r}(P)$$

Từ đó dùng tập khóa K để mã hóa khóa cá nhân thành tập S có $Nr_{combination}$ các bản mã:

$$S = \left\{ g_{K_r}(P) \middle| K_r \in K, r = \overline{1, Nr_{combination}} \right\}$$

Vị trí của phần tử trong S phụ thuộc vào vị trí phần tử tương ứng trong H và K. Thuật toán mã hoá sử dụng là DES. Các thông tin sau khi mã hoá được lưu trữ trong máy của người dùng, bao gồm: khoá cá nhân đã được mã hoá và tập các khoá mã đã băm.



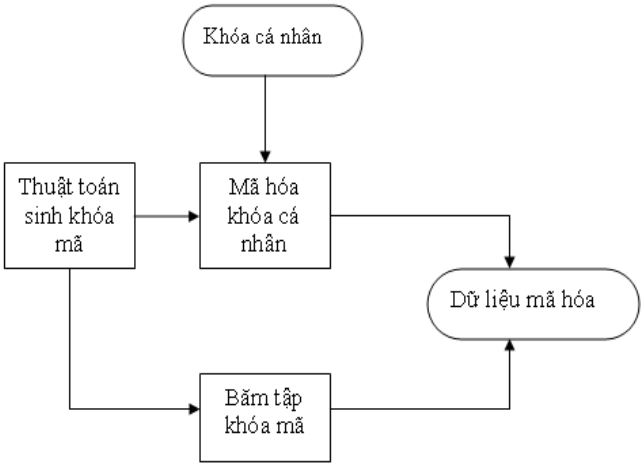
Hình 5.20. Sơ đồ khối phần mềm sinh trắc bảo vệ khóa cá nhân

Băm tập khoá

Dùng một hàm băm H thực hiện băm tập khoá K ở trên. Sở dĩ ta dùng hàm băm để đảm bảo an toàn cho khoá mã được lưu trong bộ nhớ, tránh bị truy xuất bất hợp pháp. Tập các giá trị băm như sau:

$$H = \left\{ h\left(K_r\right) \middle| K_r \in K \,\&\, r = \overline{1, Nr_{combination}} \right\}$$

Mỗi khoá mã K_r trong tập K sẽ được băm thành phần tử tương ứng $h(K_r)$, tập H cũng có $Nr_{combination}$ phần tử. Thuật toán sử dụng là MD5



Hình 5.21. Sơ đồ thuật toán mã hóa khóa cá nhân

Khối chức năng đối sánh và giải mã khóa cá nhân

Nhiệm vụ của bước này giải mã khóa bí mật bằng cách tìm ra khoá mã đã dùng để mã hoá khoá bí mật đó. Ta chú ý chỉ cần tạo ra một khoá mã từ các đặc trưng sinh trắc học vân tay và chiều dài của khoá này phải bằng với chiều dài của khoá mã được dùng để mã hoá khoá cá nhân. Ta cũng có thể tạo ra được Nrcombination các khoá mã thoả mãn điều kiện này.

Quá trình giải mã khoá cá nhân gồm 2 bước nhỏ:

Bước 1: Tìm khoá mã đã dùng để mã hoá

Đầu tiên, giá trị băm của khóa K' được tính theo hàm băm h: H'= h(K')

Ta quan tâm đến giá trị băm H' và tập các giá trị băm H chứa trong máy client và tìm trong tập H xem có giá trị H' hay không? Quá trình tìm kiếm có thể cho ra hai loại kết quả như sau:

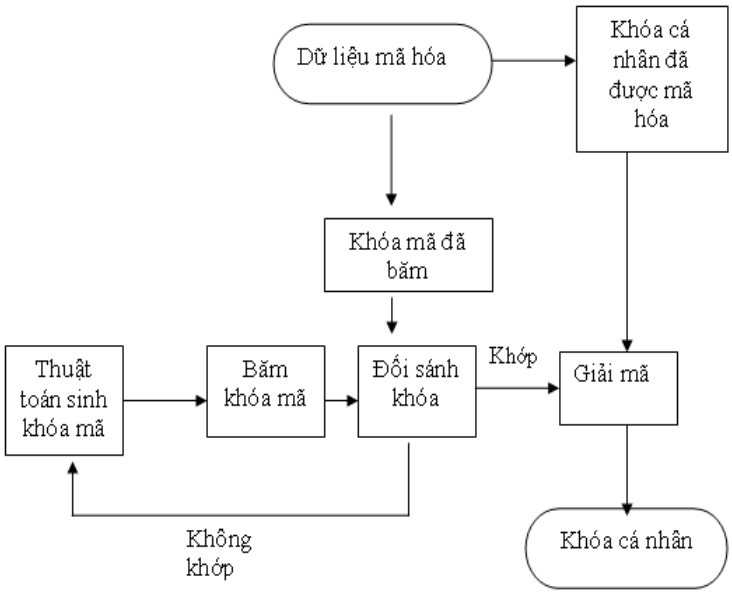
- ✓ Tìm được một giá trị băm trong H giống với H': kết quả này chỉ ra K' có thể được dùng để giải mã. Chuyển qua bước 2.
- ✓ Không tìm được: không có giá trị băm nào trong H chứa H'. Điều đó chỉ có nghĩa là khóa sinh trắc sinh ra không phù hợp. Nhưng ta vẫn có $Nr_{combination}$ khóa sinh trắc khác có thể sinh ra. Như vậy, ta phải lặp lại việc sinh khóa sinh trắc. Một khóa sinh trắc khác sẽ được sinh ra để so sánh tiếp. Quá trình sinh này được lặp lại tối đa là $Nr_{combination}$ lần. Nếu thực hiện hết $Nr_{combination}$lần mà không có một khóa sinh trắc nào phù hợp thì nghĩa là vân tay không phù hợp và việc giải mã được dừng lại. Khóa cá nhân lúc đó sẽ không thể tiếp cận được.

Bước 2: Giải mã khoá cá nhân: thực hiện tại khối giải mã.

Sau khi so sánh giá trị băm của hai khoá giống nhau, ta sẽ dùng khoá sinh trắc của giá trị băm đó để giải mã tập mã hoá khoá cá nhân trong CSDL tại máy client.

$$q : C \xrightarrow{K'} P, P = q_{K'}(C)$$

Với C là bản mã và P là khóa cá nhân ban đầu.



Hình 5.22. Quá trình giải mã khóa cá nhân

5.3.3.3. Xây dựng biểu đồ phân cấp chức năng hệ phần mềm sinh trắc

- ***Mô tả khối chức năng xử lý ảnh vân tay***

Các chức năng của khối này được mô tả trong bảng dưới đây

Chức năng	**Mô tả**
Thu nhận ảnh vân tay	Thu nhận ảnh vân tay từ cơ sở dữ liệu ảnh hoặc thu trực tiếp từ thiết bị scan
Cải thiện ảnh	Ảnh vân tay được cải thiện nhằm làm tăng chất lượng của ảnh.
Làm mảnh ảnh	Làm mảnh ảnh là bước tiền xử lý cho bước trích chọn đặc trưng ảnh
Trích chọn đặc trưng	

Bảng 5.1 Bảng mô tả các chức năng khối xử lý ảnh vân tay

Khối Xử lý ảnh được thiết kế và lập trình trong môi trường lập trình kết hợp sử dụng các thư viện mở sau với các ngôn ngữ sau:

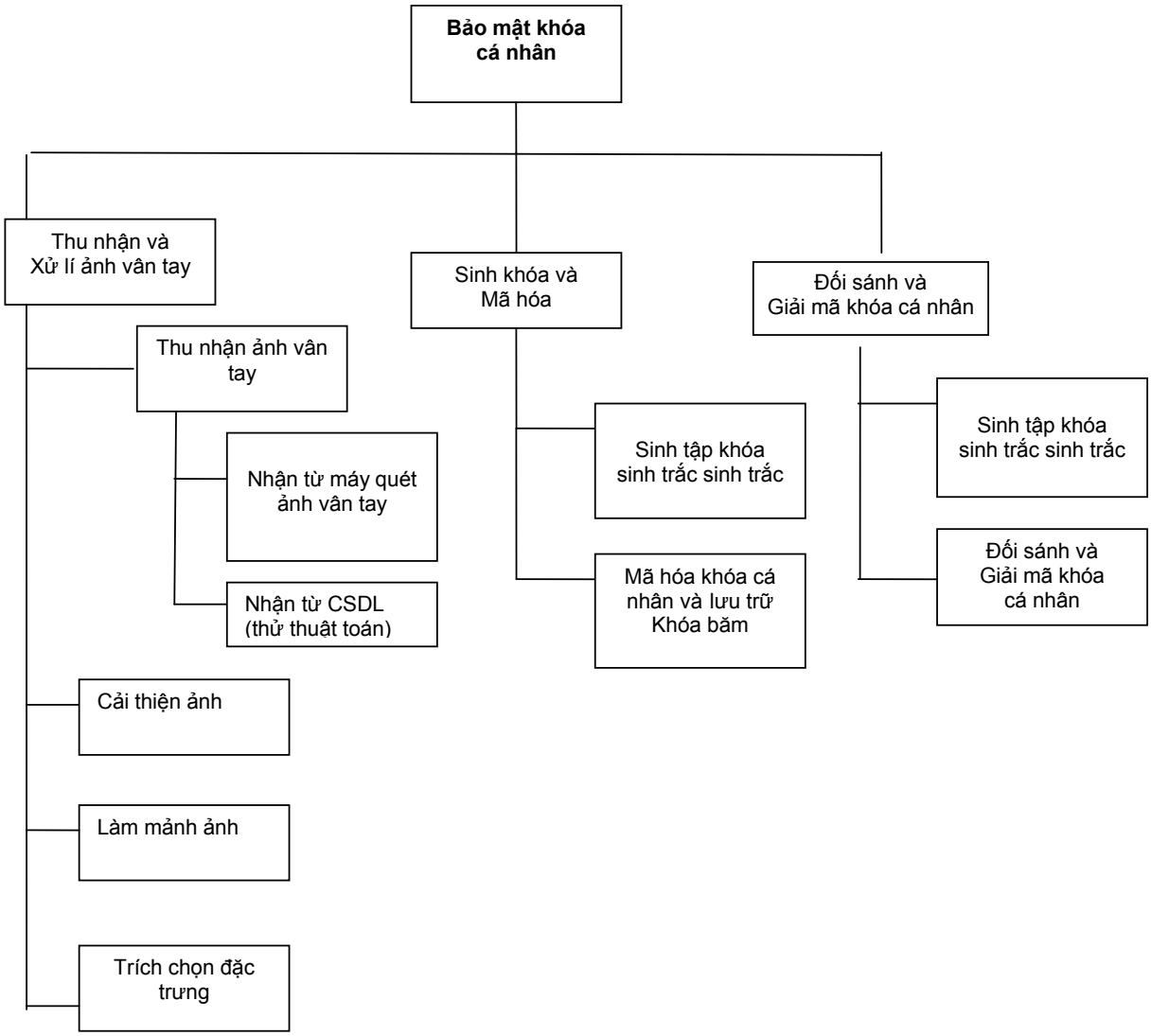
- Thư viện FreeImage hỗ trợ việc đọc và ghi các file ảnh và có hỗ trợ một số thao tác xử lý ảnh cơ bản như**:**

  - ✓ Tính toán với từng điểm ảnh
  - ✓ Thay đổi kích thước ảnh….

  Thư viện này được tham khảo tại http://freeimage.sourceforge.net . Phiên bản sử dụng trong chương trình là bản 3.9.3.0 có hỗ trợ cho ngôn ngữ Visual C++ 2003.

- Thư viện OpenSSL hỗ trợ các hàm mã hóa bảo mật và giải mã truy xuất khóa cá nhân

- Ngôn ngữ Visual C++ 2003 và Matlab.



Hình 5.23. Biểu đồ phân cấp chức năng hệ phần mềm sinh trắc

- ***Thiết kế cài đặt lập trình các chức năng***

- *Chức năng thu nhận*: Đầu vào của Môđun này là ảnh vân tay dạng *.bmp thu nhận trực truyến từ thiết bị quét vân tay, vhương trình sử dụng máy scan của Futronic model 9880.. Ảnh vân tay có thể được lấy mẫu nhiều lần để tăng độ chính xác cho tập điểm đặc trưng. Trong giai đoạn đầu thử nghiệm thuật toán, ảnh đầu vào được sử dụng từ CSDL ảnh.
- *Xử lý ảnh*: Ảnh sau khi được thu nhận sẽ được xử lý bằng Matlab. Chương trình sử dụng các hàm hỗ trợ của Matlab bằng việc xây dựng các file thư viện liên kết động .dll từ các file .m của Matlab, sau đó tích hợp vào hệ thống, chương trình cần bộ MCR (Matlab Compiler Runtime) để thực thi chương trình. Sử dụng ngôn ngữ Matlab cho kết quả khá tốt nhưng có nhược điểm về tốc độ Mođun xử lý ảnh gồm có 2 chức năng chính là cải thiện ảnh và làm mảnh ảnh. Chương trình sử dụng file fenhancement.m của Matlab để cải thiện ảnh và sử

dụng file edge.m của Matlab để làm mảnh ảnh. Cuối cùng, sau khi làm mảnh ảnh bằng Matlab, chương trình thực hiện xóa gai ảnh đã làm mảnh để tăng độ chính xác cho bước trích chọn điểm minutiae

- *Mã hoá và giải mã*

Các thuật toán chi tiêt của 2 khối chức năng đã trình bày chi tiết ở phần trên. Về công nghệ và lập trình, chức năng mã hóa khóa cá nhân sử dụng hàm thư viện **PEM_Write_PrivateKey** và chức năng giải mã khóa cá nhân sử dụng **PEM_Read _PrivateKey** của thư viện OpenSSL

5.3.4. Thử nghiệm và kết quả

Chương trình hệ thẩm định xác thực vân tay đã được thử nghiệm theo 2 kịch bản:

- Chương trình thử nghiệm với các ảnh vân tay từ CSDL ảnh vân tay dùng cho các hệ thẩm định sinh trắc.
- Chương trình thử nghiệm với các ảnh vân tay sống thu nhận từ thiết bị quét

a/ Chương trình thực hiện thử nghiệm với bộ cơ sở dữ liệu ảnh FVC 2004 (Fingerprint Verification Competition 2004 – được download từ trang web http://bias.csr.unibo.it/fvc2004)

Kịch bản thử nghiệm với 100 vân tay khác nhau, trong đó mỗi vân tay sẽ có 8 loại mẫu ảnh vân tay với các điều kiện mô tả lấy mẫu khác nhau như sau:

- Loại 1: Ngón tay đặt lệch tâm và đặt nhẹ
- Loại 2: Ngón tay đặt đúng tâm nhưng đặt nhẹ
- Loại 3: Ngón tay đặt chuẩn quy cách: đúng tâm giữa và đặt vừa phải
- Loại 4: Bề mặt ngón tay tiếp xúc không đều, lệch về phía đầu ngón.
- Loại 5: Bề mặt ngón tay tiếp xúc không đều, lệch về phía cuối ngón.
- Loại 6: Ngón tay bị đặt chéo
- Loại 7: Ngón tay bị khô, ảnh bị mờ
- Loại 8: Ngón tay bị ướt, ảnh bị nhoè.

Bảng kết quả:

Loại ảnh	Tỷ lệ chấp nhận sai FAR(%)	Tỷ lệ từ chối sai FRR (%)
Loại 1	20	20
Loại 2	20	20
Loại 3	15	10
Loại 4	20	60
Loại 5	20	60
Loại 6	10	80
Loại 7	30	40
Loại 8	40	40

b/ Chương trình thẩm định sinh trắc bảo vệ khóa cá nhân được thử nghiệm với các vân tay được quét trực tiếp từ thiết bị bởi các bạn cùng tham gia đề tài.

Kết quả thử nghiệm trong trường hợp thu nhận ảnh vân tay sống được quét trực tiếp từ scanner:

Số lần thử	Tỷ lệ chấp nhận sai - FAR(%)	Tỷ lệ từ chối sai FRR (%)
130	20	30

So sánh kết quả của 2 thí nghiệm trên, ta thấy chương trình chạy chính xác hơn với dữ liệu ảnh vân tay loại 3 so với ảnh được thu trực tiếp từ scanner, vì ảnh loại 3 là loại ảnh vân tay được đặt đúng tâm và chất lượng tốt.

Bảng kết quả cho thấy tỷ lệ lỗi đối với ảnh vân tay quét từ thiết bị còn lớn, nguyên nhân là do ảnh được thu trực tiếp từ scanner thường không ổn định

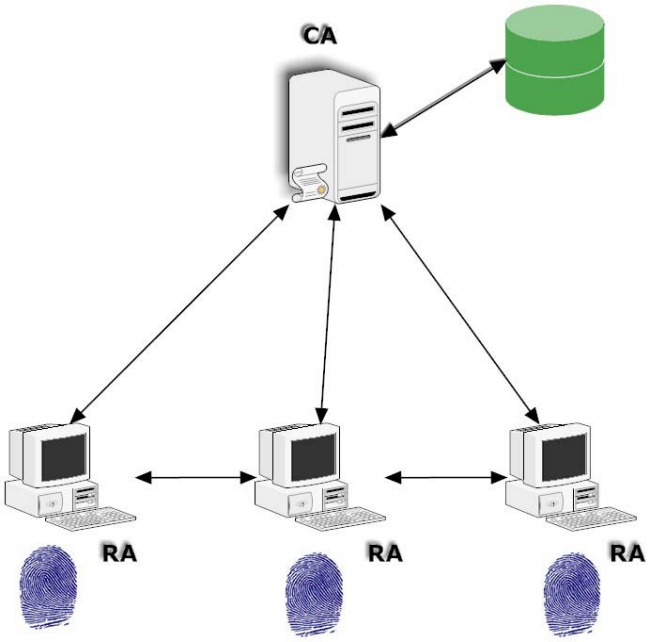
Chương 6.
PHÂN TÍCH THIẾT KẾ VÀ XÂY DỰNG HỆ THỐNG HẠ TẦNG KHÓA CÔNG KHAI PKI CHO HỆ THỐNG BK-BIOPKI

6.1. Phân tích các yêu cầu và giải pháp thiết kế hệ thống BK-BioPKI

Mô hình hệ thống mức khung cảnh

Hệ thống BK - BioPKI thuộc Đề tài nghiên cứu cấp nhà nước theo nghị định thư hợp tác với Malaysia về "Hệ thống an ninh sinh trắc học BK-BioPKI" của khoa CNTT nhằm nghiên cứu và thử nghiệm một số giải pháp tích hợp sinh trắc học vào hạ tầng khóa công khai PKI.

Mục đích của hệ thống BK – BioPKI là tạo một môi trường cơ sở hạ tầng khóa công khai trong phòng thí nghiệm với mạng cục bộ để từ đó phát triển thử nghiệm tích hợp yếu tố sinh trắc học vào PKI để nghiên cứu một số vấn đề về an toàn an ninh dựa trên sinh trắc học.



Hình 6.1. Hệ thống BK – BioPKI

Hệ thống BK – BioPKI bao gồm:

a) Cơ sở hạ tầng khóa công khai PKI gồm có: CA Server, RA, các giao dịch cơ sở, người dùng trong hệ thống. CA Server quản lý cấp phát chứng chỉ số theo chuẩn X509. Công cụ xây dựng là dùng ngôn ngữ C++ trên nền Windows và sử dụng thư viện OpenSSL; hệ quản trị cơ sở dữ liệu MySQL.

b) Hệ thẩm định sinh trắc: gồm 3 thành phần chính:

- Đăng ký sinh trắc (enrollment)
- Mã hóa lưu trữ đặc trưng sinh trắc
- Đối sánh thẩm định sinh trắc

c) Thiết kế giao diện (interface) và tích hợp phân hệ sinh trắc vào cơ sở hạ tầng khóa công khai tạo thành hệ BioPKI.

Kiến trúc một hệ PKI khi được triển khai phụ thuộc vào các chính sách và mô hình theo qui định của các cơ quan có thẩm quyền. Như đã trình bày, mục tiêu của đề tài là thử nghiệm, môi trường cài đặt hệ thống là ở phòng thí nghiệm. Do đó, kiến trúc PKI được chọn để áp dụng vào thiết kế hệ thống BK-BioPKI là kiến trúc CA đơn là hoàn toàn phù hợp với điều kiên thực tế cũng như nhiệm vụ của đề tài.

Với kiến trúc PKI – CA đơn, về mặt tổ chức hệ thống bao gồm hai phân hệ: đó là CA server và RA-Client. CA server đảm nhận vai trò của một trung tâm cấp phát chứng chỉ. Còn RA-Client vừa đóng vai trò là RA (cơ quan đăng kí chứng thư) vừa là nơi để người dùng có thể thực hiện các chức năng của mình. RA-Client cũng là nơi được tích hợp phân hệ sinh trắc vào hệ thống.

Hệ thống BK-BioPKI phải đảm bảo được các chức năng cơ bản của một cơ sở hạ tầng khóa công khai, đồng thời hệ thống được tích hợp các chức năng của phân hệ sinh trắc vào các hoạt động của hệ thống.

6.2. Giải pháp công nghệ và thiết kế hệ thống BK-BioPKI

6.2.1. Phân tích giải pháp công nghệ xây dựng hệ thống

Lựa chọn giải pháp về công nghệ

Thư viện OpenSSL được chọn để xây dựng cơ sở hạ tầng khóa công khai [4]. Ngôn ngữ phát triển hệ thống là C++ vì vừa hỗ trợ hướng đối tượng vừa tích hợp được các hàm viết bằng ngôn ngữ C trong thư viện OpenSSL. Hệ quản trị cơ sở dữ liệu là MySQL vì đây là hệ quản trị cơ sở dữ liệu mã nguồn mở và có hỗ trợ các hàm C API để thực hiện truy vấn cơ sở dữ liệu.

Đề xuất giải pháp hệ thống

- Thiết kế cơ sở hạ tầng khóa công khai nhờ sự hỗ trợ của các hàm thư viện có trong OpenSSL.
- Thiết kế phân hệ sinh trắc vân tay.
- Thiết kế tích hợp sinh trắc vào cơ sở hạ tầng khóa công khai.

6.2.2. Giới thiệu về thư viện OpenSSL

Khái quát chung về OpenSSL

OpenSSL là một kết quả của sự cộng tác nhằm phát triển một kỹ thuật bảo mật dạng thương mại, đầy đủ các đặc trưng và là bộ công cụ mã nguồn mở thực thi các giao thức như Secure Sockets Layer (SSL v2/v3) và Transport Layer Security (TSL v1) với những thuật toán mã

hóa phức tạp. Dự án được quản lý bởi hiệp hội những người tình nguyện trên thế giới, sử dụng Internet để trao đổi thông tin, lập kế hoạch và phát triển công cụ OpenSSL và các tài liệu liên quan khác [16,22,23]

SSL là giao thức đa mục đích được thiết kế để tạo ra các giao tiếp giữa hai chương trình ứng dụng trên một cổng định trước (socket 443) nhằm mã hoá toàn bộ thông tin đi/đến mà ngày nay được sử dụng rộng rãi cho giao dịch điện tử như truyền số hiệu thẻ tín dụng, mật khẩu, số bí mật cá nhân (PIN) trên Internet. [23]

Ngày nay giao thức Secure Socket Layer (SSL) đã được sử dụng rộng rãi trên World Wide Web trong việc xác thực và mã hoá thông tin giữa client và server. Tổ chức IETF (Internet Engineering Task Force) đã chuẩn hoá SSL và đặt lại tên là TLS (Transport Layer Security). Mặc dù là có sự thay đổi về tên nhưng TLS chỉ là một phiên bản mới của SSL. Phiên bản TLS 1.0 tương đương với phiên bản SSL 3.1. Tuy nhiên SSL là thuật ngữ được sử dụng rộng rãi hơn.

Tính mở của thư viện OpenSSL cho phép can thiệp tới quá trình tạo và quản lý chứng chỉ số, phù hợp với yêu cầu của đề tài. Do vậy đề tài lựa chọn xây dựng một hệ thống PKI trên nền tảng thư viện OpenSSL.

OpenSSL là thư viện cho lập trình với ngôn ngữ C và có thể cài đặt trên nhiều môi trường thực hiện C khác nhau như Microsoft Visual C++. Borland C++ Builder…

OpenSSL có thể được sử dụng trên nhiều hệ điều hành khác nhau từ các hệ thống UNIX đến Window.

Cài đặt thư viện OpenSSL

Để cài đặt thư viện OpenSSL trên hệ điều hành Window trước hết cần download phiên bản của thư viện này dành cho Window tại địa chỉ:
http://www.slproweb.com/products/Win32OpenSSL.html
Sau đó, chạy file install để cài đặt (giả sử vào thư mục C:\Openssl). Để sử dụng thư viện này với Microsoft Visual C++ cần làm các bước sau:
Copy tất cả các file trong thư mục 'C:\OpenSSL\lib\VC' vào thư mục Visual C++ 'lib'. Thư mục này đôi khi được đăt ở địa chỉ 'C:\Program Files\Microsoft Visual Studio\VC98\lib' or 'C:\Program Files\Microsoft Visual C++\lib'.
Tiếp theo, copy tất cả trong thư mục 'C:\OpenSSL\include' tới thư mục Visual C++ 'include'.
Quá trình cài đặt hoàn tất và có thể bắt đầu lập trình với thư viện OPENSSL.

Thành phần của bộ thư viện OpenSSL bao gồm:

- Thư viện về mã hóa: hầu hết các thuật toán phổ biến về mã hóa đối xứng, mã hóa công khai, hàm băm ... đều được hiện thực trên thư viện này. Thư viện có chức năng sinh số ngẫu nhiên lớn, và hỗ trợ nhiều định dang lưu trữ và quản lý khóa, chứng chỉ số. Ngoài ra, OpenSSL cho phép tích hợp với các bộ phần cứng tăng tốc mã hóa phổ biến trong phiên bản mới nhất là 0.9.8.
- Thư viện về giao thức SSL: tất cả các phiên bản của giao thức SSL đều được hỗ trợ, bao gồm cả giao thức mới nhất là TLS v1.

Lập trình sử dụng OpenSSL

Để sử dụng thư viện OpenSSL, cần cho các file khai báo đặc tả (file .h) sau vào file mã nguồn:

```
#include <openssl/bio.h>
#include <openssl/err.h>
#include <openssl/rand.h>
#include <openssl/ssl.h>
#include <openssl/x509.h>
#include <openssl/x509v3.h>
```

Ngoài ra cần thêm file applink.c là file liên kết phân hệ khi biên dịch chương trình. File này chỉ sử dụng cho các phiên bản thư viện 0.9.8 trở về sau. Khi liên kết (link), cần đặt thông số cho thư viện cần thêm là libeay32.lib và ssleay32.lib.

Khởi tạo thư viện

Thư viện cần được khởi tạo trước khi sử dụng, bao gồm:

- Khởi tạo thông số cho sử dụng các hàm mã hóa và băm

```
OpenSSL_add_all_algorithms();
OpenSSL_add_all_digests();
```

- Khởi tạo quản lý bộ nhớ, nạp các hàm quản lý lỗi.

```
CRYPTO_mem_ctrl(CRYPTO_MEM_CHECK_ON);
CRYPTO_malloc_init();
ERR_load_crypto_strings();
```

- Khởi tạo sử dụng thư viện SSL

```
SSL_library_init();
SSL_load_error_strings();
```

Sử dụng

Tập các hàm API của OpenSSL chia ra theo nhóm chức năng, mỗi nhóm chức năng bắt đầu tên hàm bằng một tiền tố. Ví dụ, các hàm về thư viện X.509 luôn có tên bắt đầu là X509_, các hàm giao tiếp vào ra có tiền tố của tên BIO_, các hàm mã hóa là EVP_, các hàm giao thức SSL là SSL_.

- Sử dụng các hàm mã hóa

Quá trình thực hiện mã hóa như sau

- Tạo context chứa thông tin về mã hóa: lưu trong con trỏ kiểu EVP_CIPHER_CTX:

```
EVP_CIPHER_CTX *x = NULL;
x = (EVP_CIPHER_CTX*) malloc(sizeof(EVP_CIPHER_CTX));
EVP_CIPHER_CTX_init(x);
```

- Chỉ định thuật toán, khóa mã cho quá trình mã hóa/giải mã: dùng một trong các hàm sau:

```
int EVP_EncryptInit(EVP_CIPHER_CTX *ctx,const EVP_CIPHER *type,
unsigned char *key, unsigned char *iv);
```

int EVP_DecryptInit(EVP_CIPHER_CTX *ctx, const EVP_CIPHER
*type, unsigned char *key, unsigned char *iv);

- Thêm dữ liệu cần mã hóa:

int EVP_EncryptUpdate(EVP_CIPHER_CTX *ctx, unsigned char *out, int*outl, unsigned char *in, int inl);

- Lấy ra dữ liệu đã mã hóa:

int EVP_EncryptFinal(EVP_CIPHER_CTX *ctx, unsigned char *out, int*outl);

• Sử dụng giao thức SSL

- Tạo context cấu hình kết nối SSL: dùng các hàm SSL_CTX_
- Tạo một kết nối vào ra thông thường: theo giao thức TCP/IP bằng các hàm BIO_: BIO_new_connect, BIO_do_connect…
- Tạo một socket SSL: dựa trên kết nối BIO và context cấu hình SSL: SSL_new,
- SSL_set_bio, SSL_connect…
- Đọc ghi dữ liệu qua socket SSL: bằng các hàm SSL_read, SSL_write.
- Đóng kết nối SSL và giải phóng context: SSL_close, SSL_CTX_free.

• Sử dụng thư viện X.509

Yêu cầu chứng chỉ số thể hiện bằng đối tượng X509_REQ. Trong đối tượng này bao gồm tên định danh của người đăng ký, được thể hiện bằng X509_NAME. Thành phần mở rộng của yêu cầu chứng chỉ là X509_EXTENSION.

Các hàm của X.509 chia theo chức năng:

- X509_NAME_*: thao tác với đối tượng X509_NAME
- X509_PKEY* và X509_PUBKEY*: thao tác với khóa công khai/cá nhân.
- X509_REQ*: thao tác với yêu cầu chứng chỉ số.
- X509_CRL*: thao tác với danh sách CRL.
- X509_REVOKED*: thao tác với một chứng chỉ số bị hủy nằm trong danh sách CRL.

Ngoài ra còn một số hàm khác.

Các bước tạo yêu cầu chứng chỉ như sau:

- Tạo đối tượng tên định danh X509_NAME
- Tạo cặp khóa công khai/cá nhân, cho khóa công khai vào yêu cầu chứng chỉ số.
- Thêm các thành phần mở rộng nếu cần.
- Thực hiện ký chứng thực nội dung yêu cầu chứng chỉ.

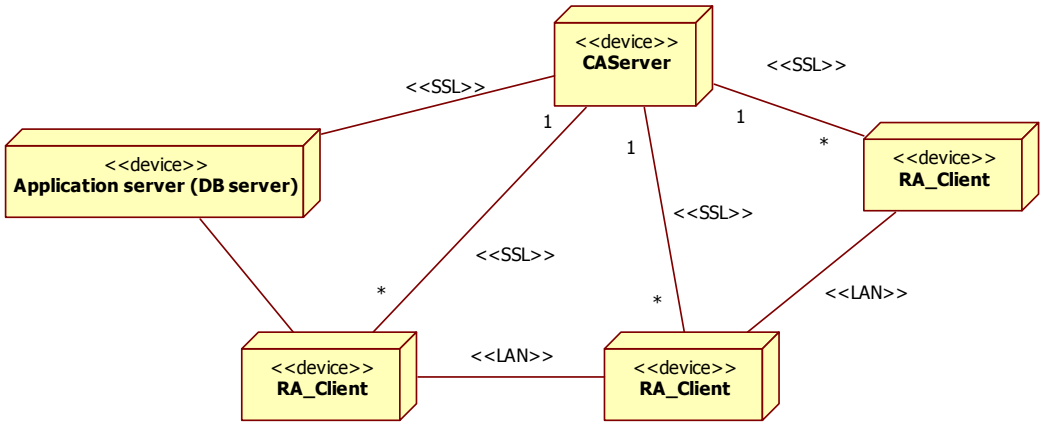
CA phát hành chứng chỉ số từ yêu cầu chứng chỉ:

- Lấy thông tin X509_NAME trong yêu cầu chứng chỉ và gán cho trường Subject của chứng chỉ số.
- Lấy thông tin X509_NAME trong chứng chỉ số gốc của CA và gán cho trường Issuer của chứng chỉ số.
- Dùng khóa công khai trong yêu cầu chứng chỉ số và kiểm tra chữ ký. Lấy khóa công khai cho vào chứng chỉ số.
- Thêm các thành phần mở rộng nếu cần
- Thực hiện ký chứng chỉ bằng khóa cá nhân của CA.

Thư viện OpenSSL đang trong quá trình phát triển, tài liệu thư viện được liệt kê tại

http://www.openssl.org/docs/.

6.3. Phân tích thiết kế các thành phần chức năng của hệ thống BK-BioPKI



Hình 6.2. Sơ đồ triển khai của hệ thống

Xuất phát từ mục tiêu của đề tài và do môi trường cài đặt hệ thống là ở PTN nên kiến trúc PKI được chọn để áp dụng vào thiết kế hệ thống BK – BioPKI là kiến trúc CA đơn. Kiến trúc một hệ PKI còn phụ thuộc vào các chính sách và mô hình triển khai PKI theo qui định của cơ quan có thẩm quyền.

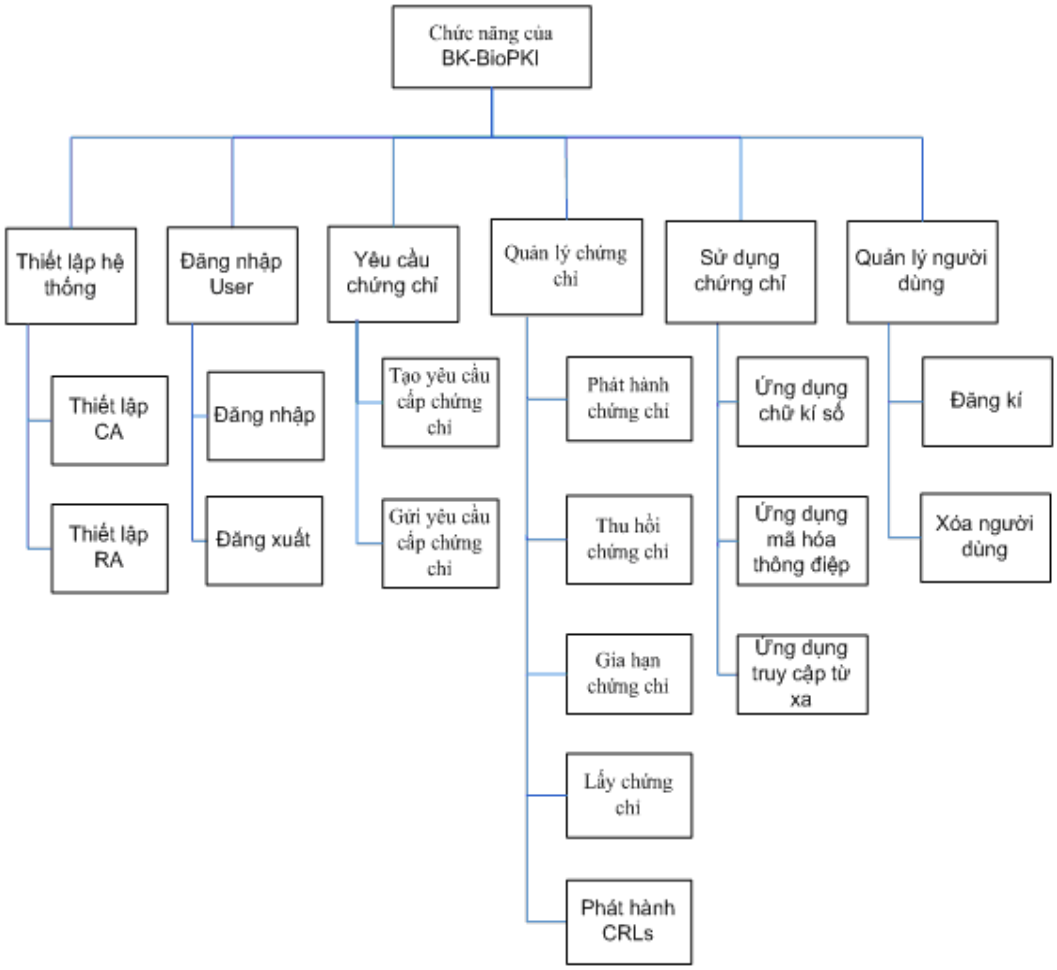
Trong giai đoạn hiện nay hệ thống BK – BioPKI được xây dựng trong phòng thí nghiệm với kiến trúc CA đơn là phù hợp với điều kiện thực tế và nhiệm vụ của đề tài.

Hệ thống BK – BioPKI phải đảm bảo được các chức năng cơ bản của một cơ sở hạ tầng khóa công khai, đồng thời hệ thống có tích hợp các chức năng của phân hệ sinh trắc học.
Do yêu cầu nêu trên và do kiến trúc PKI được chọn là CA đơn nên các chức năng chính của hệ thống có thể được thể hiện qua biểu đồ phân rã chức năng như hình 6.3.

Như trên đã phân tích vì hệ thống BK – BioPKI là một cơ sở hạ tầng khóa công khai nên nó phải có các chức năng cơ bản: tạo yêu cầu xin cấp chứng chỉ, cấp phát chứng chỉ, quản lý việc gia hạn chứng chỉ và hủy bỏ chứng chỉ. Các chứng chỉ được lựa chọn theo chuẩn X509 vì là chuẩn được sử dụng rộng rãi hiện nay đồng thời chuẩn chứng chỉ này được thư viện OpenSSL hỗ trợ.

Trong phương án thiết kế hiện nay hệ thống có kiến trúc CA đơn nên các RA được thiết kế để đảm nhiệm chức năng quản lý người dùng để giảm tải cho CA, mỗi RA quản lý các người dùng đăng kí với nó. CA trong hệ thống BK – BioPKI chỉ đảm nhiệm các chức năng liên quan tới chứng chỉ. RA trong hệ thống BK – BioPKI sẽ đảm nhận việc quản lý người dùng của hệ thống, đồng thời là nơi sinh khóa, tạo yêu cầu cấp chứng chỉ cho các người dùng. Các tổ chức hệ thống như vậy sẽ giúp CA không phải đảm nhận quá nhiều công việc mà các công việc được chia ra các RA. Bên cạnh đó cách tổ chức này còn có ưu điểm là khóa cá nhân

sinh tại RA sẽ có độ mật cao hơn so với cách sinh khóa tại CA vì nếu khóa sinh tại CA sẽ phải qua một bước phân phối khóa từ CA tới người dùng.

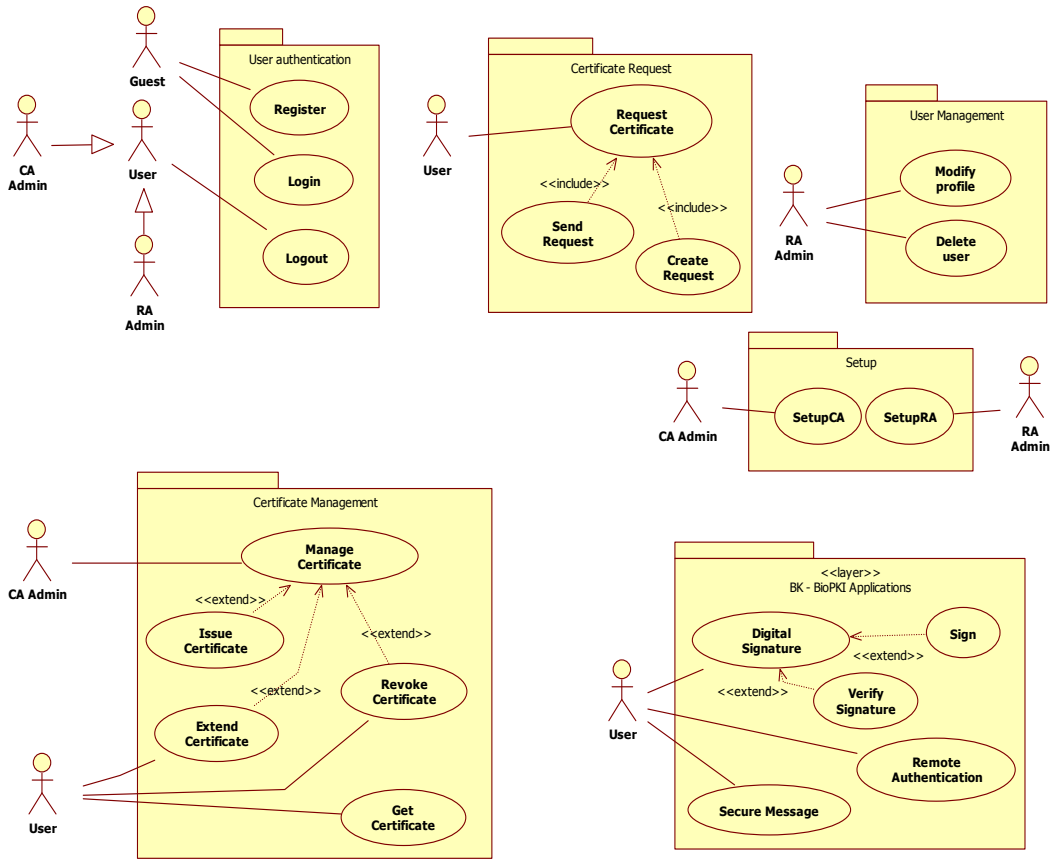


Hình 6.3. Biểu đồ phân rã chức năng của hệ thống BK – BioPKI

6.4. Thiết kế xây dựng và lập trình phần mềm cơ sở các chức năng hoạt động hệ thống BK-BioPKI

6.4.1. Các tình huống hoạt động giao dịch cơ sở của hệ thống

Trước khi đi vào thiết kế các hoạt động của hệ thống BK – BioPKI, ta xét lại các chức năng của hệ thống cung cấp dưới cách nhìn của các tình huống sử dụng sau:



Hình 6.4. Các tình huống sử dụng giao dịch trong hệ thống BK – BioPKI

Với biểu đồ này, các chức năng của hệ thống gắn liền với các tác nhân bao gồm: người quản trị CA- CA Amin, người quản trị RA- RA Admin và người dùng của hệ thống.

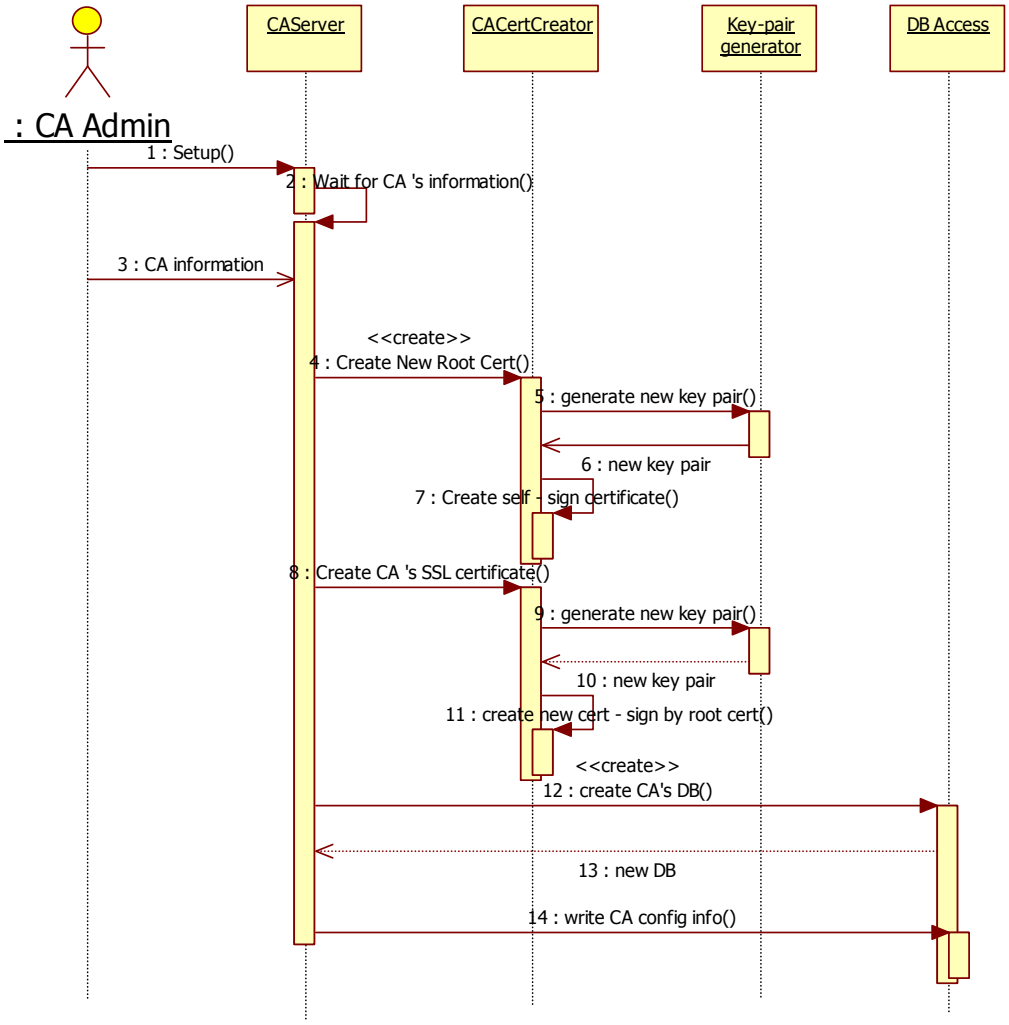
6.4.2. Thiết kế các giao dịch cơ sở của hệ thống

Tiếp theo đây là thiết kế cho các tình huống sử dụng chính của hệ thống liên quan tới các hoạt động cơ sở của cơ sở hạ tầng khóa công khai, trong đó chủ yếu là thiết kế cho phía CA Server

Thiết lập hệ thống: thiết lập cho CA và RA

CA và RA đều cần phải thiết lập để có thể hoạt động được.

Thiết lập tại CAServer:



Hình 6.5. Biểu đồ diễn tiến quá trình thiết lập của CA Server

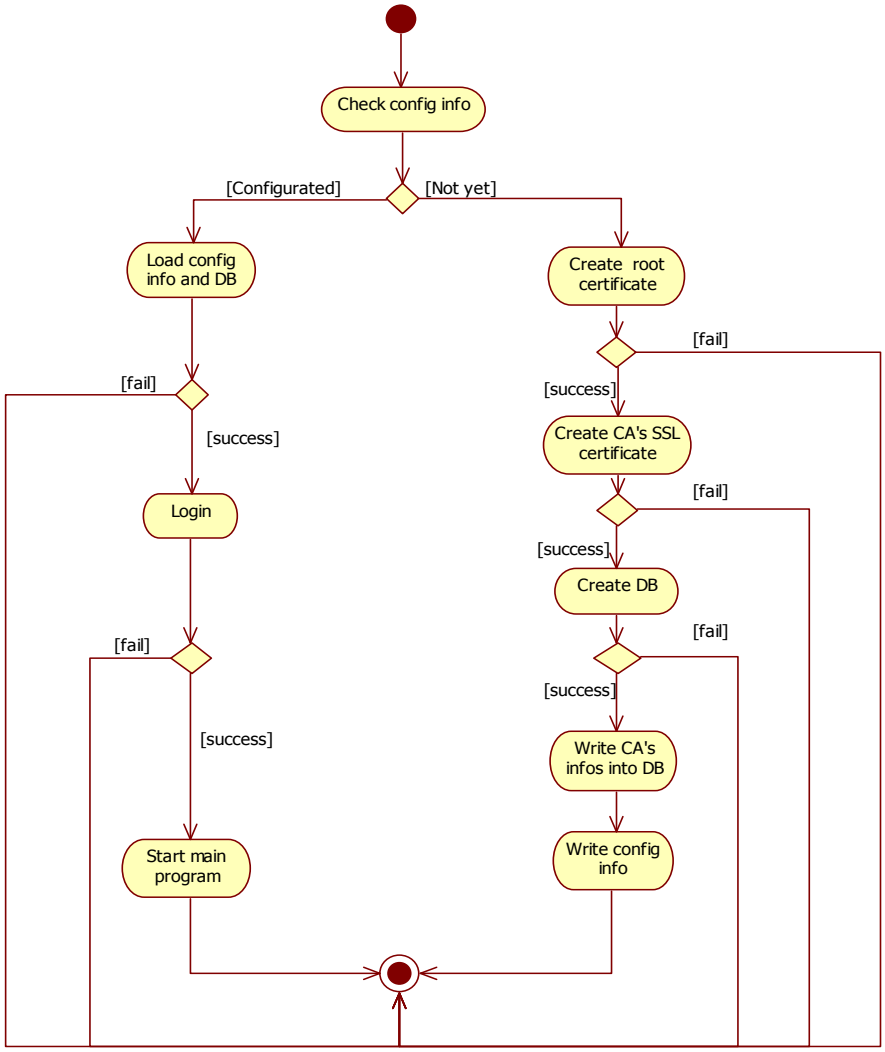
Thiết lập CA lần đầu tiên là quá trình tạo chứng chỉ cho CA: có 2 chứng chỉ: một là chứng chỉ gốc của CA dùng trong việc cấp phát chứng chỉ; hai là chứng chỉ dành riêng cho việc tạo kênh SSL với các RAClient. CA sẽ tự sinh ra cặp khóa tương ứng cho mỗi chứng chỉ, và mọi chứng chỉ được được kí bởi khóa riêng của chứng chỉ gốc CA (root certificate).. Chứng chỉ gốc này của CA sẽ được trao đổi offline với các RAClient.

***Các bước của quá trình thiết lập được thiết kế* bao gồm:**

1. Người quản trị CA sẽ kích hoạt chức năng thiết lập cho CA.
2. CA Server yêu cầu người quản trị cung cấp các thông tin về CA. lựa chọn các thông tin về độ dài khóa, thuật toán... cho việc tạo chứng chỉ của CA.
3. Người quản trị cung cấp đầy đủ các thông tin cần thiết.
4. CA Server yêu cầu bộ phận tạo chứng chỉ tạo chứng chỉ gốc
5. Đầu tiên sinh bộ phận sinh khóa sẽ sinh cặp khóa cho chứng chỉ gốc
6. Cặp khóa được gửi lại cho bộ phận tạo chứng chỉ

7. Khi đã có cặp khóa cho chứng chỉ gốc, bộ phận tạo chứng chỉ sẽ tạo ra chứng chỉ số gốc của CA với CA tự kí bằng khóa bí mật trong cặp khóa vừa được tạo.
8. CA Server yêu cầu bộ phận tạo chứng chỉ tạo chứng chỉ phục vụ cho kênh SSL nối với nó.
9. Bộ phận tạo chứng chỉ yêu cầu bộ phận sinh khóa sinh cặp khóa cho chứng chỉ mới.
10. Cặp khóa được gửi lại cho bộ phận tạo chứng chỉ.
11. Chứng chỉ SSL được kí xác nhận bởi chữ kí của CA(khóa bí mật của CA).
12. CA Server tạo cơ sở dữ liệu cho nó.
13. Nếu cơ sở dữ liệu được tạo thành công thì:
14. CA Server lưu thông tin cấu hình của nó vào cơ sở dữ liệu.

Dưới đây là biểu đồ hoạt động khởi tạo tại CAServer, biểu đồ mô tả hoạt động khởi tạo của CA, trong đó có bao gồm diễn biến của việc thiết lập CA trong trường hợp hệ thống chưa được thiết lập.



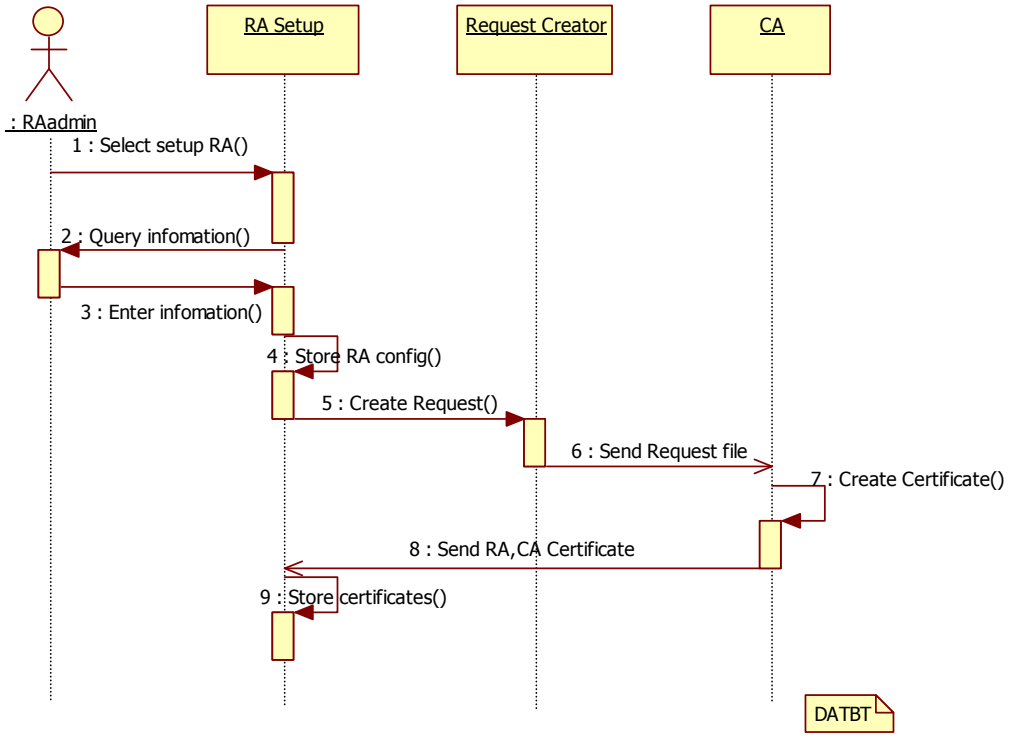
Hình 6.6. Biểu đồ hoạt động khởi động của CA Server

Thiết lập cho các RAClient:

RAClient tạo mới cơ sở dữ liệu của nó và lưu các thông tin về cơ sở dữ liệu vào Registry của hệ điều hành.

Mỗi RA sẽ tạo ra yêu cầu cấp chứng chỉ cho mình. (Sinh cặp khóa của RA và tạo một yêu cầu cấp chứng chỉ tương ứng cặp khóa đó). Yêu cầu này được gửi tới CA theo kiểu offline.

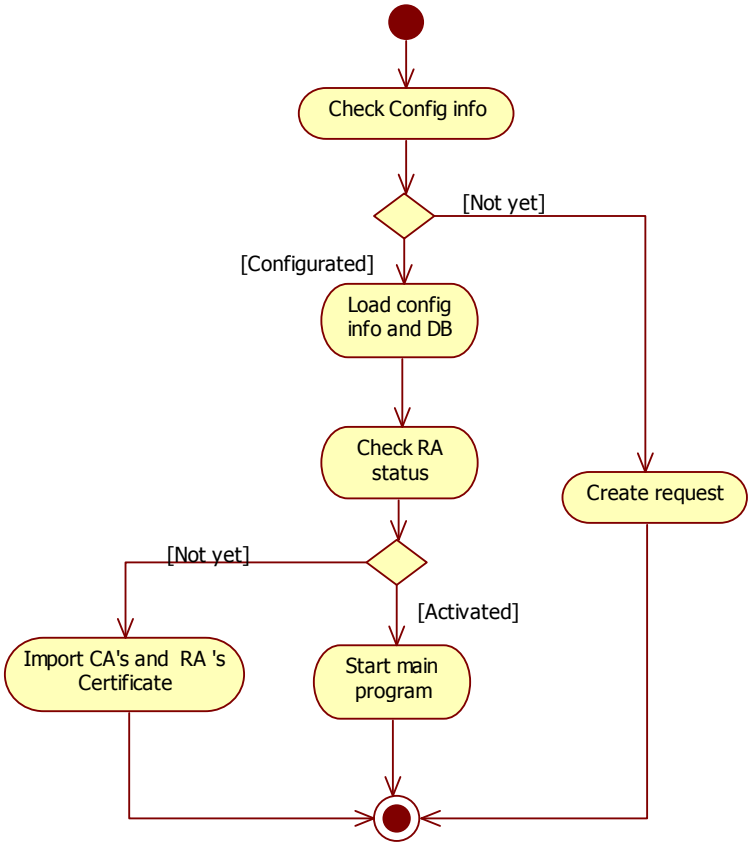
Tại CAServer, CA Admin sẽ cấp chứng chỉ cho RA từ các yêu cầu trên. Các chứng chỉ của RA được gửi offline về cho RA. Hình sau là thiết kế quá trình thiết lập cho RA



Hình 6.7

Sau khi có được chứng chỉ, RA nhập chứng chỉ của nó cùng với chứng chỉ của CA, lưu vào cơ sở dữ liệu. Chứng chỉ của RA sẽ được dùng để tạo kênh SSL kết nối tới CAServer.

Biểu đồ hoạt động khởi tạo của RAClient như sau:



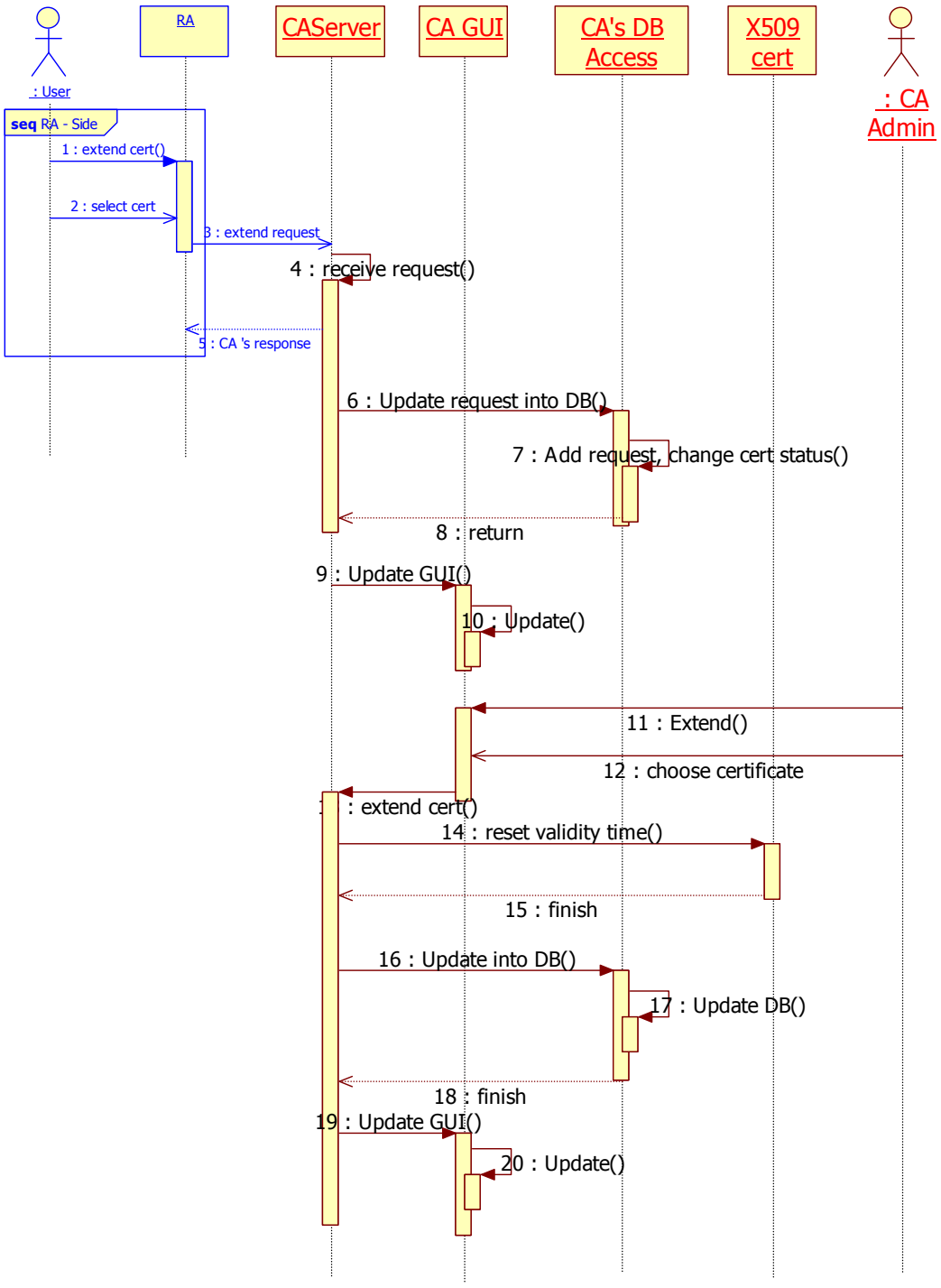
Hình 6.8. Biểu đồ hoạt động khởi động của RA Client

Quản lý chứng chỉ: gia hạn, thu hồi, cấp mới chứng chỉ

Gia hạn chứng chỉ:

Khi chứng chỉ hết hạn hoặc sắp hết hạn, người dùng yêu cầu CA gia hạn thời gian sử dụng chứng chỉ. Người dùng sẽ chọn ra chứng chỉ nào cần gia hạn, sau đó RA gửi yêu cầu gia hạn tới CA. Khi CA nhận được yêu cầu, nó lưu yêu cầu gia hạn để đợi CA Admin duyệt. CA Admin sẽ quyết định có gia hạn cho chứng chỉ hay không. Nếu đồng ý gia hạn, chứng chỉ sẽ được đặt lại thời gian có hiệu lực bắt đầu từ thời điểm được gia hạn và kéo dài 1 năm.

Biểu đồ diễn tiến sau đây mô tả quá trình gia hạn cho một chứng chỉ (chi tiết thiết kế trong tài liệu kĩ thuật của hệ thống).

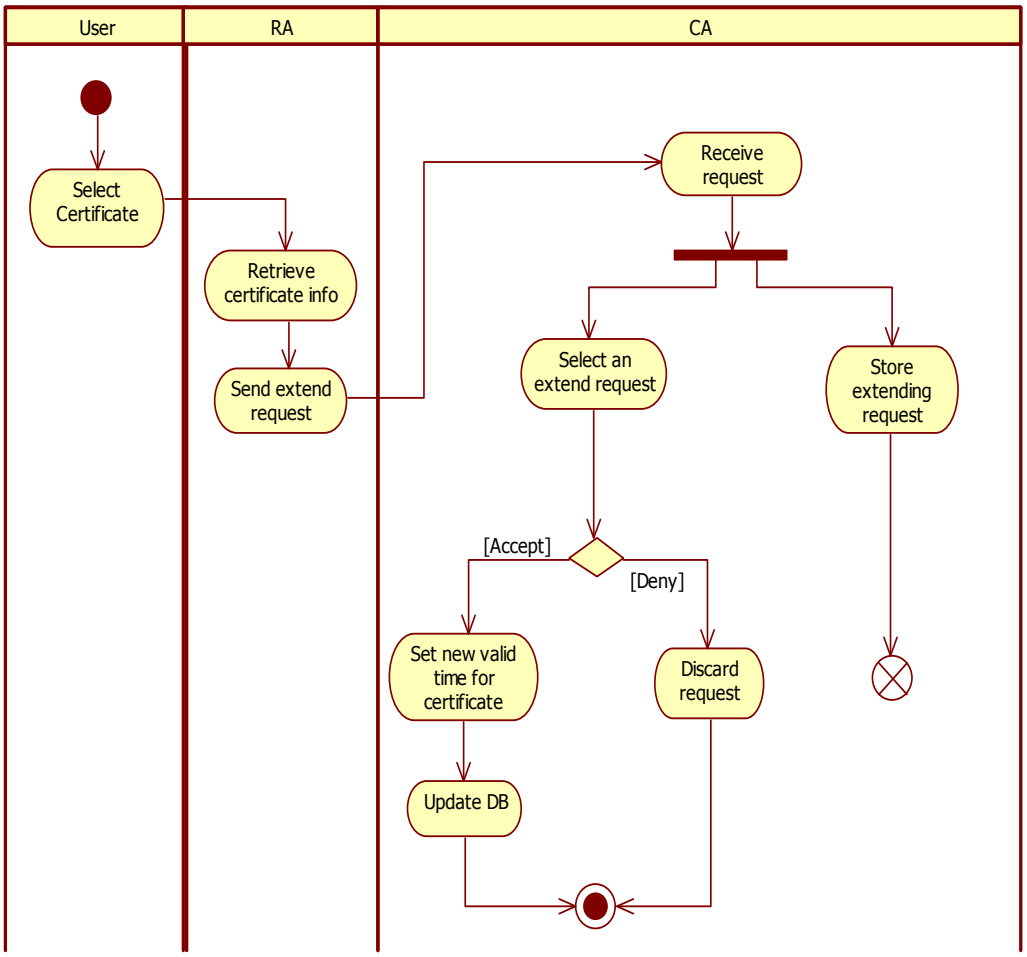


Hình 6.9. Biểu đồ diễn tiến quá trình gia hạn một chứng chỉ

Khi CA nhận được yêu cầu, nó sẽ lưu yêu cầu và cập nhật trạng thái của chứng chỉ, đồng thời cập nhật giao diện người dùng cho CA. (các bước 4 – 10 trên biểu đồ).

Khi có người quản trị CA quyết định gia hạn, chứng chỉ sẽ được gia hạn như đã nói ở trên, CA sẽ cập nhật cơ sở dữ liệu và giao diện để hoàn thành việc gia hạn. (Các bước còn lại trên biểu đồ).

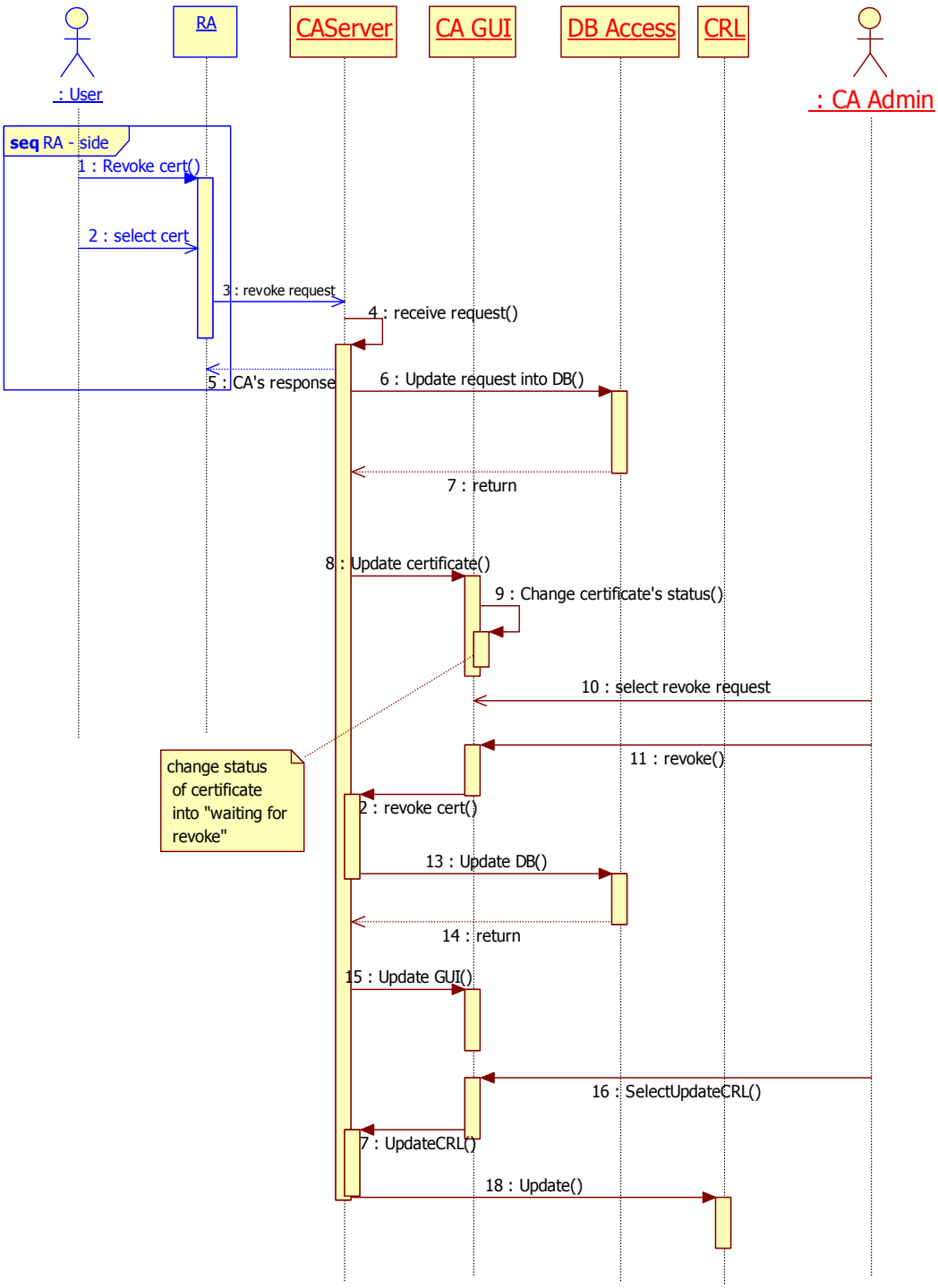
Hoạt động gia hạn có thể được mô hình hóa trong biểu đồ sau:



Hình 6-10. Biểu đồ hoạt động gia hạn chứng chỉ

Thu hồi chứng chỉ:

Biểu đồ diễn tiến của quá trình thu hồi một chứng chỉ được thể hiện dưới đây. Quá trình thu hồi bắt đầu bên phía RA (màu xanh trên hình vẽ).

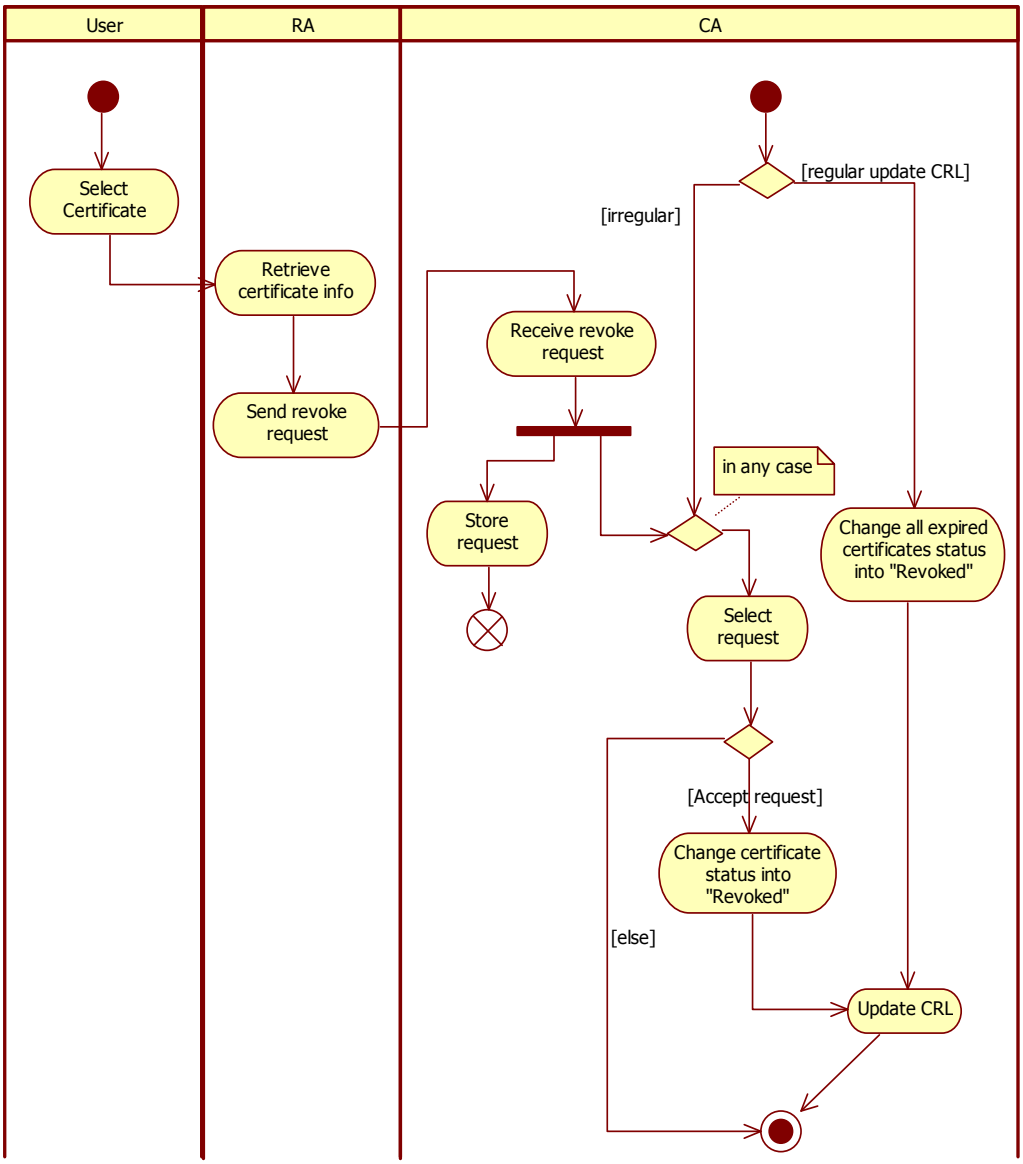


Hình 6-11. Biểu đồ diễn tiến của giao dịch thu hồi một chứng chỉ

Việc thu hồi chứng chỉ có thể theo định kì hoặc tại một thời điểm CA Admin quyết định thu hồi một chứng chỉ nhất định nào đó.

Người dùng có thể xin thu hồi chứng chỉ của mình khi bị mất khóa cá nhân. Trong trường hợp này người dùng gửi yêu cầu cho CA (thông qua RA) để thu hồi chứng chỉ. Khi CA nhận

được yêu cầu thu hồi một chứng chỉ, yêu cầu này sẽ được lưu vào hàng đợi của CA chờ duyệt. Thông tin về chứng chỉ bị yêu cầu hủy sẽ được cập nhật vào cơ sở dữ liệu và trên giao diện người dùng của CA để người quản trị CA có thể xem xét và duyệt yêu cầu. (Các bước 6, 7, 8, 9 trên biểu đồ). Khi người quản trị CA chọn một yêu cầu và duyệt thu thồi, CA sẽ thu hồi chứng chỉ, cập nhật thông tin về chứng chỉ vào cơ sở dữ liệu và cập nhật giao diện người dùng của CA. (Các bước còn lại trên biểu đồ diễn tiến).
Biểu đồ hoạt động thu hồi chứng chỉ như sau:

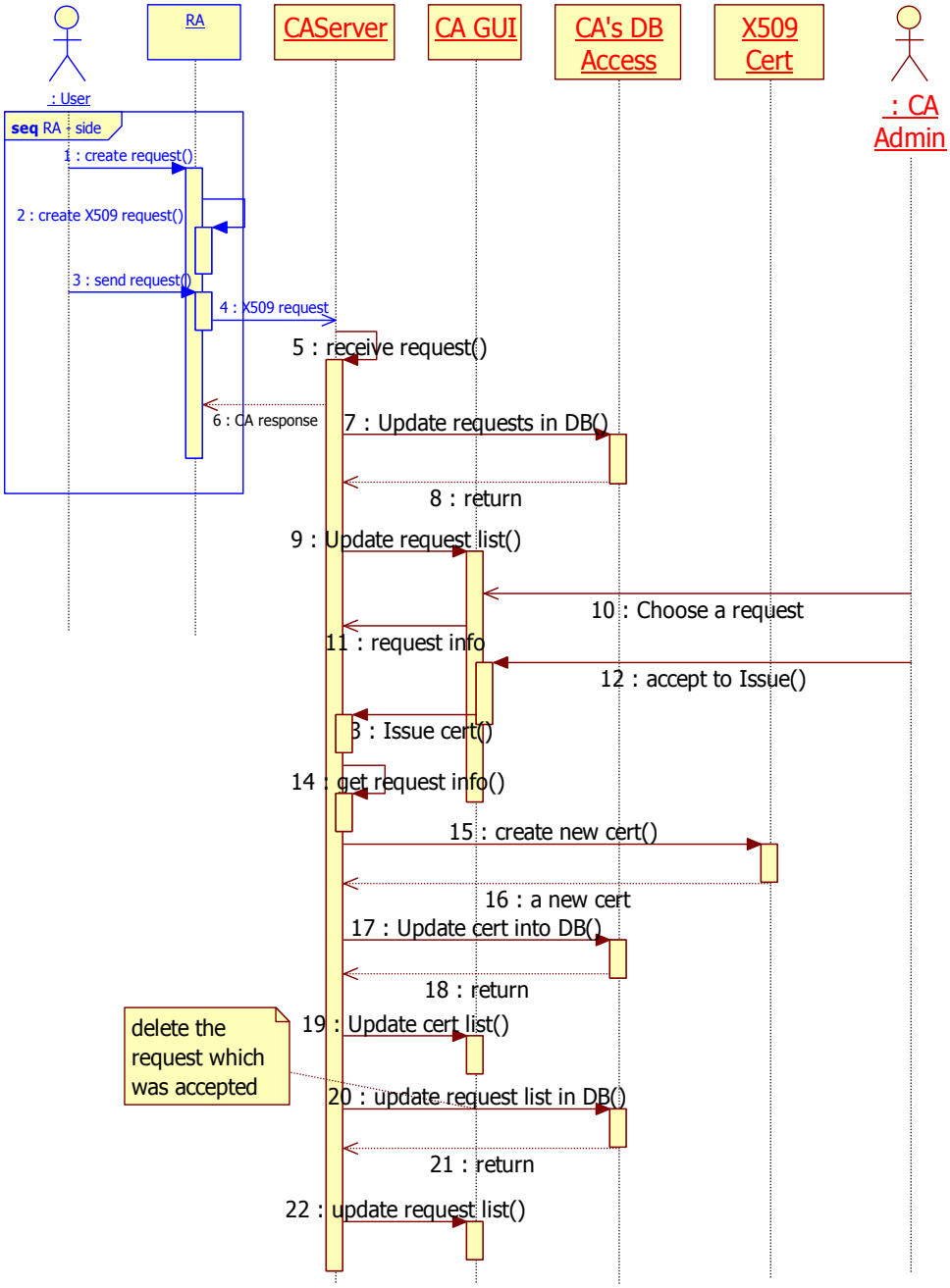


Hình 6.10. Biểu đồ hoạt động thu hồi chứng chỉ

Cấp mới chứng chỉ

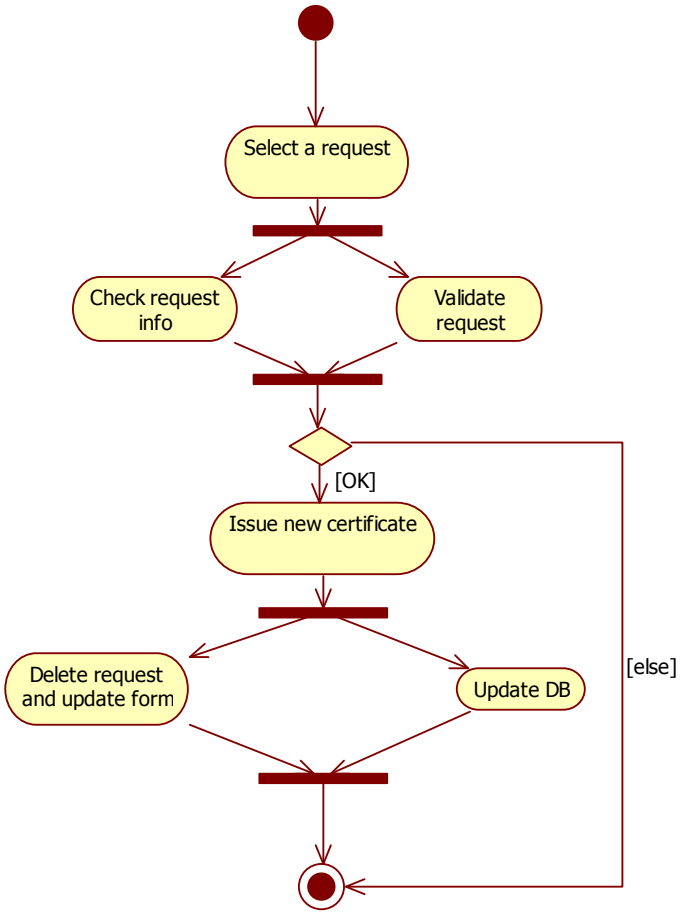
Quá trình cấp mới một chứng chỉ có thể coi bắt đầu từ khi người dùng yêu cầu cấp chứng chỉ Ở đây xét quá trình cấp tại phía CA Server. Biểu đồ diễn tiến chi tiết như hình vẽ dưới đây.

Khi yêu cầu được gửi tới cho CA, yêu cầu này sẽ được lưu vào cơ sở dữ liệu, sau đó giao diện CA Server sẽ được cập nhật để người quản trị biết được. Người quản trị CA (CA Admin) lựa chọn một trong số các yêu cầu cấp chứng chỉ để duyệt cấp. CA kiểm tra các thông tin trong yêu cầu chứng chỉ và sự tương ứng của cặp khóa của yêu cầu đó. Nếu các thông tin hợp lệ thì sẽ cấp mới chứng chỉ cho yêu cầu này. Sau khi tạo mới chứng chỉ, yêu cầu sẽ bị xóa khỏi danh sách chờ duyệt cấp, chứng chỉ mới được cập nhật vào cơ sở dữ liệu của CA. Quá trình cấp chứng chỉ hoàn tất. Từng bước nói trên được thể hiện trên biểu đồ diễn tiến sau:



Hình 6.11. Biểu đồ diễn tiến cấp mới một chứng chỉ cho người dùng

Hoạt động phát hành chứng chỉ có thể được thể hiện trên biểu đồ sau:



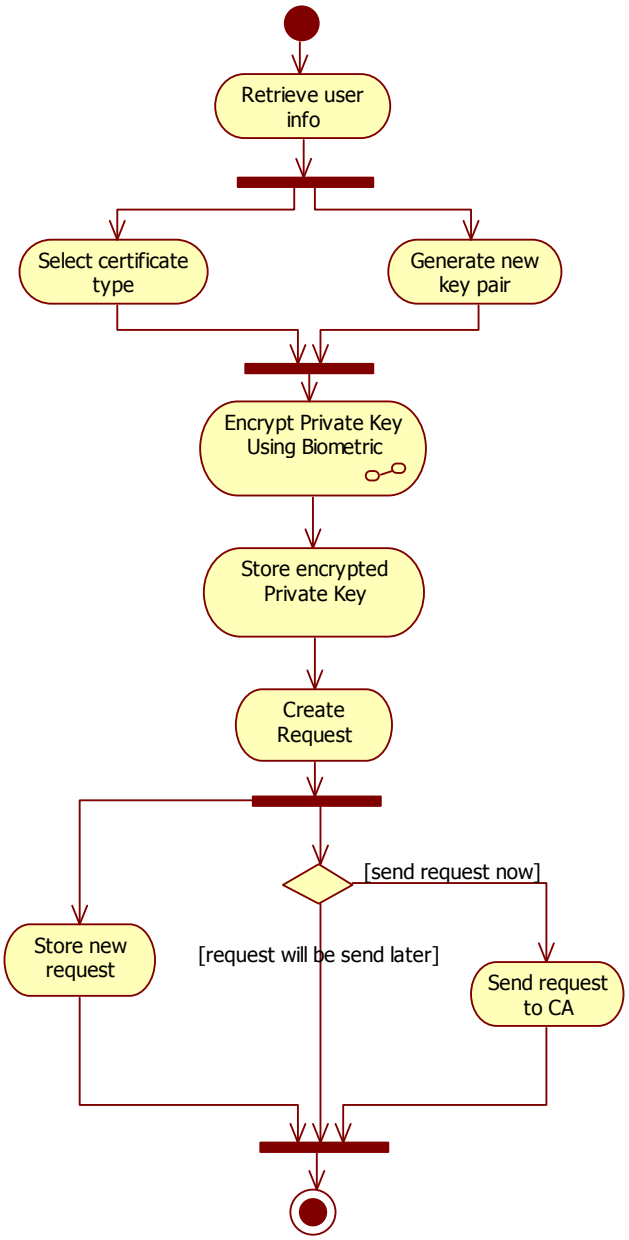
Hình 6.12. Biểu đồ hoạt động phát hành chứng chỉ

Đăng kí người dùng vào hệ thống

Khi một người muốn đăng kí vào hệ thống, người đó sẽ phải chạy chương trình RA Client và kích hoạt chức năng đăng kí người dùng. Hệ thống sẽ hiển thị form để người dùng điền các thông tin đăng nhập. Các thông tin này được dùng để RA sau này quản lý người dùng. Đồng thời, người dùng được yêu cầu quét vân tay để lấy đặc trưng sinh trắc học nhằm mục đích xác thực sau này.

Yêu cầu cấp chứng chỉ

Người dùng chọn tạo yêu cầu chứng chỉ từ giao diện của chương trình. Hệ thống lấy thông tin chung về người dùng từ cơ sở dữ liệu, sau đó hiển thị form để người dùng nhập thông tin bổ sung. RA sẽ sinh cặp khóa cá nhân và công khai cho người dùng. Đặc trưng vân tay được dùng để mã hóa khóa cá nhân và lưu vào cơ sở dữ liệu tại RA. Khóa cá nhân được dùng để kí lên yêu cầu cấp chứng chỉ. Yêu cầu được lưu vào cơ sở dữ liệu và được gửi lên cho CA chờ duyệt cấp.

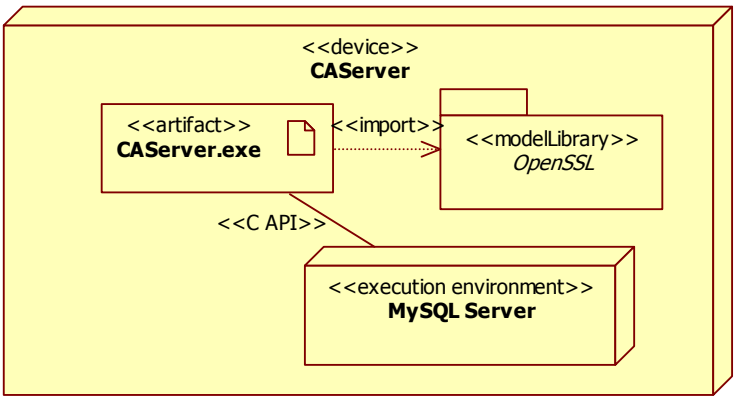


Hình 6.13. Biểu đồ hoạt động tạo yêu cầu cấp chứng chỉ

6.5. Thiết kế các thành phần chính trong cơ sở hạ tầng khóa công khai của hệ thống BK – BioPKI

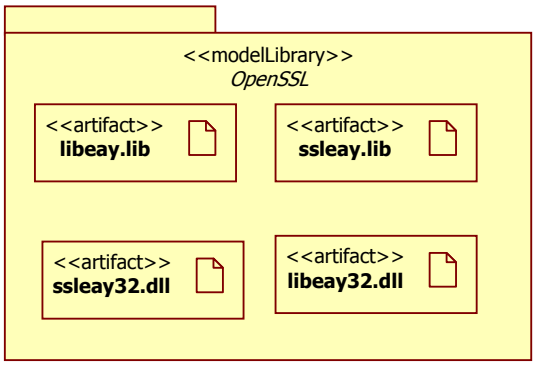
Hệ thống có kiến trúc đơn CA. Việc duyệt cấp, xác định hiệu lực của chứng chỉ là do CA quyết định. Việc sinh cặp khóa và tạo yêu cầu chứng chỉ được thực hiện ở tại các RA. Mỗi RA có thể quản lý nhiều người dùng. Người dùng muốn đăng nhập vào hệ thống thì phải đăng kí với RA, sau đó đăng nhập và thực hiện việc xin cấp, sử dụng các chứng chỉ số do CA duyệt cấp.

CA:



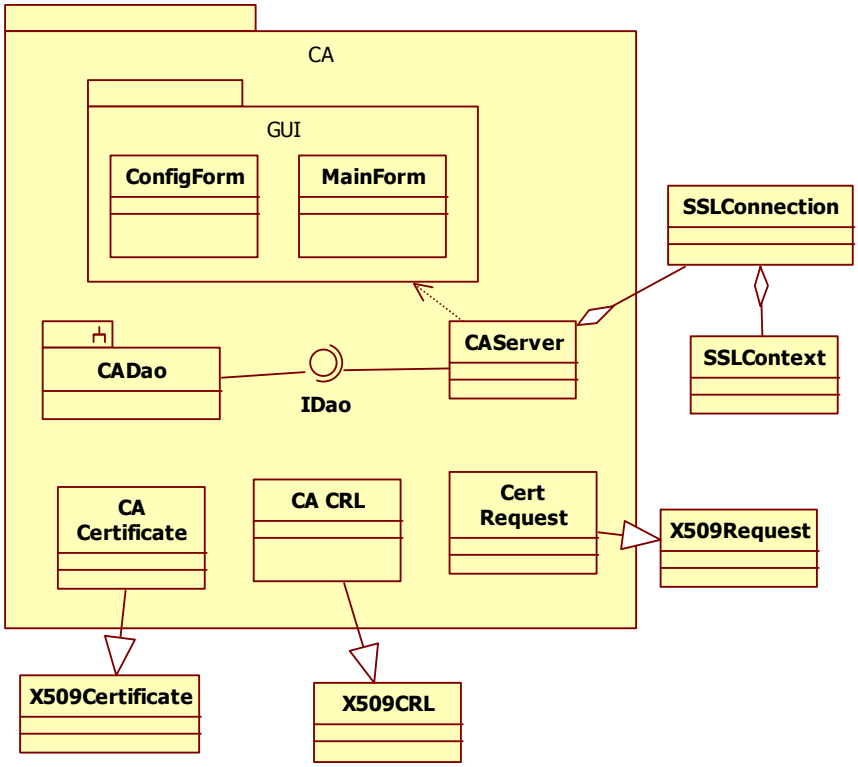
Hình 6.14. CA Server

CA là một phân hệ chính của hệ thống, được cài trên máy Server. CAServer.exe là chương trình thực hiện mọi nhiệm vụ liên quan tới CA. Trên cùng máy Server, có cài hệ quản trị cơ sở dữ liệu MySQL, mọi dữ liệu CA quản lý đều dùng MySQL. Việc tạo mới, cập nhật, thay đổi nội dung cơ sở dữ liệu của CA được gọi qua API của MySQL. CA và RA client đều phải dùng tới thư viện OpenSSL.



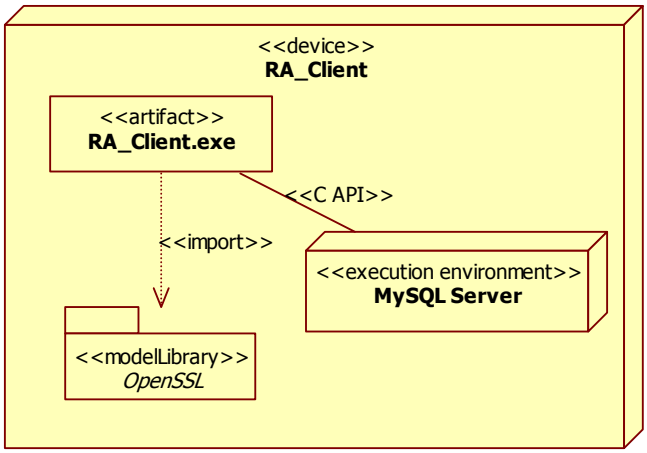
Hình 6.15. Thư viện OpenSSL

CA được thiết kế gồm nhóm các lớp cung cấp giao diện cho người dùng; nhóm các lớp xử lý liên quan tới an toàn an ninh và nhóm các lớp điều khiển hoạt động của CAServer như trong biểu đồ gói dưới đây.



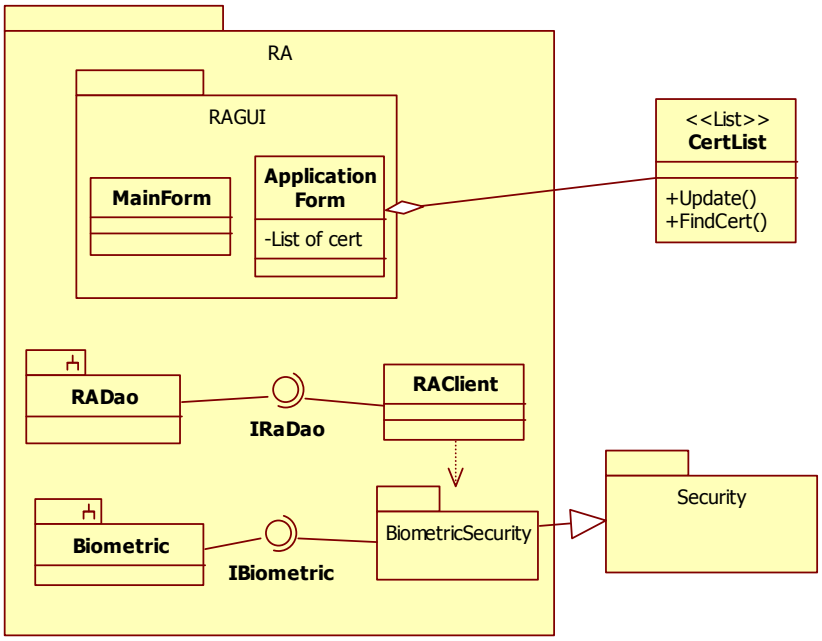
Hình 6.16. Biểu đồ thiết kế lớp của CAServer trong hệ thống BK – BioPKI

RA:



Hình 6.17. RAClient

RAClient là phân hệ chính thứ hai của hệ thống. Nó đảm nhận chức năng của một RA trong hệ PKI, đồng thời là giao diện chính cho người dùng tham gia vào hệ thống BK_BioPKI và sử dụng các dịch vụ của hệ thống. Mỗi RAClient nằm trên một máy PC trong phòng Lab.



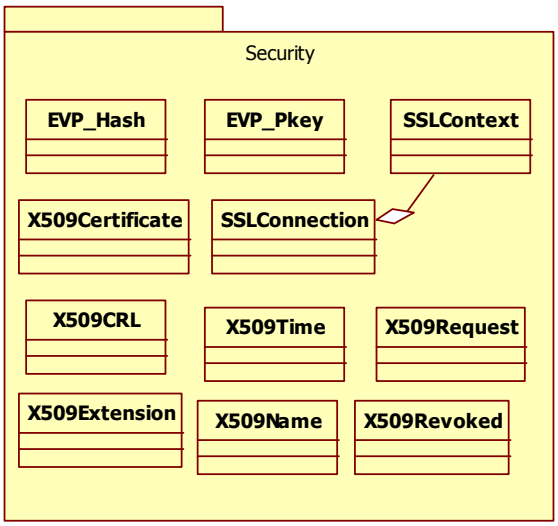
Hình 6.18. Biểu đồ thiết kế lớp cho RAClient

RAClient có cơ sở dữ liệu riêng để quản lý thông tin về người dùng và các chứng chỉ của các người dùng đăng ký với nó. Ở tại mỗi máy Client đều có cài MySQL. RAClient cũng dùng thư viện OpenSSL trong mã hóa, bảo mật.

Yếu tố sinh trắc học được tích hợp ở pha đăng kí người dùng tại RA và trong bước tạo chứng chỉ.

Các lớp liên quan tới bảo mật

Để xây dựng hệ thống BK – BioPKI, một nhóm các lớp được xây dựng từ các hàm của thư viện OpenSSL.



Hình 6.19. Các lớp xây dựng từ thư viện OpenSSL

Lớp EVPHash để thực hiện các hàm băm. Lớp EVPPkey là giao diện để gọi các hàm liên quan tới mã hóa giải mã. Hai lớp SSLConnection và SSLContext phục vụ cho kênh mật theo giao thức SSL. Các lớp X509* là các lớp xây dựng cho việc sử dụng chứng chỉ theo dạng X509.

Chứng chỉ số theo định dạng X509 version 3. Các chứng chỉ có thể dùng để: tạo chữ kí số; mã hóa bảo mật; hoặc dùng trong ứng dụng truy cập từ xa. Riêng chứng cặp chứng chỉ của RA và chứng chỉ SSL của CA được dùng để tạo kênh SSL giữa CA và RA.

6.6. Thiết kế xây dựng và lập trình phần mềm người dùng trong hệ thống BK-bioPKI

6.6.1. Phân tích yêu cầu

Dựa trên các yêu cầu về chức năng và kiến trúc của hệ thống BK-PKI, chương phần mềm người dùng trong hệ thống BK-bioPKI phải đảm bảo các chức năng cơ sở sau:

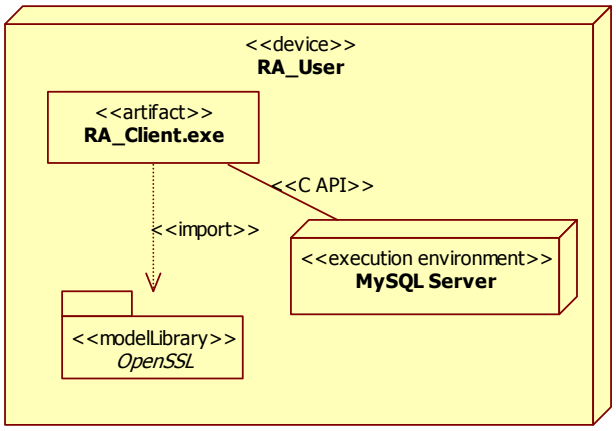
- Thiết lập RA
- Đăng nhập, đăng xuất chương trình
- Xin cấp chứng chỉ
- Gia hạn chứng chỉ
- Thu hồi chứng chỉ
- Sử dụng chứng chỉ
- Quản lý người dùng: đăng kí, sửa đổi, xóa bỏ người dùng.

Như vậy ta có thể thấy phần mềm người dùng trong hệ thống là sự kết hợp giữa RA và End entity trong mô hình hệ thống PKI tổng quát. Phần mềm này vừa đóng vai trò là một RA trong việc giao tiếp với CA (kết nối SSL, gửi yêu cầu, nhận chứng chỉ…) đồng thời lại là nơi để các thực thể đầu cuối (người dùng) thực hiện các chức năng của mình (yêu cầu cấp chứng chỉ, thu hồi chứng chỉ, sử dụng chứng chỉ…).

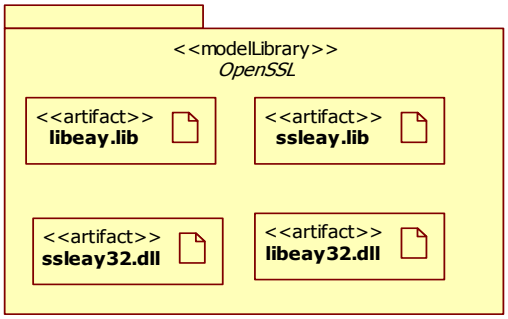
6.6.2. Giải pháp và phân tích các chức năng

- ***Giải pháp***

Phần mềm người dùng trong hệ thống được thiết kế, xây dựng dựa trên giải pháp chung của hệ thống đã trình bày.

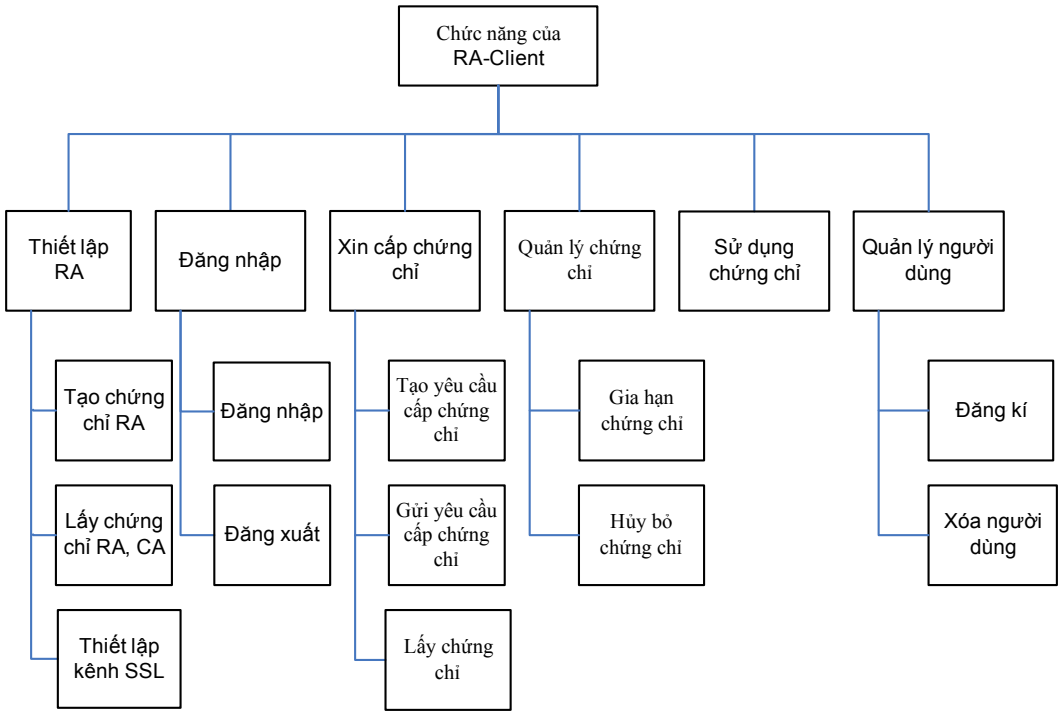


Hình 6.20. Sơ đồ triển khai phần mềm người dùng RA-Client



Hình 6.21. Thư viện OpenSSL

- ***Biểu đồ phân cấp các chức năng cơ sở của phần mềm người dùng trong hệ thống***



Hình 6.22. Các chức năng RA-Client

Các chức năng trong phần mềm người dùng bao gồm:

- Thiết lập RA: đây là chức năng đầu tiên phải thực hiện để có thể thiết lập một hệ thống PKI. Mục đích của chức năng này là đăng kí, thành lập RA. Để thực hiện điều đó, cần phải có một chứng chỉ RA do CA cấp, đồng thời RA cũng phải có chứng chỉ CA để chứng thực CA mà mình kết nối đến. Sau khi RA và CA có cặp chứng chỉ của nhau, kênh mật SSL có thể được thiết lập.
- Đăng nhập: đây là chức năng kiểm soát người truy cập vào chương trình. Để đăng nhập thành công, người dùng cần phải có một user và password đã được đăng kí. Sau khi tích hợp sinh trắc vào hệ thống, ngoài password người dùng sẽ phải sử dụng dấu vân tay của mình để truy cập chương trình. Đi kèm với chức năng đăng nhập là chức năng đăng xuất, giúp người sử dụng thoát khỏi chương trình an toàn.
- Xin cấp chứng chỉ: khi đã truy cập chương trình, người dùng có thể thực hiện chức năng xin cấp chứng chỉ. Để có thể xin cấp chứng chỉ, người dùng cần tạo yêu cầu chứng chỉ, gửi yêu cầu chứng chỉ và cuối cùng là lấy chứng chỉ về (nếu yêu cầu được chấp nhận).
- Quản lý chứng chỉ: người dùng có thể thực hiện chức năng quản lý chứng chỉ của mình bằng cách yêu cầu gia hạn những chứng chỉ sắp hết hạn hoặc yêu cầu thu hồi những chứng chỉ mà mình cảm thấy không an toàn hoặc không cần thiết…
- Sử dụng chứng chỉ: đây là chức năng giúp người dùng có thể lấy được chứng chỉ cùng khóa cá nhân của chứng chỉ đó để sử dụng trong các ứng dụng của hệ thống.
- Quản lý người dùng: chức năng này bao gồm chức năng đăng kí người dùng, thay đổi thông tin người dùng và xóa bỏ người dùng. Đăng kí người dùng cho phép một người sử dụng đăng kí user, password và các thông tin cần thiết khác để có thể đăng nhập hệ thống thành công. Chức năng thay đổi thông tin người dùng cho phép người dùng thay đổi các thông tin về bản thân người dùng đó. Chức năng xóa bỏ người dùng thuộc quyền của RA administrator (người có chứng chỉ RA đăng kí với CA lúc thiết lập RA). Chức năng này cho phép RA administrator có thể xóa bỏ những user được đăng kí tại RA đó.

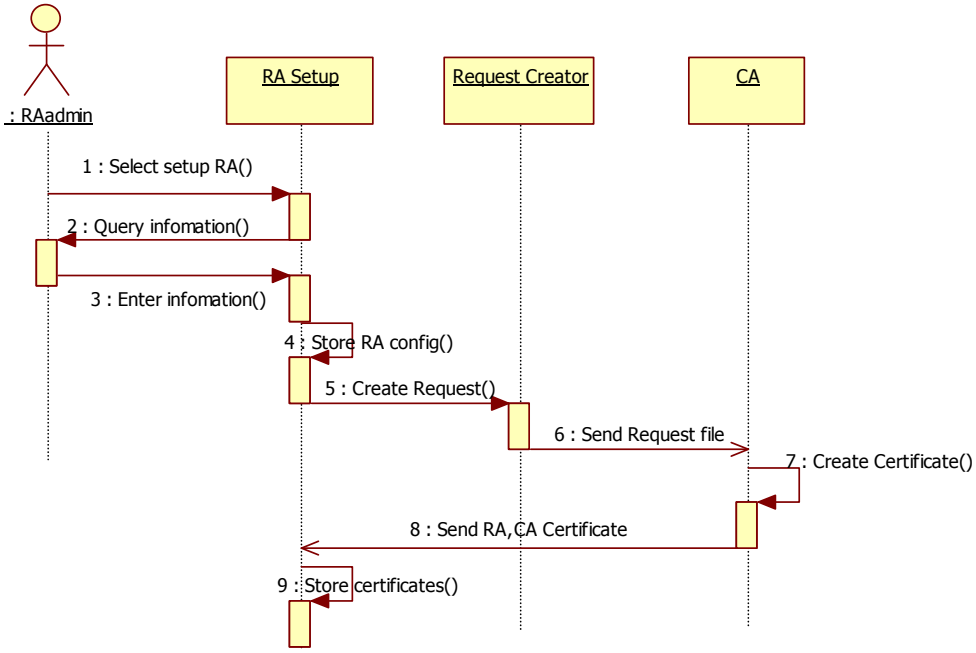
6.6.3. Xây dựng kịch bản các chức năng phần mềm người dùng

Thiết lập RA

Chức năng thiết lập RA là chức năng thực hiện quá trình RA tạo cơ sở dữ liệu, xin cấp chứng chỉ, đồng thời lưu trữ các thông tin cần thiết để có thể liên kết với cơ sở dữ liệu và tạo kênh SSL với CA sau này.

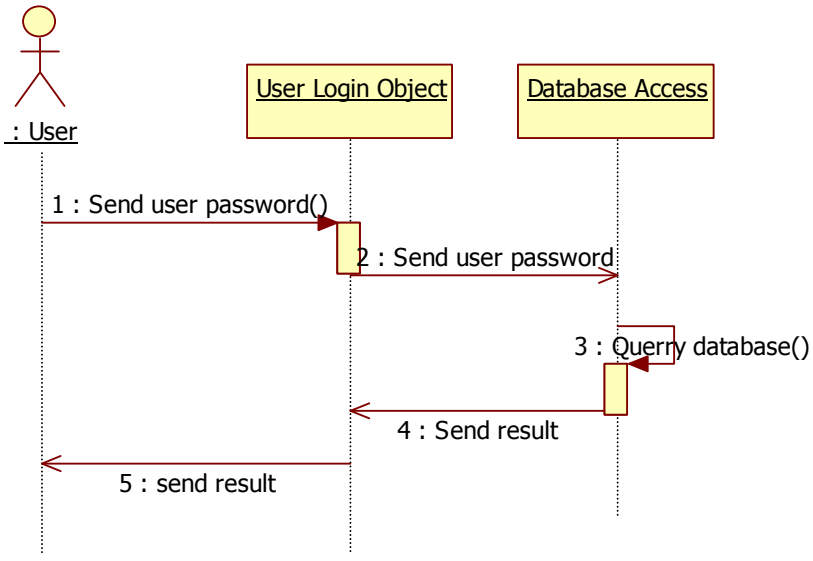
1. RAadmin chọn setup RA từ giao diện chương trình.
2. RAadmin được yêu cầu nhập các thông tin cần thiết (bao gồm thông tin profile, thông tin kết nối CA (ip address), thông tin kết nối cơ sở dữ liệu).
3. RAadmin nhập thông tin theo yêu cầu.
4. RA setup lưu trữ các thông tin này.
5. RA setup gọi hàm Create Request của đối tượng Request Creator.
6. Yêu cầu cấp chứng chỉ được gửi đến CA.
7. CA tạo chứng chỉ theo yêu cầu.

8. Chứng chỉ RA, CA được gửi cho RA thông qua kênh mật (trong trường hợp này là gửi offline).
9. RA setup lưu lại các chứng chỉ để tạo kênh SSL sau này.



Hình 6.23. Kịch bản giao dịch thiết lập RA

Đăng nhập người dùng



Hình 6.24. Kịch bản giao dịch đăng nhập người dùng

Đăng nhập người dùng là chức năng cho phép người dùng được truy cập vào chương trình để thực hiện các chức năng khác của chương trình. Người dùng được chia làm làm loại đó là người dùng bình thường và RA administrator.

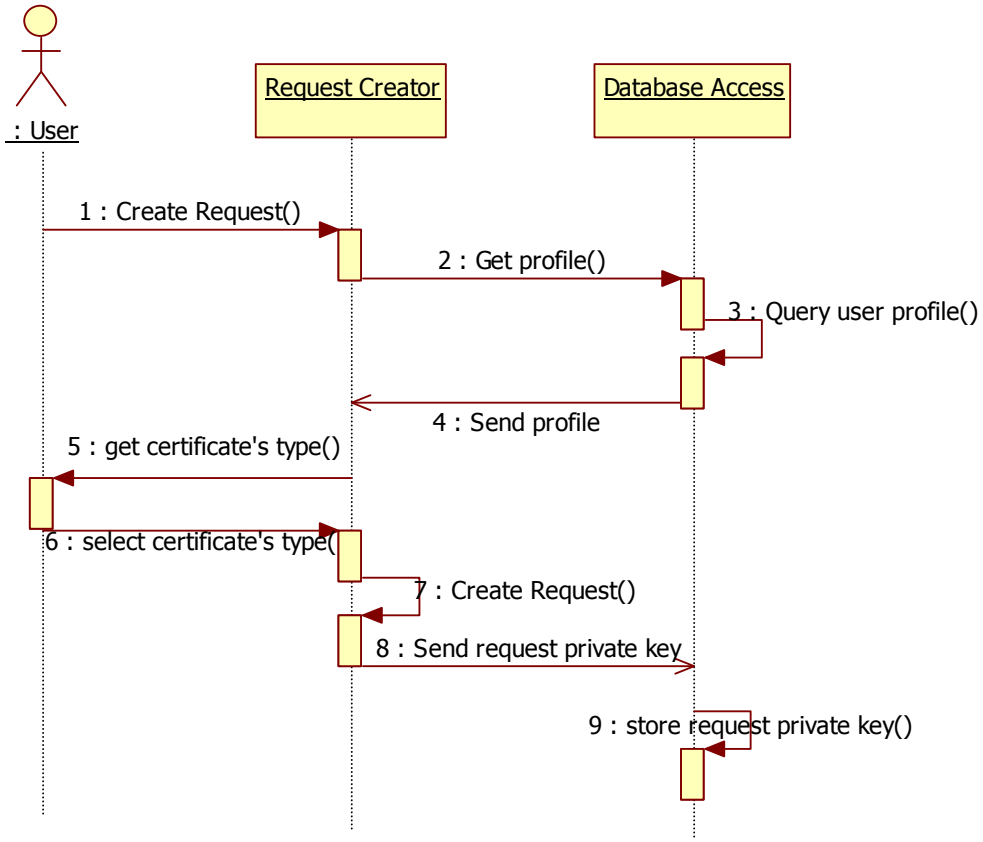
Kịch bản đăng nhập người dùng:

1. Người dùng chạy chương trình, nhập user, password vào form đăng nhập.
2. Đối tượng phụ trách đăng nhập người dùng của hệ thống (User Login Object) gửi user, password cho đối tượng giao tiếp với cơ sở dữ liệu (Database Access).
3. Database Access thực hiện truy vấn dữ liệu (bảng tblUser).
4. Kết quả truy vấn được chuyển cho User Login Object.
5. User Login Object thông báo kết quả đăng nhập cho người dùng. Nếu kết quả đăng nhập là thất bại, người dùng có thể đăng nhập tiếp tối đa 2 lần, nếu vẫn không thành công chương trình sẽ tự động thoát.

Xin cấp chứng chỉ

Chức năng xin cấp chứng chỉ là chức năng thực hiện ba quá trình: quá trình tạo yêu cầu cấp chứng chỉ, quá trình gửi yêu cầu cấp chứng chỉ lên cho CA và quá trình lấy chứng chỉ ở CA về (nếu được đồng ý cấp).

Quá trình tạo yêu cầu cấp chứng chỉ



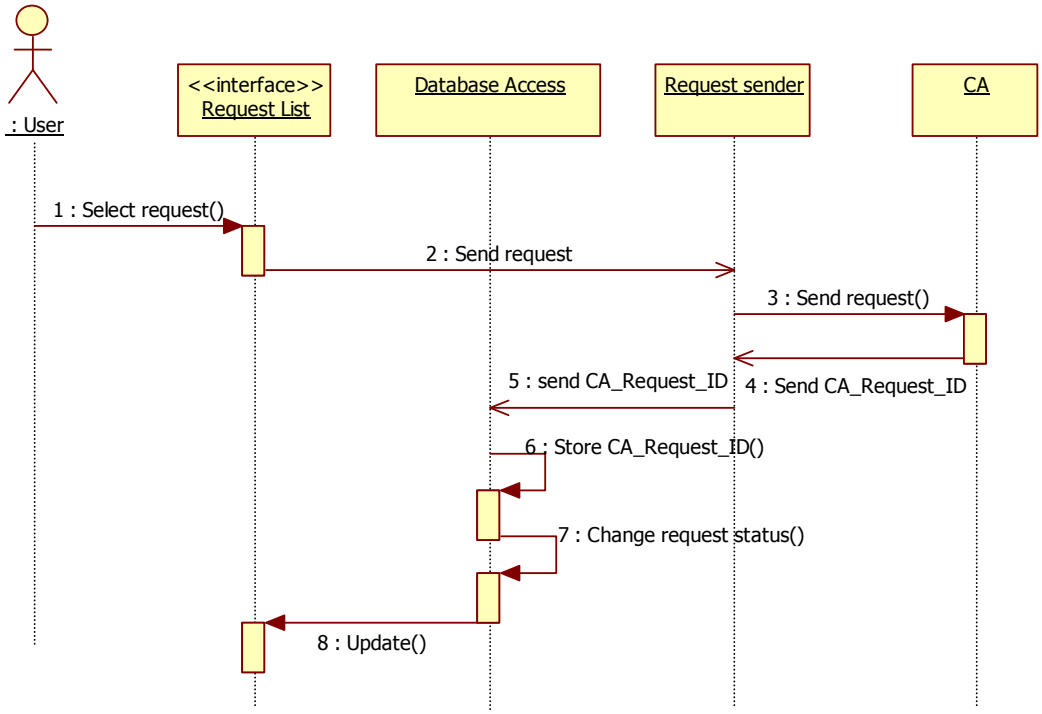
Hình 6.25. Kịch bản giao dịch tạo yêu cầu cấp chứng chỉ.

Kịch bản tạo yêu cầu chứng chỉ:

1. Người dùng yêu cầu tạo yêu cầu cấp chứng chỉ

2. Đối tượng tạo yêu cầu chứng chỉ (Request Creator) gửi yêu cầu lấy profile của người dùng đến đối tượng giao tiếp với cơ sở dữ liệu (Database Access).
3. Database Access thực hiện truy vấn cơ sở dữ liệu để lấy profile của người dùng.
4. Profile của người dùng được gửi đến Request Creator.
5. Người dùng được yêu cầu chọn loại chứng chỉ mà người dùng yêu cầu cấp.
6. Người dùng chọn loại chứng chỉ.
7. Tạo yêu cầu chứng chỉ: bao gồm các quá trình tạo cặp khóa RSA (public key và khóa cá nhân), quá trình tạo yêu cầu và quá trình kí (sử dụng khóa cá nhân vừa tạo) lên yêu cầu.
8. Yêu cầu và privatkey tương ứng vừa tạo được gửi đến Database Access.
9. Database Access lưu yêu cầu, khóa cá nhân vào cơ sở dữ liệu. Trong quá trình này mã yêu cầu cấp chứng chỉ ở RA (RA_request_ID) được tạo ra ứng với yêu cầu đó.

Kịch bản gửi yêu cầu chứng chỉ cho CA

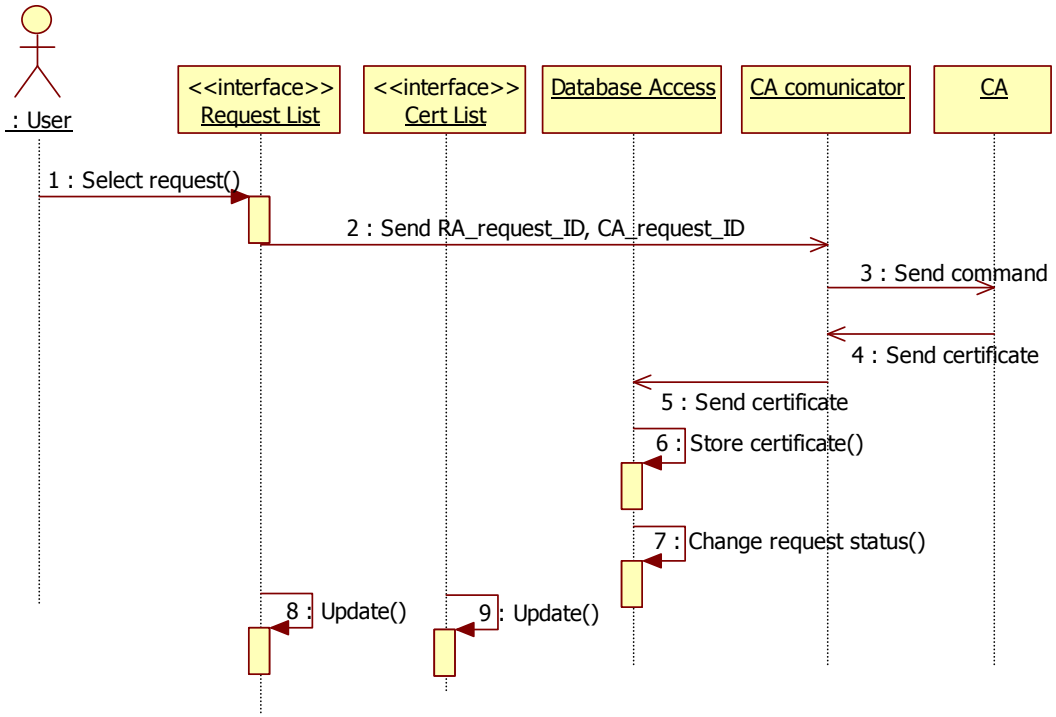


Hình 6.26. Kịch bản giao dịch gửi yêu cầu cấp chứng chỉ.

1. Người dùng chọn yêu cầu gửi cho CA.
2. Yêu cầu được chọn được gửi cho đối tượng phụ trách việc gửi request cho CA (request sender).
3. Request được gửi đến CA thông qua kênh mật SSL.
4. Ngay khi nhận được request, CA gửi trả mã yêu cầu chứng chỉ ở CA (CA_request_ID) cho Request sender.

5. CA_request_ID được gửi cho Database Access để lưu vào cơ sở dữ liệu.
6. CA_request_ID được lưu vào cơ sở dữ liệu tương ứng với yêu cầu đã gửi.
7. Trạng thái của yêu cầu chứng chỉ được sử đổi (submitted).
8. Trạng thái yêu cầu chứng chỉ ở giao diện được cập nhật.

Kịch bản lấy chứng chỉ từ CA



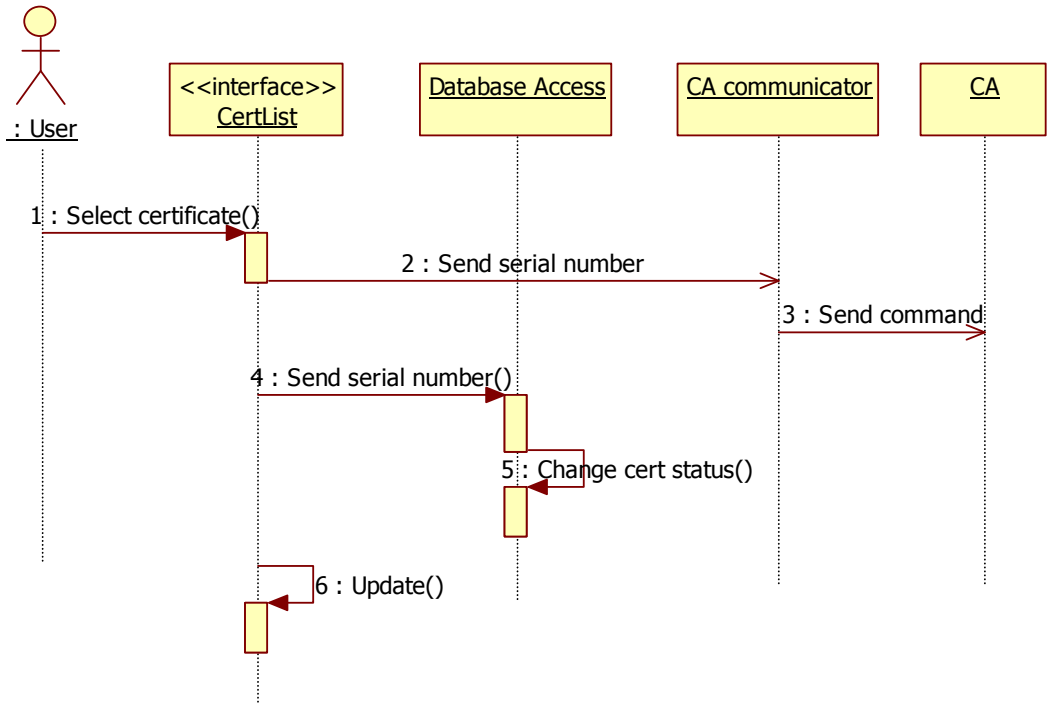
Hình 6.27. Kịch bản giao dịch lấy chứng chỉ

1. Người dùng chọn yêu cầu cấp chứng chỉ từ giao diện chương trình, và yêu cầu lấy chứng chỉ từ CA ứng với yêu cầu cấp chứng chỉ đó.
2. RA_request_ID, CA_request_ID tương ứng với yêu cầu đó được gửi đến đối tượng giao tiếp với CA (CA communicator).
3. CA communicator tạo lệnh lấy chứng chỉ và gửi lệnh đó cho CA. Lệnh lấy chứng chỉ có dạng GETCERT RA_request_ID CA_request_ID.
4. CA nhận được lệnh dựa vào CA_request_ID để tìm chứng chỉ tương ứng. Nếu không có chứng chỉ thì thông báo cho RA, nếu có thì gửi chứng chỉ cho CA communicator.
5. Chứng chỉ được gửi tới Database Access.
6. Chứng chỉ được lưu vào cơ sở dữ liệu.
7. Trạng thái của yêu cầu chứng chỉ tương ứng được sửa đổi (Issued).
8. Trạng thái của yêu cầu chứng chỉ được sửa đổi ở giao diện danh sách yêu cầu.
9. Danh sách chứng chỉ được update.

Gia hạn chứng chỉ

Chức năng gia hạn chứng chỉ gồm quá trình gửi yêu cầu gia hạn chứng chỉ lên CA và quá trình lấy chứng chỉ đã gia hạn (nếu được CA đồng ý) từ CA.

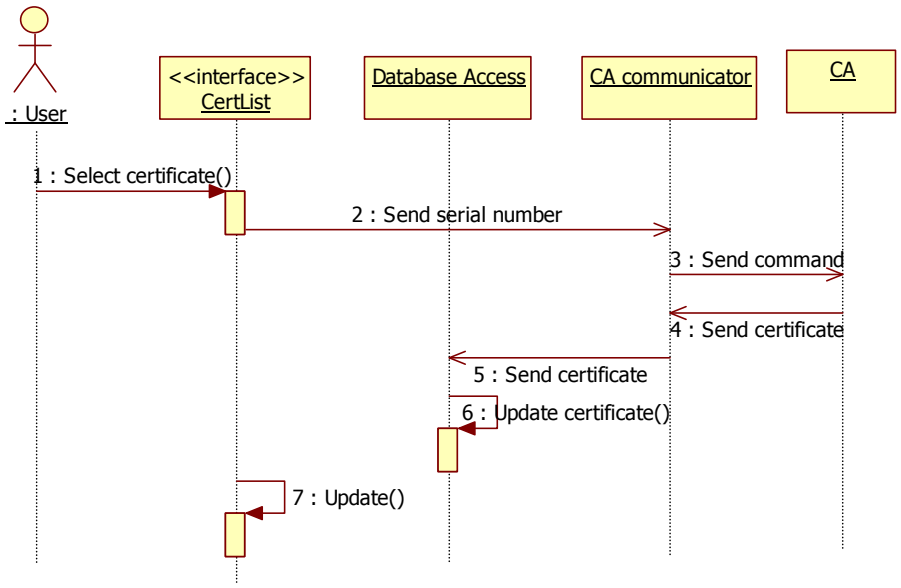
Kịch bản quá trình gửi yêu cầu gia hạn lên CA.



Hình 6.28. Giao dịch giao dịch gia hạn chứng chỉ.

1. Người dùng chọn chứng chỉ cần gia hạn từ danh sách chứng chỉ và yêu cầu gia hạn chứng chỉ.
2. Serial number của chứng chỉ đó được gửi đến CA communicator.
3. CA communicator gửi lệnh gia hạn chứng chỉ đến cho CA. Lệnh gia hạn chứng chỉ có dạng Extend SerialNumber.
4. Serial Number được gửi đến Database Access.
5. Đổi trạng thái của chứng chỉ tương ứng trong cơ sở dữ liệu thành “chờ xin gia hạn”.
6. Cập nhật giao diện danh sách chứng chỉ.

Kịch bản quá trình lấy chứng chỉ đã được gia hạn từ CA.

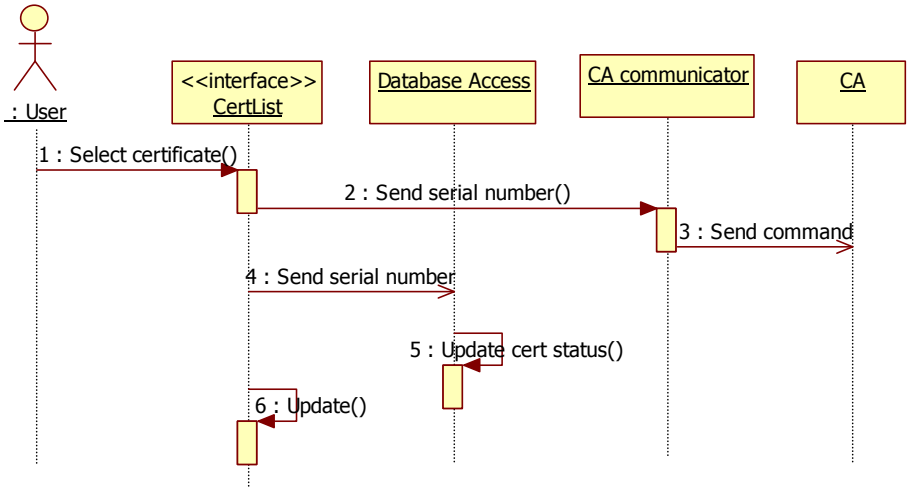


Hình 6.29. Giao dịch giao dịch lấy chứng chỉ đã gia hạn

1. Người dùng chọn certificate có trạng thái đang chờ gia hạn
2. Serial number của chứng chỉ đó được gửi đến CA communicator.
3. CA communicator gửi lệnh lấy chứng chỉ gia hạn đến cho CA.
4. CA nhận được lệnh, dựa vào số serial number để gửi chứng chỉ đã gia hạn cho RA.
5. CA communicator gửi chứng chỉ đã được gia hạn cho Database Access.
6. Database Access dựa vào serial number trong chứng chỉ để thay mới chứng chỉ trong cơ sở dữ liệu, thay đổi trạng thái chứng chỉ.
7. Cập nhật giao diện danh sách chứng chỉ.

Thu hồi chứng chỉ

Thu hồi chứng chỉ là chức năng cho phép người dùng thông báo cho CA biết chứng chỉ mình muốn CA thu hồi.

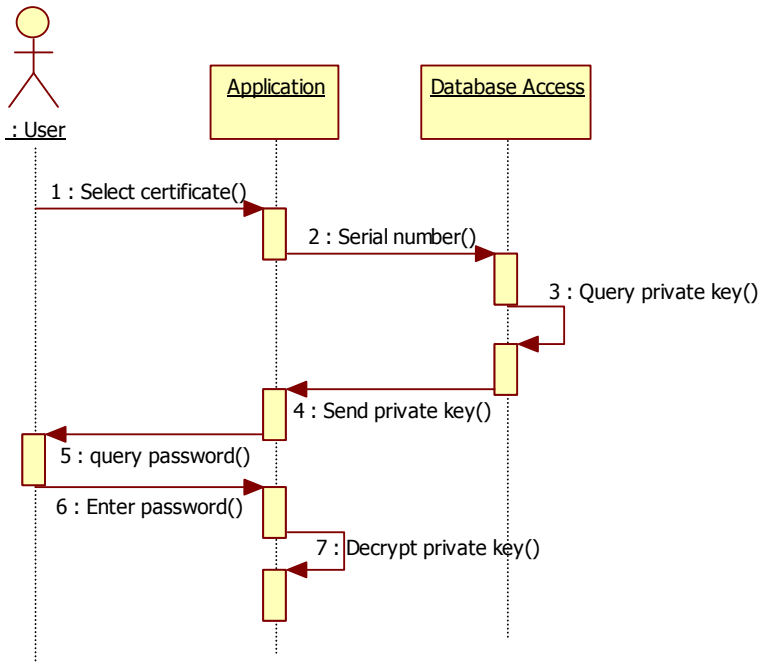


Hình 6.30. Giao dịch thu hồi chứng chỉ.

Kịch bản thu hồi chứng chỉ:

1. Người dùng chọn chứng chỉ cần thu hồi.
2. Serial number được gửi đến CA communicator.
3. CA communicator gửi lệnh thu hồi hồi chứng chỉ cho CA.
4. Serial number được gửi đến Database access.
5. Trạng thái chứng chỉ được update trong cơ sở dữ liệu.
6. Và trong giao diện danh sách chứng chỉ.

Sử dụng chứng chỉ



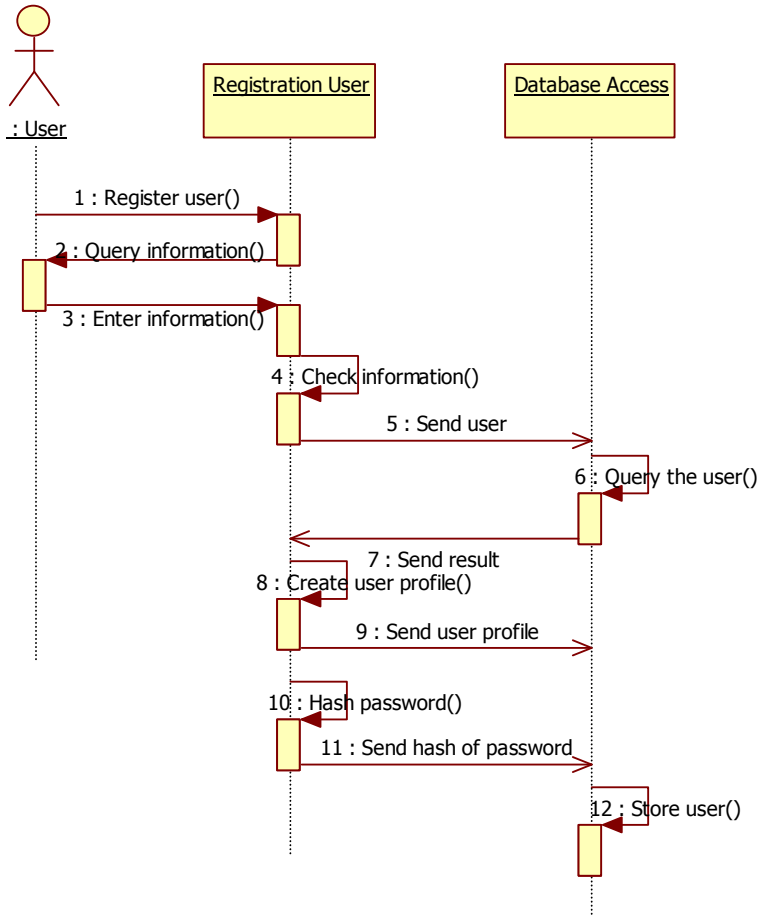
Hình 6.31. Giao dịch sử dụng chứng chỉ.

Việc sử dụng chứng chỉ ở đây mang ý nghĩa là việc lấy và giải mã khóa cá nhân của chứng chỉ đó. Chứng chỉ được sử dụng trong các ứng dụng của chương trình là ứng dụng chữ kí số, ứng dụng mã hóa thông điệp và ứng dụng truy cập từ xa. Kịch bản quá trình này như sau:

1. Người dùng chọn chứng chỉ từ giao diện danh sách chứng chỉ của một ứng dụng cụ thể.
2. Serial number của chứng chỉ đó được gửi đến cho Database Access.
3. Khóa cá nhân (đã được mã hóa bằng password) được lấy từ cơ sơ dữ liệu.
4. Khóa cá nhân được gửi cho ứng dụng.
5. Người dùng được yêu cầu nhập password giải mã.
6. Password được nhập.
7. Khóa cá nhân được giải mã, có thể sử dụng.

Quản lý người dùng trong hệ thống

Đăng kí người dùng

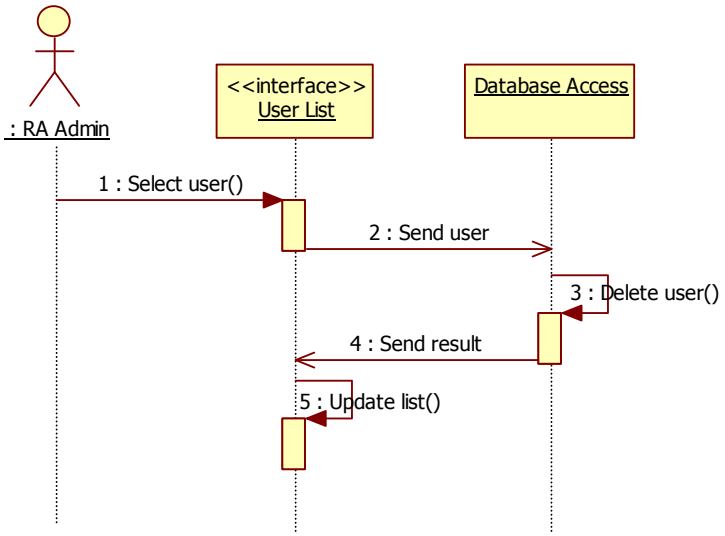


Hình 6.32. Kịch bản giao dịch đăng ký user

1. Người sử dụng chọn đăng kí người dùng từ giao diện của hệ thống.
2. Hệ thống yêu cầu người dùng nhập thông tin.
3. Người dùng điền thông tin theo yêu cầu.
4. Hệ thông kiểm tra thông tin mà người dùng đã nhập.
5. Tên User được gửi đến Database Access.
6. Database Access thực hiện truy vấn xem tên này đã được sử dụng chưa.
7. Gửi kết quả cho Registration User.
8. Nếu user này đã có thì thông báo cho người dùng đặt tên khác, nếu chưa có thì tạo profile cho người dùng.
9. Gửi profile cho Database Access.
10. Băm password của người dùng.
11. Gửi mã băm password cho Database Access.
12. Database Access lưu các thông tin người dùng vào bảng tblUser.

Xóa người dùng:

Chức năng này chỉ xuất hiện khi người dùng đăng nhập với tư cách RA admin. Mục đích của chức năng này là giúp RA admin có thể xóa người dùng trong danh sách quản lý của mình. Việc xóa người dùng liên quan đến rất nhiều vấn đề như chứng chỉ của người dùng đó, các yêu cầu cấp chứng chỉ người dùng đó sẽ ra sao…Do đó việc xây dựng một chính sách phù hợp là rất cần thiết. Tuy nhiên, do điều kiện làm đồ án có hạn nên đồ án này chưa tìm hiểu kĩ được vấn đề này. Hiện tại, khi xóa người dùng thì các chứng chỉ và yêu cầu cấp chứng chỉ cũng bị xóa.



Hình 6.33. Kịch bản xóa người dùng

1. RA admin chọn người dùng cần xóa từ danh sách người dùng.
2. User được gửi đến Database Access.
3. Database Access thực hiện việc xóa user (bao gồm xóa người dùng, các chứng chỉ, yêu cầu cấp chứng chỉ và các khóa cá nhân của người dùng đó).
4. Kết quả của việc xóa người dùng được gửi trả lại.
5. Danh sách người dùng được cập nhật.

6.6.4. Thiết kế cơ sở dữ liệu phần mềm

Sau khi xem xét kịch bản các chức năng của chương trình, xem xét các đối tượng trong chương trình, xây dựng các phụ thuộc hàm trên các đối tượng đó, đồng thời phân tích tính tần suất sử dụng của các đối tượng, cơ sở dữ liệu cho chương trình được thiết kế như sau:

Bảng User

Trường	Khóa chính	Kiểu dữ liệu	Mô tả
User	Yes	Varchar(20)	Tên người sử dụng
Profile	No	BLOB	Lưu trữ thông tin user theo chuẩn X509Name
Password	No	Varchar(20)	Lưu mã băm của password đăng nhập hệ thống của user

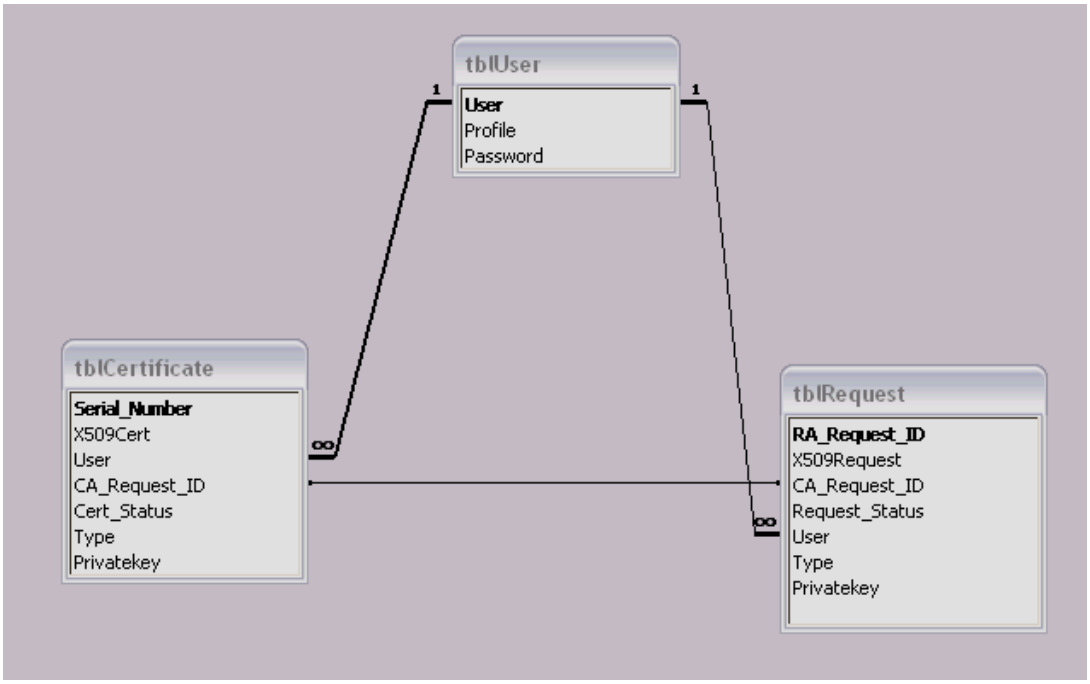
Bảng Request

Trường	Khóa chính	Kiểu dữ liệu	Mô tả
RA RequestID	Yes	Interger	Tự động tăng, dùng làm mã yêu cầu mà RA cung cấp cho user.
X509Request	No	BLOB	Được tạo ra từ X509Name bằng hàm chuẩn của X509
Private key	No	BLOB	Lưu khóa cá nhân khi yêu cầu được tạo ra.
CA RequestID	No	Interger	Đây là mã yêu cầu RA nhận được từ CA ngay khi CA nhận được request. Sử dụng để lấy chứng chỉ từ CA
Request Status	No	Interger	1: Requested 2: Submitted (Request đã được gửi lên CA và nhận được CA RequestID, chỉ khi nhận được cái này rồi mới chuyển) 3: Issued (Yêu cầu đã được chấp nhận) 4: Denied (Yêu cầu bị từ chối)
User	No	Varchar (20)	Khóa ngoài, liên kết nhiều-1 với bảng User.
Type	No	Interger	Loại chứng chỉ được yêu cầu cấp 0: chứng chỉ RA 1: chứng chỉ sử dụng chữ kí số 2: chứng chỉ sử dụng để mã hóa thông điệp 3: chứng chỉ sử dụng để truy cập từ xa

Bảng Certificate

Trường	Khóa chính	Kiểu dữ liệu	Mô tả
Serial Number	Yes	Interger	Serial number của chứng chỉ
X509Cert	No	BLOB	Lưu chứng chỉ dạng pem
User	No	Varchar(20)	Khóa ngoài, lk nhiều – 1 với bảng User
CA RequestID	No	Integer	Được đồng bộ từ bảng Request
Cert Status	No	Integer	1: đang hoạt động 2: bị hủy 3: hết hạn 4: đang gia hạn 5: đang xin hủy
Private key	No	BLOB	Lưu khóa cá nhân, được đồng bộ từ bảng Request
Type	No	Interger	Loại chứng chỉ 0: chứng chỉ RA 1: chứng chỉ sử dụng chữ kí số 2: chứng chỉ sử dụng để mã hóa thông điệp 3: chứng chỉ sử dụng để truy cập từ xa

Quan hệ giữa các bảng:



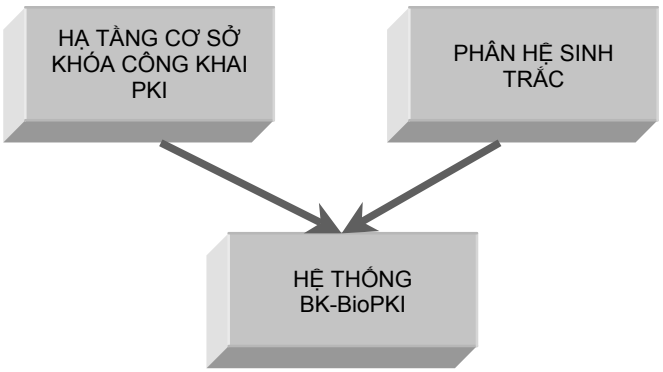
Hình 6.34. Quan hệ các bảng trong CSDL

Chương 7.
THIẾT KẾ TÍCH HỢP HỆ THỐNG AN NINH THÔNG TIN BK-BIOPKI VÀ THỬ NGHIỆM

7.1. Hệ thống tích hợp và yêu cầu thiết kế

Hệ thống BK-BioPKI được thiết kế theo mô hình PKI-CA đơn. Phân hệ sinh trắc sẽ được tích hợp vào cơ sở hạ tầng PKI theo các chức năng sau:

- Đăng kí và kiểm soát đăng nhập người dùng sử dụng dấu sinh trắc vân tay kết hợp password của người dùng.
- Xin cấp chứng chỉ và sử dụng chứng chỉ bằng cách tích hợp sinh trắc vân tay để bảo vệ truy cập khóa cá nhân trong các giao dịch và ứng dụng.



Hình 7.1. Mô hình tích hợp hệ thống

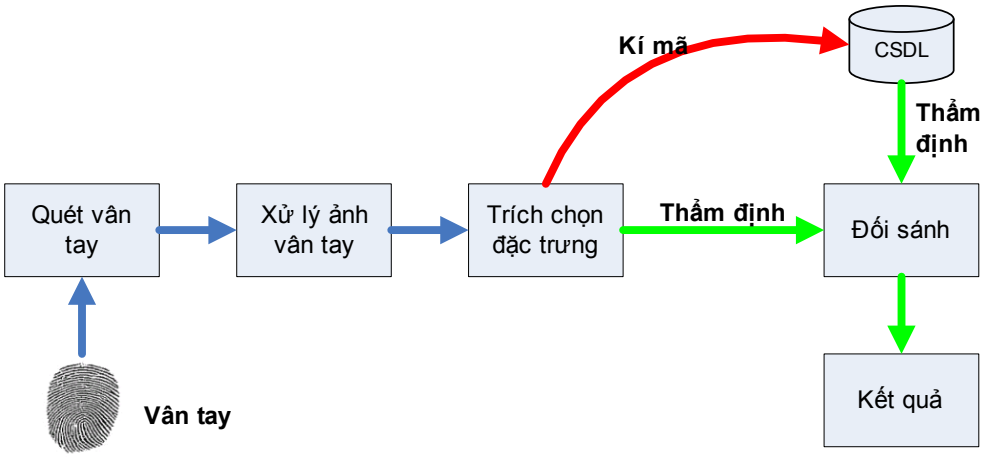
7.2. Đề xuất mô hình tích hợp 2 phân hệ sinh trắc vân tay vào cơ sở hạ tầng PKI thành hệ BK-BioPKI

Phân hệ sinh trắc 1: Xác thực sinh trắc trong hoạt động đăng ký người dùng và đăng nhập hệ thống

Phân hệ sinh trắc 2: Sinh khóa sinh trắc mã hóa bảo mật khóa cá nhân trong các hoạt động xin cấp chứng chỉ và sử dụng chứng chỉ số
Chi tiết hoạt động của mô hình tích hợp được trình bày trong các phần dưới đây

7.3. Thiết kế tích hợp phân hệ sinh trắc 1 thẩm định vân tay người dùng

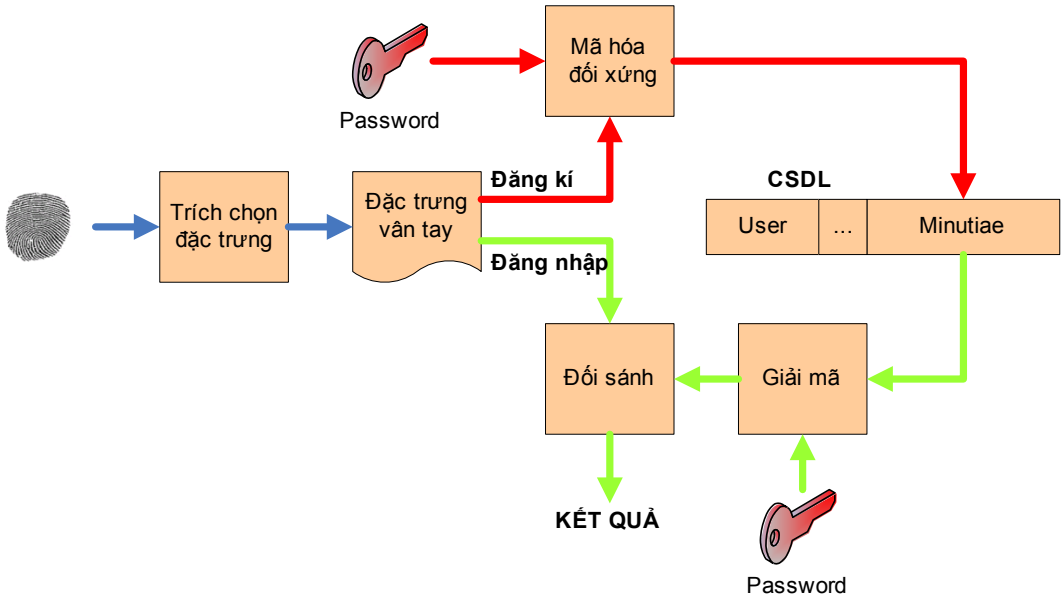
Tích hợp phân hệ sinh trắc 1 vào quá trình đăng ký người dùng



Hình 7.2. Phân hệ sinh trắc thẩm định vân tay người dùng

Phân hệ sinh trắc thẩm định vân tay có đầu vào là vân tay sống của người dùng. Người dùng cho vân tay vào thiết bị quét vân tay, ảnh vân tay được thu nhận và xử lý, sau đó đặc trưng vân tay của người dùng sẽ được trích chọn. Trong quá trình kí mã (enrollment), đặc trưng vân tay được lưu vào cơ sở dữ liệu. Còn trong quá trình thẩm định, đặc trưng vân tay sẽ được đối sánh với đặc trưng đã được giả mã từ cơ sở dữ liệu, từ đó đưa ra kết quả thẩm định.

Phân tích thiết kế tích hợp Phân hệ sinh trắc 1



Hình 7.3. Tích hợp phân hệ sinh trắc 1 thẩm định đăng nhập người dùng trong hệ thống

Để tích hợp phân hệ này vào hệ thống, ta chia phân hệ thành hai phần: phần thứ nhất là phần trích chọn đặc trưng từ vân tay của người dùng lấy trực tiếp, phần thứ hai bao gồm quá trình mã hóa đặc trưng vân tay, lưu vào cơ sở dữ liệu, quá trình đối sánh và đưa ra kết quả. Phần thứ nhất sẽ được thực thi bằng các gọi hàm chạy tiến trình từ hệ thống, phần thứ hai

chính là giao diện tích hợp sẽ được thiết kế trong hệ thống. Hai phần này được giao tiếp thông file text. File text đó là đầu ra của tiến trình phân hệ chứa thông tin các đặc trưng. File text đó như sau: chứa nhiều dòng (số lượng dòng ứng với số điểm đặc trưng), mỗi dòng có 4 số tự nhiên, phân cách nhau bởi 1 dấu cách, như sau:

A B C D

Trong đó: A và B là tọa độ của điểm đặc trưng.

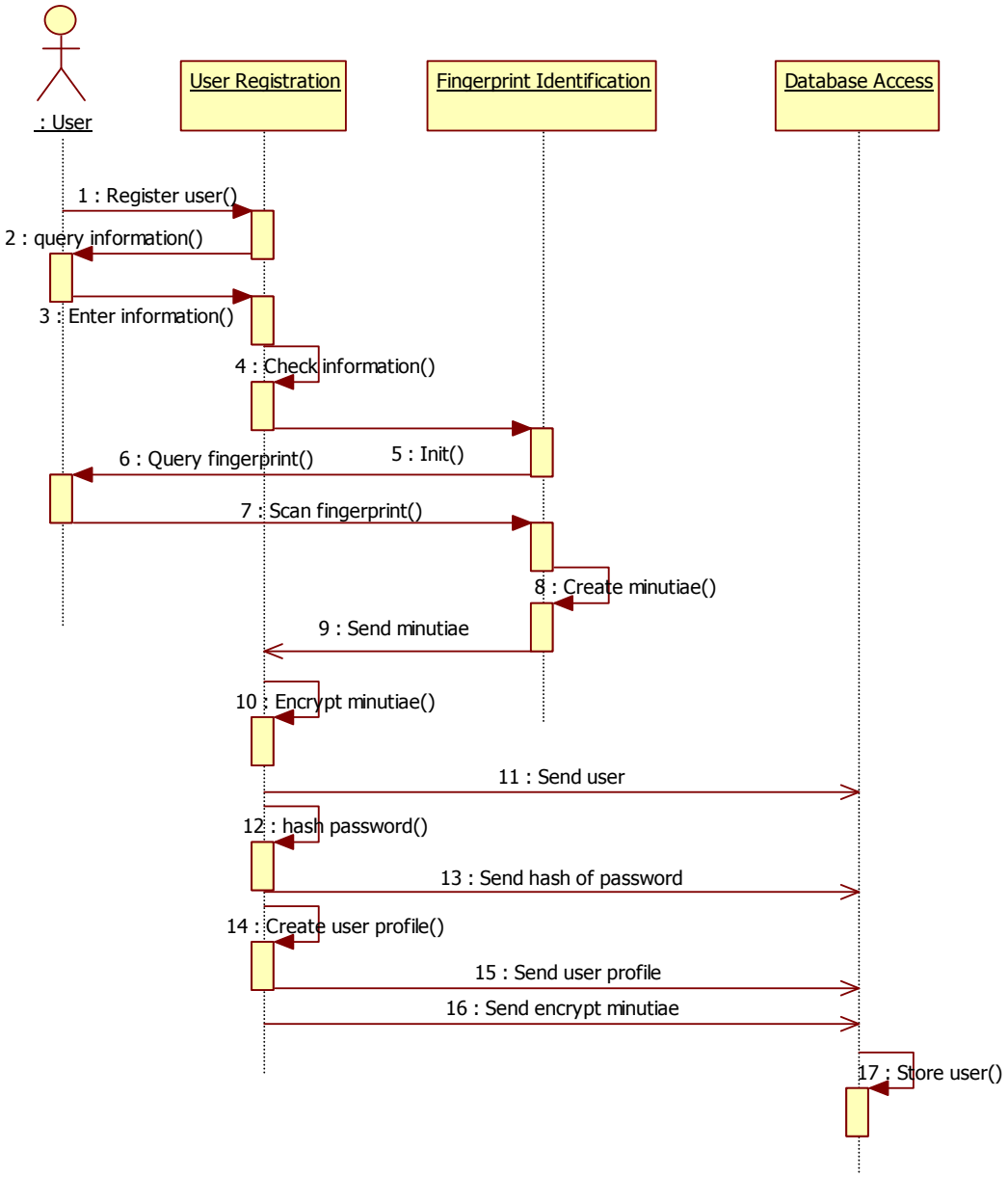
C là hướng của điểm (có 8 hướng ứng với các giá trị từ 0 → 7)

D là kiểu đặc trưng (0: điểm cụt, 1: điểm rẽ nhánh).

Thiết kế kịch bản tích hợp

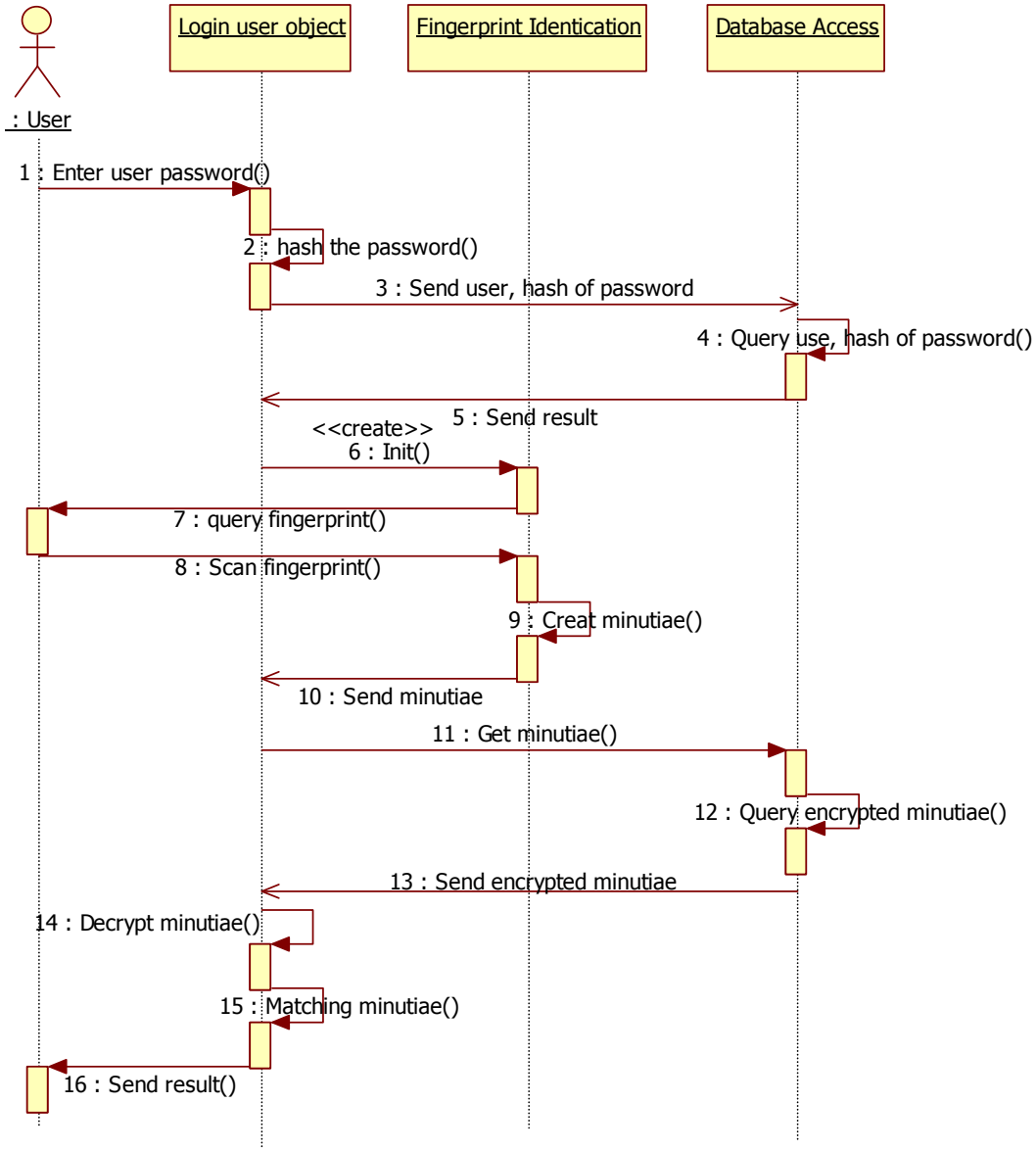
Kịch bản đăng kí user

1. Người dùng yêu cầu đăng kí user.
2. Đối tượng phụ trách đăng kí user (User Registration) yêu cầu người dùng nhập thông tin cần thiết (user, password, comfirm password, comman name, email address, country,...).
3. Người dùng nhập thông tin theo yêu cầu.
4. User registration kiểm tra một số thông tin người dùng nhập vào.
5. Khởi tạo đối tượng thẩm định vân tay người dùng.
6. Yêu cầu người dùng quét vân tay.
7. Người dùng quét vân tay.
8. Đặc trưng vân tay (Minutiae) của người dùng được sinh ra.
9. Minutiae được gửi cho User Registration.
10. Minutiae được mã hóa bằng password của người dùng.
11. Băm password của người dùng.
12. Gửi user cho Database access.
13. Gửi mã băm password cho Database Access.
14. Tạo profile từ thông tin của người dùng.
15. Gửi profile cho Database Access.
16. Gửi Minutiae đã mã hóa cho Database Access.
17. Database lưu trữ tất cả các thông tin nhận được của người dùng.



Hình 7.4. Kịch bản đăng kí người dùng

Kịch bản đăng nhập user



Hình 7.5. Kịch bản đăng nhập người dùng

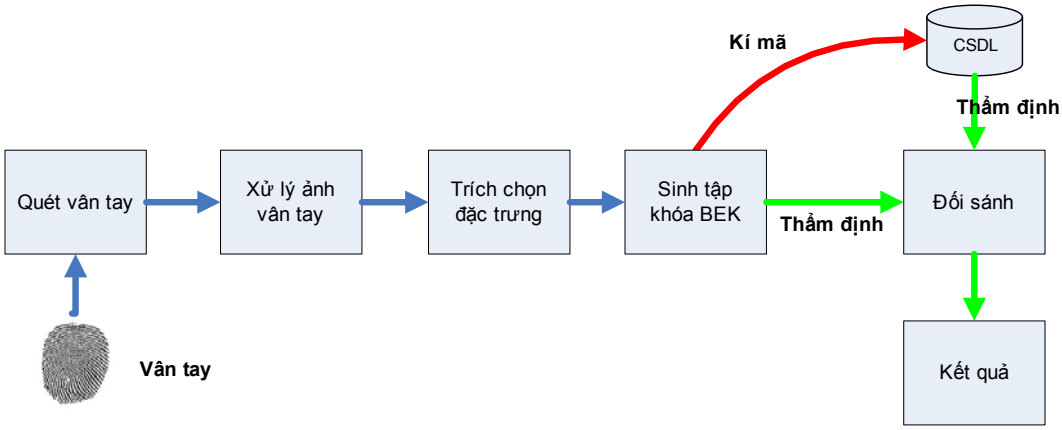
1. Người dùng nhập user, password.
2. Password được băm.
3. User, mã băm của password được gửi đến đối tượng truy cập cơ sở dữ liệu (Database Access).
4. Database Access thực hiện truy vấn cơ sở dữ liệu user và mã băm password.
5. Kết quả truy vân được gửi đến cho đối tượng phụ trách login người dùng (Login user object).

6. Nếu kết quả truy vấn là sai, người dùng phải nhập lại user password, việc nhập lại được tối đa 2 lần. Nếu kết quả truy vấn là đúng, Login user object khởi tạo đối tượng thẩm định vân tay người dùng (Fingerprint Identication).
7. Người dùng được yêu cầu quét vân tay.
8. Người dùng quét vân tay.
9. Minutiae của mẫu vân tay người dùng được tạo.
10. Minutiae được gửi đến Login user object.
11. Login user object gọi hàm Minutiae của Database Access.
12. Database Access truy vấn cơ sở dữ liệu.
13. Minutiae trong cơ sở dữ liệu là minutiae đã được mã hóa được gửi đến cho Login user object.
14. Login user object dùng password của người dùng để giải mã Minutiae (lấy từ cơ sở dữ liệu).
15. Minutiae đã giải mã được so sánh với minutiae tạo ra từ vân tay sống của người dùng.
16. Kết quả so sánh được thông báo cho người dùng. Nếu kết quả đạt, người dùng được đăng nhập hệ thống. Nếu kết quả không đạt, người dùng được quét lại vân tay 2 lần nữa.

7.4. Thiết kế tích hợp Phân hệ sinh trắc 2 sinh khóa sinh trắc bảo vệ khóa cá nhân.

Ở đây, phân hệ sinh trắc sẽ được tích hợp vào hoạt động chức năng cơ sở của PKI đó là xin cấp chứng chỉ và sử dụng chứng chỉ. Việc tích hợp này có mục đích bảo vệ khóa cá nhân bởi vân tay người dùng.

7.4.1. Phân hệ sinh trắc sinh khóa bảo vệ khóa cá nhân

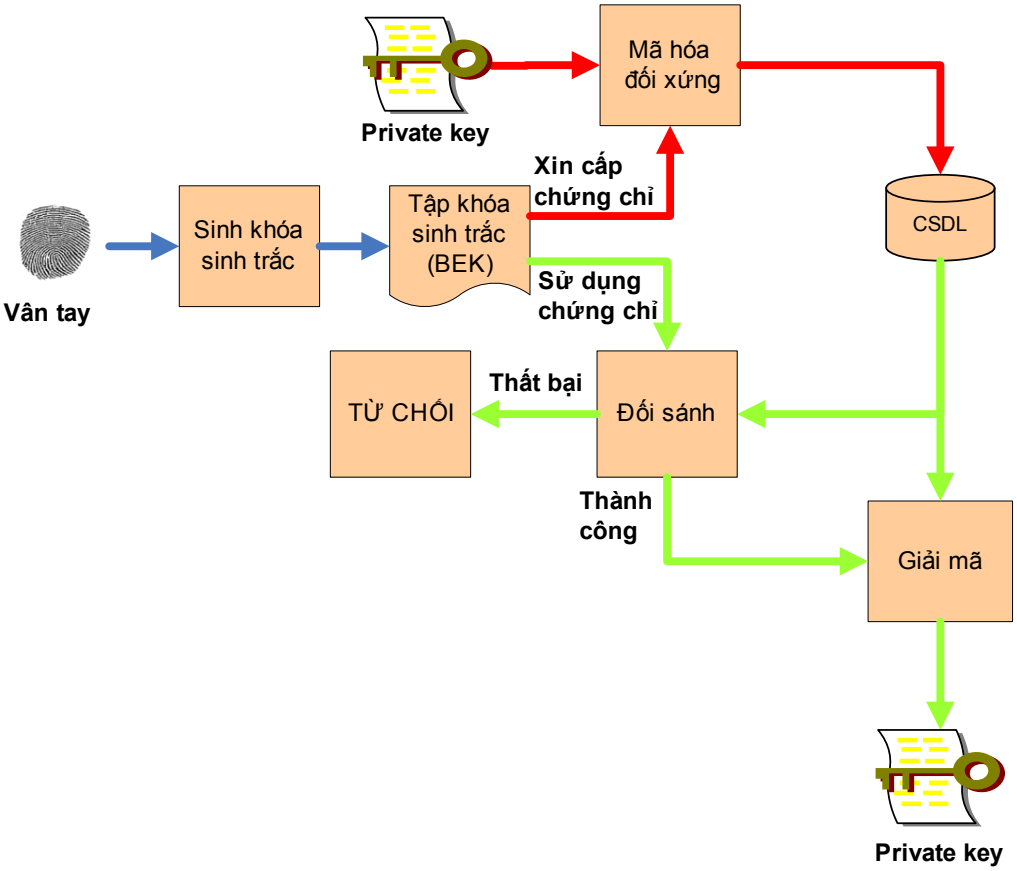


Hình 7.6. Phân hệ sinh trắc học sinh khóa bảo vệ khóa cá nhân

Phân hệ sinh trắc sinh khóa bảo vệ khóa cá nhân có đầu vào là vân tay sống của người dùng. Người dùng cho vân tay vào thiết bị quét vân tay, ảnh vân tay được thu nhận và xử lý, sau đó đặc trưng vân tay của người dùng sẽ được trích chọn. Từ đặc trưng vân tay, tập khóa

BEK (Biometric encryption key) được sinh ra. Trong quá trình kí mã (enrollment), tập khóa BEK được lưu vào cơ sở dữ liệu (lưu mã băm của từng khóa). Còn trong quá trình thẩm định, tập khóa BEK sẽ được đối sánh với tập khóa BEK (mã băm) từ cơ sở dữ liệu, từ đó đưa ra kết quả thẩm định.

7.4.2. Mô hình tích hợp phân hệ sinh trắc sinh khóa bảo vệ khóa cá nhân vào hệ thống và thiết kế hệ thống



Hình 7.7. Mô hình tích hợp phân hệ sinh trắc 2 sinh khóa bảo vệ khóa cá nhân vào hệ thống.

Phân hệ sinh trắc sinh khóa bảo vệ khóa cá nhân được tích hợp vào hệ thống một cách hoàn toàn, thống nhất theo ba thành phần sau: thành phần quét và thu nhận ảnh vân tay trực tiếp từ vân tay người dùng thông qua thiết bị quét vân tay, thành phần sinh khóa sinh trắc học và thành phần giao diện tích hợp với hạ tầng cơ sở PKI đã có. Hai thành phần quét, thu nhận vân tay và sinh khóa sinh trắc được giữ nguyên để tích hợp và hệ thống. Riêng thành phần thứ ba có những thay đổi so với phân hệ ban đầu. Cụ thể như sau: quá trình kí mã được tích hợp vào hoạt động xin cấp chứng chỉ (cụ thể là quá trình tạo yêu cầu cấp chứng chỉ), và quá trình thẩm định được tích hợp vào hoạt động sử dụng chứng chỉ của hệ thống PKI. Trong quá trình xin cấp chứng chỉ, tập khóa BEK được dùng để mã hóa khóa cá nhân trước khi bị băm ra thay vì chỉ bị băm ra như trong quá trình kí mã. Còn trong quá trình đối sánh, kết quả

của quá trình này sẽ là khóa cá nhân đã được giải mã hoặc là NULL (nếu đối sánh không thành công).

Như vậy ta cần phải thiết kế cơ sở dữ liệu để lưu trữ khóa cá nhân đã mã hóa, tập mã băm BEKs. Khóa cá nhân cần được mã hóa bởi tập BEKs gồm 125 khóa khác nhau. Trong quá trình sử dụng, khóa cá nhân sẽ được giải mã từ một trong 125 private đã mã hóa. Do đó, để thuận tiện cho việc lưu trữ cũng như truy vấn cơ sở dữ liệu, ta thiết kế một bảng riêng để lưu trữ khóa cá nhân. Bảng này được liên kết với bảng tblRequest thông qua trường RA_request_ID. Cụ thể cơ sở dữ liệu mới của chương trình như sau:

Bảng User

Trường	Khóa chính	Kiểu dữ liệu	Mô tả
User	Yes	Varchar(20)	Tên người sử dụng
Profile	No	BLOB	Lưu trữ thông tin user theo chuẩn X509Name
Password	No	Varchar(20)	Lưu mã băm của password đăng nhập hệ thống của user
Fingerprint	No	BLOB	Lưu trữ vân tay của user ngay lúc đăng kí

Bảng Request

Trường	Khóa chính	Kiểu dữ liệu	Mô tả
RA RequestID	Yes	Interger	Tự động tăng, dùng làm mã yêu cầu mà RA cung cấp cho user.
X509Request	No	BLOB	Được tạo ra từ X509Name bằng hàm chuẩn của X509
CA RequestID	No	Interger	Đây là mã yêu cầu RA nhận được từ CA ngay khi CA nhận được request. Sử dụng để lấy chứng chỉ từ CA
Request Status	No	Interger	0: Requested 1: Submitted (Request đã được gửi lên CA và nhận được CA RequestID, chỉ khi nhận được cái này rồi mới chuyển) 2: Issued (Yêu cầu đã được chấp nhận) 3: Denied (Yêu cầu bị từ chối)
User	No	Varchar (20)	Khóa ngoài, liên kết nhiều -1 với bảng User.
Type	No	Interger	Loại chứng chỉ được yêu cầu cấp 0: chứng chỉ RA 1: chứng chỉ sử dụng chữ kí số 2: chứng chỉ sử dụng để mã hóa thông điệp 3: chứng chỉ sử dụng để truy cập từ xa

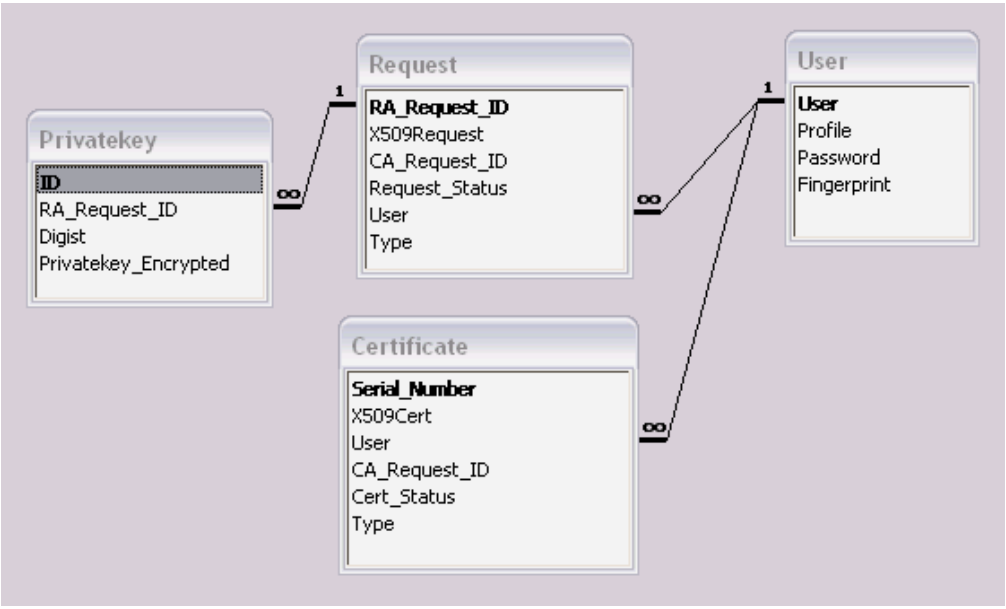
Bảng Certificate

Trường	Khóa chính	Kiểu dữ liệu	Mô tả
Serial Number	Yes	Interger	Serial number của chứng chỉ
X509Cert	No	BLOB	Lưu chứng chỉ dạng pem
User	No	Varchar(20)	Khóa ngoài, lk nhiều – 1 với bảng User
CA RequestID	No	Integer	Được đồng bộ từ bảng Request
Cert Status	No	Integer	1: đang hoạt động 2: bị hủy 3: hết hạn 4: đang gia hạn 5: đang xin hủy
Type	No	Interger	Loại chứng chỉ 0: chứng chỉ sử dụng chữ kí số 1: chứng chỉ sử dụng để mã hóa thông điệp 3: chứng chỉ sử dụng để truy cập từ xa

Bảng Khóa cá nhân

Trường	Khóa chính	Kiểu dữ liệu	Mô tả
ID	Yes	Interger	Tự động tăng
RARequestID	No	Interger	Mã yêu cầu ở RA
Digist	No	Varchar(30)	Mã băm của từng đặc trưng vân tay
Khóa cá nhân_Encryptedkey	No	BLOB	Chứa khóa cá nhân được mã hóa bởi từng đặc trưng vân tay tương ứng

Quan hệ giữa các bảng

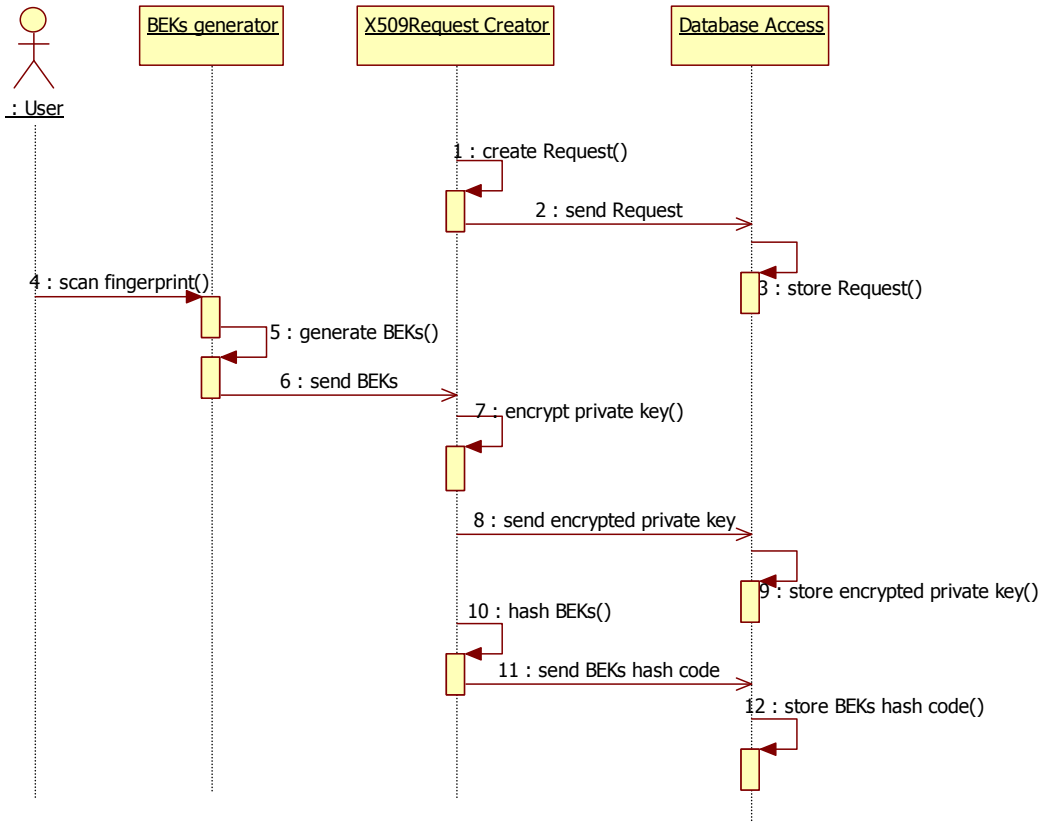


Hình 7.8. Quan hệ giữa các bảng trong CSDL

7.4.3. Thiết kế các kịch bản hoạt động tích hợp

- **Kịch bản quá trình xin cấp chứng chỉ**

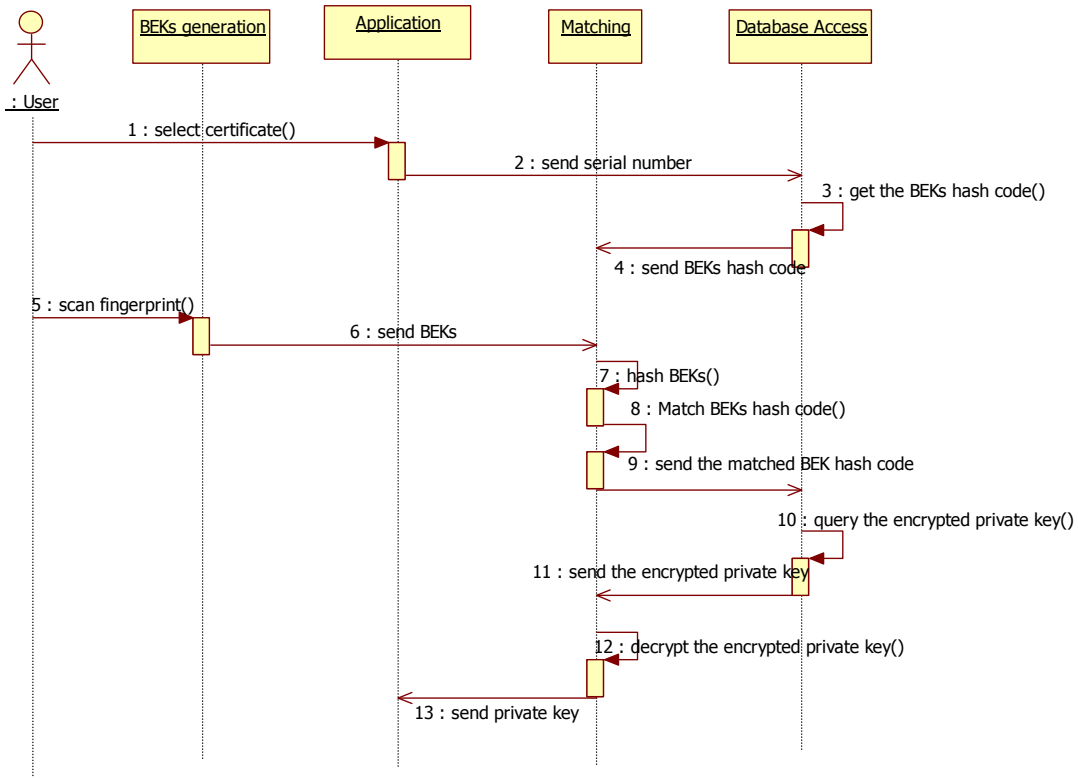
Quá trình lưu trữ khóa cá nhân nằm trong quá trình tạo yêu cầu chứng chỉ. Sau đây là kịch bản chi tiết của quá trình này:



Hình 7.9. Kịch bản tạo yêu cầu chứng chỉ

1. Khi người dùng yêu cầu tạo yêu cầu xin cấp chứng chỉ, quá trình tạo chứng chỉ được thực hiện.
2. Yêu cầu cấp chứng được chuyển tới đối tượng giao tiếp với cơ sở dữ liệu.
3. Yêu cầu cấp chứng chỉ được lưu vào cơ sở dữ liệu.
4. Người dùng được yêu cầu quét vân tay.
5. Sinh tập khóa bảo vệ khóa cá nhân (BEKs) từ vân tay của người dùng.
6. BEKs được chuyển đến Request Creator.
7. BEKs được dùng làm khóa để mã hóa khóa cá nhân (mã hóa đối xứng –DES)
8. Tập khóa cá nhân đã được mã hóa được chuyển tới đối tượng giao tiếp với cơ sở dữ liệu
9. Tập khóa cá nhân đã mã hóa được lưu vào cơ sở dữ liệu (tương ứng với mã yêu cầu chứng chỉ ở RA).
10. Tập khóa mã hóa khóa cá nhân-BEKs được băm từng BEK.
11. Chuyển tập mã băm của BEKs đến đối tượng giao tiếp với cơ sở dữ liệu.
12. Lưu tập mã băm của BEKs vào cơ sở dữ liệu (tương ứng với mã yêu cầu chứng chỉ ở RA và tập khóa cá nhân đã được mã hóa).

- **Kịch bản quá trình sử dụng chứng chỉ**



Hình 7.10. Kịch bản sử dụng chứng chỉ

Quá trình sử dụng private khi người dùng cần sử dụng chứng chỉ trong các ứng dụng cụ thể của chương trình như: ứng dụng chữ kí số, ứng dụng truy cập từ xa và ứng dụng mã hóa thông điệp.

1. Người dùng chọn chứng chỉ sẽ sử dụng từ giao diện của một trong các ứng dụng trên.
2. Serial number của chứng chỉ được chọn được gửi đến đối tượng giao tiếp cơ sở dữ liệu (Database access).
3. Dựa vào serial number, tập mã băm BEKs tương ứng được truy vấn từ cơ sở dữ liệu.
4. Tập mã băm BEKs được gửi đến đối tượng đối sánh vân tay (Matching).
5. Người dùng được yêu cầu quét vân tay để đối sánh.
6. Tập BEKs lại được sinh ra từ vân tay sống của người dùng.
7. Tập BEKs này được gửi đến đối tượng đối tượng đối sánh.
8. Tập BEKs này được băm lần lượt từng khóa.
9. Lần lượt mã băm của từng khóa được so sánh với tập mã băm BEKs lấy từ cơ sơ dữ liệu. Nếu không có mã băm nào giống nhau thì thông báo từ chối cho phép sử dụng khóa cá nhân (chứng chỉ). Nếu có mã băm giống với một mã băm trong tập mã băm BEKs lấy từ cơ sở dữ liệu thì tiếp bước mã băm được matching này được gửi đến Database access.

10. Dựa vào mã băm này cùng với serial number, khóa cá nhân đã được mã hóa được truy vấn từ cơ sở dữ liệu.
11. Khóa cá nhân đã được mã hóa này được gửi đến cho đối tượng đối sánh.
12. BEK tương ứng được dùng để giải mã khóa cá nhân.
13. Gửi khóa cá nhân đã giải mã đến ứng dụng cần sử dụng.

7.5. Xây dựng thử nghiệm ứng dụng chữ ký số trong hệ thống BK-BioPKI và thử nghiệm

Đây là một ứng dụng cơ bản của hệ PKI. Mục này đi sâu chi tiết vào ứng dụng và sẽ trình bày từ nguyên lý cho tới thiết kế cài đặt ứng dụng trong hệ thống BK-BioPKI. Trong ứng dụng đã có tích hợp yếu tố sinh trắc học theo hướng dùng đặc trứng sinh trắc học để bảo vệ khóa cá nhân.

7.5.1. Mục đích của chữ kí số

Chữ kí số ra đời cùng với kĩ thuật mã hóa bất đối xứng, nó giải quyết được vấn đề kí dấu đặc trưng trước đó không thể thực hiện được trong hệ mã hóa đối xứng. Ngày nay đã nó trở thành một ứng dụng phổ biến trong các giao dịch điện tử. Mục này sẽ trình bày một số khái niệm quan trọng có liên quan tới chữ kí số.

7.5.2. Vấn đề xác thực

Cùng với sự phát triển mạnh mẽ của mạng Internet và các công nghệ mới, các giao dịch điện tử cũng đã tăng lên không ngừng. Để đảm bảo cho các giao dịch thành công thì xác thực là một đòi hỏi tất yếu. Giống như trong các giao dịch truyền thống từ trước tới nay, trong giao dịch điện tử cũng cần phải có sự xác thực chủ thể và xác thực các nội dung trao đổi. Việc xác thực càng trở nên quan trọng hơn trong môi trường mở như mạng Internet với nhiều kiểu tấn công đa dạng.

Trong một giao dịch điện tử, bài toán xác thực nhằm giải quyết hai vấn đề chính là giả mạo thông điệp và mạo danh. Xác thực, theo [1] là việc gán một định danh với chủ thể tương ứng. Một thực thể có thể được xác thực nhờ các thông tin như:

- thông tin mật mà thực thể đó biết (mật khẩu)
- cái mà thực thể đó có (ví dụ như thẻ tín dụng...)
- thông tin về thực thể (như đặc trưng vân tay, nhãn cầu ...)
- vị trí của thực thế (ví dụ như khi dùng GPS để giám sát vị trí của thực thể)

Xác thực thông điệp nhằm đảm bảo được sự toàn vẹn của nội dung thông điệp cũng như nguồn gốc thông điệp. Để xác thực thông điệp có thể thực hiện theo nhiều cách, các cách này có thể chia làm 3 loại chính là: mã hóa thông điệp; mã xác thực thông điệp (MAC); và các hàm băm.

Mã hóa dùng trong xác thực: dùng chính bản mã của thông điệp để xác thực.

Với hệ mã đối xứng, nếu chỉ có hai bên tham gia trao đổi thông điệp biết khóa mật dùng để mã hóa thông điệp thì có thể coi thông điệp được mã được xác thực nguồn gốc và sự toàn vẹn.

Trong hệ mã công khai, tùy theo cách dùng khóa nào để mã mà ta có thông điệp mã hóa thỏa mãn một số tính chất khác nhau. Để đảm bảo tính xác thực cho thông điệp M là do người A tạo ra, A sẽ dùng khóa riêng của mình để mã hóa M. Khi đó bên nhận luôn xác thực được nguồn gốc của M là từ A.

Mã xác thực thông điệp (MAC): là một khối dữ liệu đặc trưng cho thông điệp được mã hóa để làm dấu hiệu xác thực cho thông điệp đó, khối này được gắn kèm với thông điệp khi gửi đi. Tại phía nhận từ thông điệp nhận được, bên nhận sẽ tính lại mã MAC này để kiểm tra tính toàn vẹn, trật tự dữ liệu v.v... của thông điệp.

Các hàm băm: Các hàm băm cũng là một loại dấu hiệu xác thực thông điệp. Nó được tạo ra từ nội dung thông điệp, nó chỉ khác với MAC ở chỗ không cần phải mã hóa

Người ta dùng mã băm của thông điệp để tạo chữ kí số cho thông điệp đó.

Xác thực bằng chữ kí số

Chữ kí số theo chuẩn X.800 về kiến trúc an ninh cho hệ thống mở - là một cơ chế an ninh (security mechanism). Nó là dữ liệu thêm vào – hoặc dạng mã hóa – của một đơn vị dữ liệu nhằm cho phép người nhận đơn vị dữ liệu đó có thể kiểm tra được nguồn gốc đơn vị dữ liệu và tính toàn vẹn của dữ liệu [3].

Chữ kí số là một cơ chế xác thực được dùng phổ biến trong các hệ thống có sử dụng mã hóa công khai. Một ứng dụng chữ kí số gồm hai quá trình:

- Kí lên dữ liệu và
- Kiểm tra chữ kí

Quá trình kí sử dụng thông tin riêng của người kí (bí mật và duy nhất). Quá trình kiểm tra chữ kí dùng các thông tin công khai. Đặc điểm quan trọng của chữ kí là nó chỉ có thể được tạo ra từ thông tin riêng (private) của người kí. Điều này cho phép chống phủ nhận khi kiểm tra.

Chữ kí số được tạo ra từ khóa cá nhân (private key) của người kí. Do đó, dữ liệu đã kí không thể được tại ra bởi ai khác ngoài người có khóa cá nhân người kí. Người nhận cũng không thể tạo ra chữ kí của người gửi. Đây là khả năng chống phủ nhận và xác thực nguồn gốc của chữ kí số.

Trong thực tế các ứng dụng, chữ kí thường được tạo ra từ mã băm của thông điệp, do mã băm này đặc trưng cho thông điệp nên chữ kí số xác thực được sự toàn vẹn của thông điệp, đảm bảo thông điệp không bị sửa đổi.

7.5.3. Xác thực trong hệ PKI

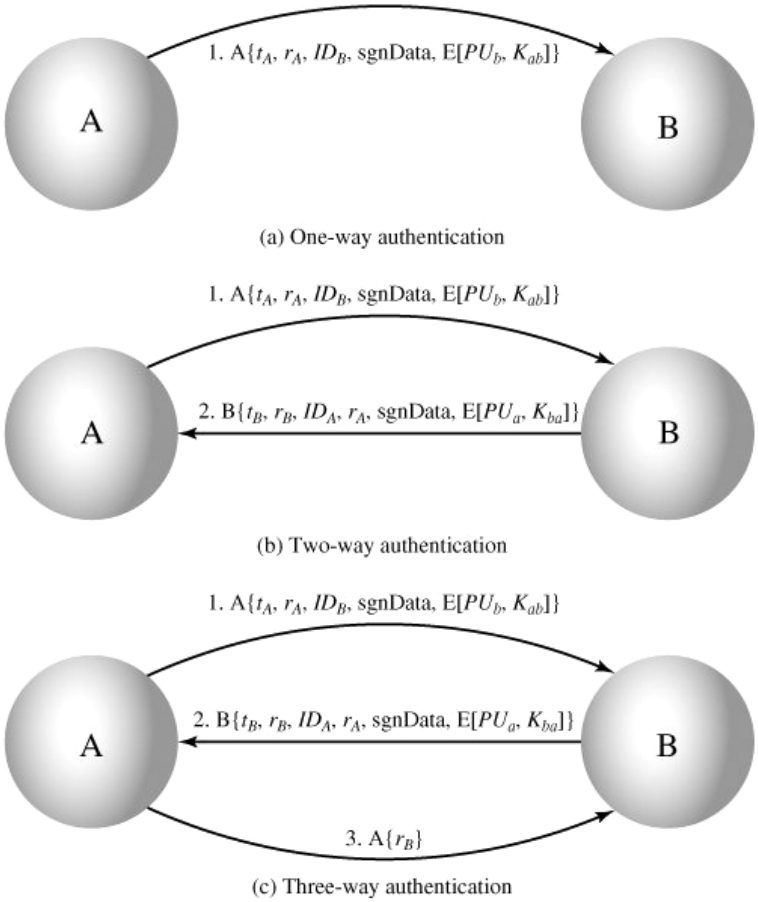
Trong một hệ PKI, các chứng chỉ số được dùng trong các giao dịch nhằm đảm bảo an toàn cho các giao dịch và đảm bảo tính xác thực. Xác thực ở đây bao gồm cả xác thực người dùng lẫn xác thực nội dung thông điệp.

Các phương pháp mã hóa công khai cùng với các hàm băm một chiều sẽ được sử dụng để thực hiện việc xác thực. Trong một hệ PKI bình thường, có thể coi khóa riêng của mỗi người là dấu hiệu đặc trưng của người đó và có thể đem để kí lên các thông điệp trong giao dịch. Trong hệ PKI có ứng dụng sinh trắc học, dấu hiệu đặc trưng của mỗi người sẽ là dấu hiệu sinh trắc học của người đó, khi đó khóa riêng của mỗi người có thể được bảo vệ bởi dấu hiệu sinh trắc học của họ hoặc dấu hiệu sinh trắc học có thể sẽ được sử dụng làm khóa riêng.

Mô hình xác thực trong sơ đồ quản lý chứng chỉ bởi CA

Trong một hệ PKI, CA làm nhiệm vụ quản lý chứng chỉ số. Mỗi chứng chỉ chứa thông tin về chủ sở hữu nó, một khóa công khai của người chủ chứng chỉ và được kí xác nhận bởi khóa riêng của CA. Mỗi người dùng trong hệ PKI đều phải có khóa công khai của CA và CA coi như được tin tưởng tuyệt đối. Chứng chỉ được cấp bởi CA đều có thể được kiểm tra bởi bất kì người dùng nào. Nên chứng chỉ sẽ được dùng để xác thực người dùng. Kết hợp với chữ kí số, chứng chỉ sẽ giúp xác thực cả người dùng lẫn thông điệp.

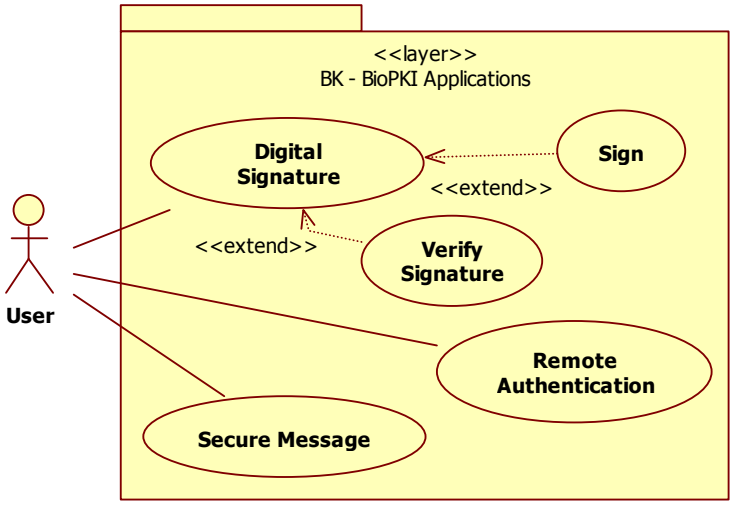
Tùy theo yêu cầu sử dụng, có thể xác thực theo một trong ba cách: xác thực một chiều, xác thực hai chiều hay xác thực ba chiều.



Hình 7.11. Các mô hình xác thực
(a) Xác thực một chiều; (b) xác thực hai chiều; (c) xác thực 3 chiều

7.5.4. Thiết kế ứng dụng trên cơ sở hệ thống BK – BioPKI

Ứng dụng chữ kí số là một thành phần trong nhóm các ứng dụng của hệ thống. Hai chức năng chính hệ thống cung cấp liên quan tới ứng dụng này là chức năng kí và chức năng kiểm tra chữ kí.



Hình 7.12. Biểu đồ usecase nhóm các chức năng liên quan tới ứng dụng trên nền PKI

Trong phạm vi đề tài này, ứng dụng xác thực sẽ được xây dựng nhằm xác thực nội dung thông điệp và xác thực người dùng. Ứng dụng được xây dựng nằm trong hệ thống BK-BioPKI đã được xây dựng từ trước. Mục tiêu của việc xác thực trong ứng dụng này là: Xác thực sự toàn vẹn thông điệp; Xác thực người kí thông điệp; Chống phủ nhận đối với người kí.

- Thuật toán băm sử dụng đảm bảo chỉ cần sai khác một bít ở đầu vào thì chuỗi bit ở đầu ra sẽ thay đổi.
- Bên nhận bên gửi biết mình đang giao dịch với ai, việc xác thực người dùng thông qua chứng chỉ số.
- Thuật toán mã hóa giải mã với cặp khóa riêng – công khai đảm bảo chính xác: mã hóa bằng khóa này chỉ có thể giải mã trở lạibằng khóa kia.
- Khóa riêng đặc trưng cho chủ của nó. Không có khóa riêng trùng nhau.
- Hệ thống BK-BioPKI có 1 CA cấp chứng chỉ cho các người dùng của hệ thống, có các loại chứng chỉ tương ứng với các ứng dụng khác nhau.
- Mô đun ứng dụng này nằm trong hệ BK-BioPKI hiện có nên nó sẽ sử dụng các chức năng đã có liên quan đến chứng chỉ. Sử dụng các hàm các lớp đã được xây dựng để làm việc với chứng chỉ số.
- Hệ thống này chỉ có một CA. coi như mọi client tham gia vào hệ thống đều phải có khóa công khai của CA và đều tin tưởng vào CA không điều kiện.

- Ứng dụng xác thực thông điệp giữa hai client, giả thiết là bên gửi biết địa chỉ bên nhận (địa chỉ IP, số cổng). Quá trình giao dịch sẽ chỉ có hai bên tham gia: bên gửi và bên nhận.

Giải pháp thực hiện xác thực dùng chữ kí số là dùng hàm băm một chiều băm nội dung thông điệp M ra thành chuỗi bit gọi là Message-Digest (MD) MD này sẽ được mã hóa bởi khóa riêng của người kí thành chuỗi bit S. S chính là chữ kí của người kí lên thông điệp M.

Xác nhận chữ kí: thông điệp M' nhận được sẽ được băm thành MD'. Giải mã MD từ chữ kí bằng khóa công khai của người kí (khóa này bên xác nhận biết trước) sau đó so khớp MD với MD' xem có đúng không.

Chữ kí được xác nhận (verify) là đảm bảo cho sự toàn vẹn nội dung của M và khẳng định được người tạo ra chữ kí. Bởi vì chữ kí được xác nhận khi và chỉ khi MD = MD' tức là thỏa mãn đồng thời các điều kiện sau:
M' = M (nếu không thì chắc chắn MD khác MD')
Khóa công khai của người kí tương ứng với khóa riêng đã kí.

- **Thiết kế kịch bản ứng dụng**

Từ các tiền đề trên, kịch bản ứng dụng có thể được mô tả như sau:

Hai người dùng của hệ thống tham gia vào một giao dịch thông điệp có sử dụng chữ kí số. Tạm gọi hai người đó là A và B. A gửi cho B thông điệp M (là một file dữ liệu), A đồng thời dùng một chứng chỉ số của mình để tạo chữ kí số. Chính xác là A dùng khóa riêng Pr_A (ứng với chứng chỉ $Cert_A$ của A đã được CA xác nhận) để kí lên M tạo thành chữ kí S_A. Cả M, số Serial của $Cert_A$ và S_A được gắn lại và gửi cho B.

Khi B nhận được file đã được kí và B muốn kiểm tra chữ kí có đúng không thì trước tiên, hệ thống sẽ tách nội dung file và các thông tin liên quan tới chữ kí ra.

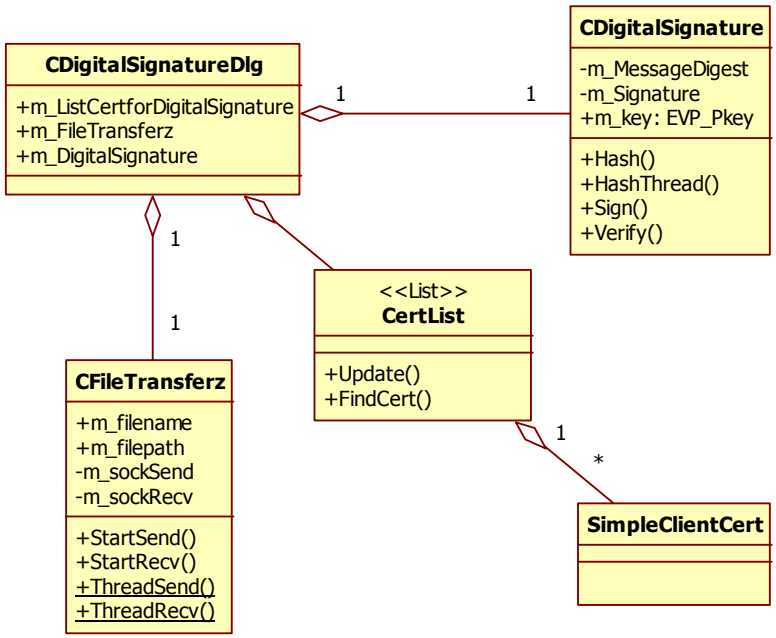
Tiếp theo B sẽ dùng dịch vụ do hệ thống cung cấp để lấy chứng chỉ $Cert_A$ và kiểm tra xem có đúng là chứng chỉ hợp lệ hay không. Sau đó nếu chứng chỉ hợp lệ thì B lấy khóa công khai Pb_A của A từ chứng chỉ. B dùng Pb_A để kiểm tra lại chữ kí và file M để xác thực xem có phải đúng là A đã kí chữ kí này không.

Nếu chứng chỉ không hợp lệ hoặc nếu M không toàn vẹn hoặc không phải A kí chứng chỉ thì kết quả việc kiểm tra sẽ biết được ngay. Trái lại chữ kí là hợp lệ và file M không bị thay đổi trên đường truyền.

Điểm đáng lưu ý ở đây là việc thử nghiệm tích hợp sinh trắc học vân tay vào ứng dụng. Đặc trưng vân tay được dùng để mã hóa khóa cá nhân. Mỗi khi cần lầy khóa cá nhân ra kí thì người dùng phải quét vân tay để hệ thống lấy đặc trưng vân tay ra đối chiếu và giải mã khóa cá nhân.

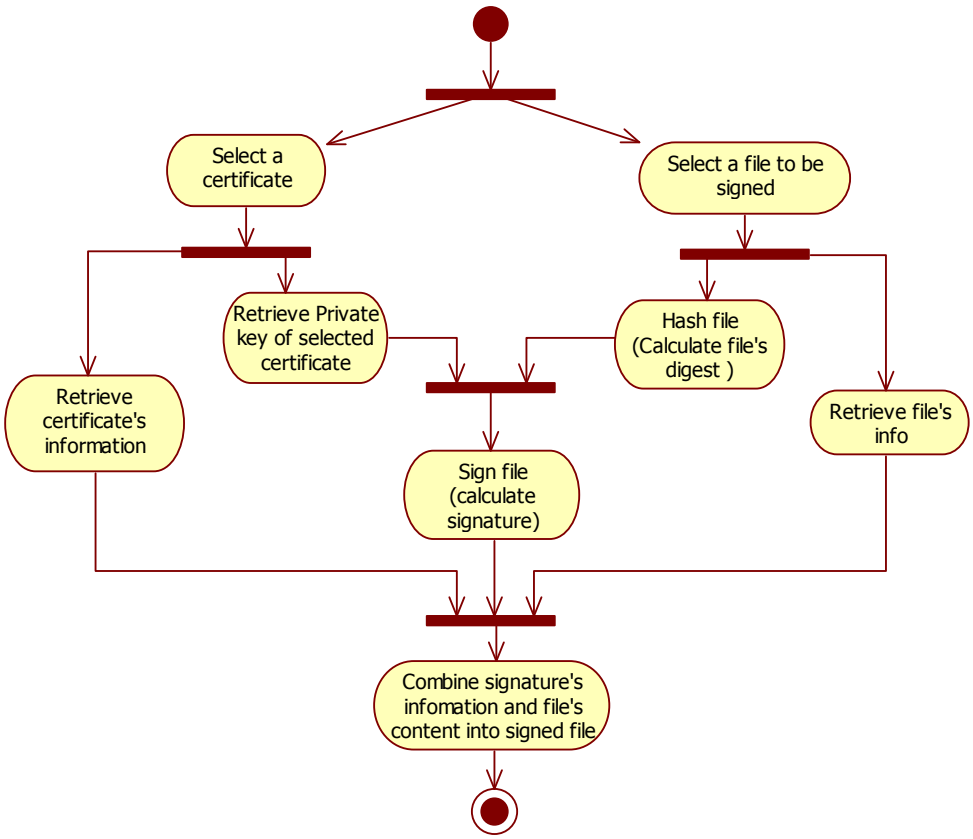
7.5.5. Thiết kế triển khai ứng dụng

Từ kịch bản trên, ứng dụng được thiết kế bao gồm hai phân hệ chính là phân hệ gửi file giữa các máy client và phân hệ chữ kí số.



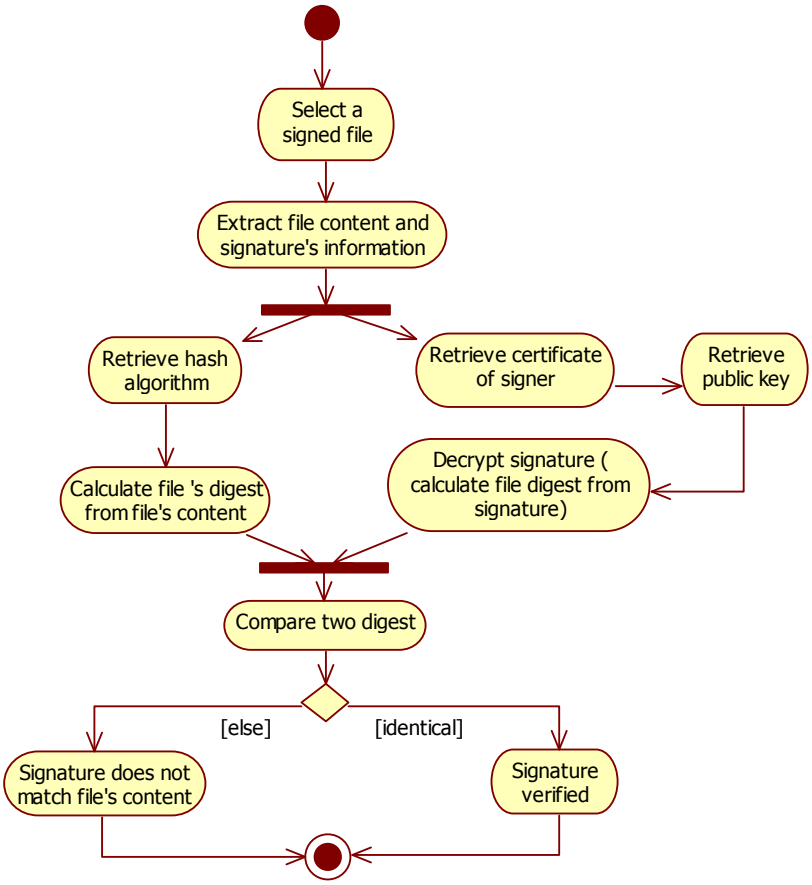
Hình 7.13. Biểu đồ lớp của ứng dụng chữ kí số

Hai hoạt động chính của ứng dụng là kí và kiểm tra, được thiết kế hoạt động như sau:



Hình 7.14. Biểu đồ hoạt động tạo chữ kí số

Quá trình kiểm tra như sau:

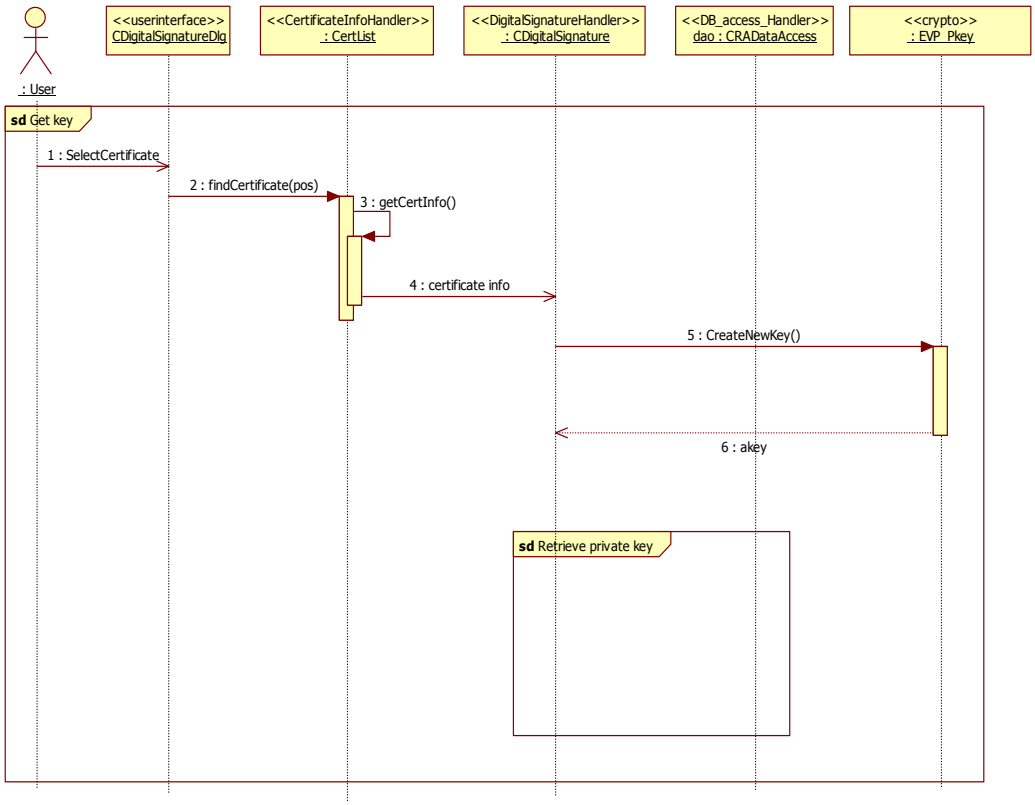


Hình 7.15. Biểu đồ hoạt động kiểm tra chữ kí số

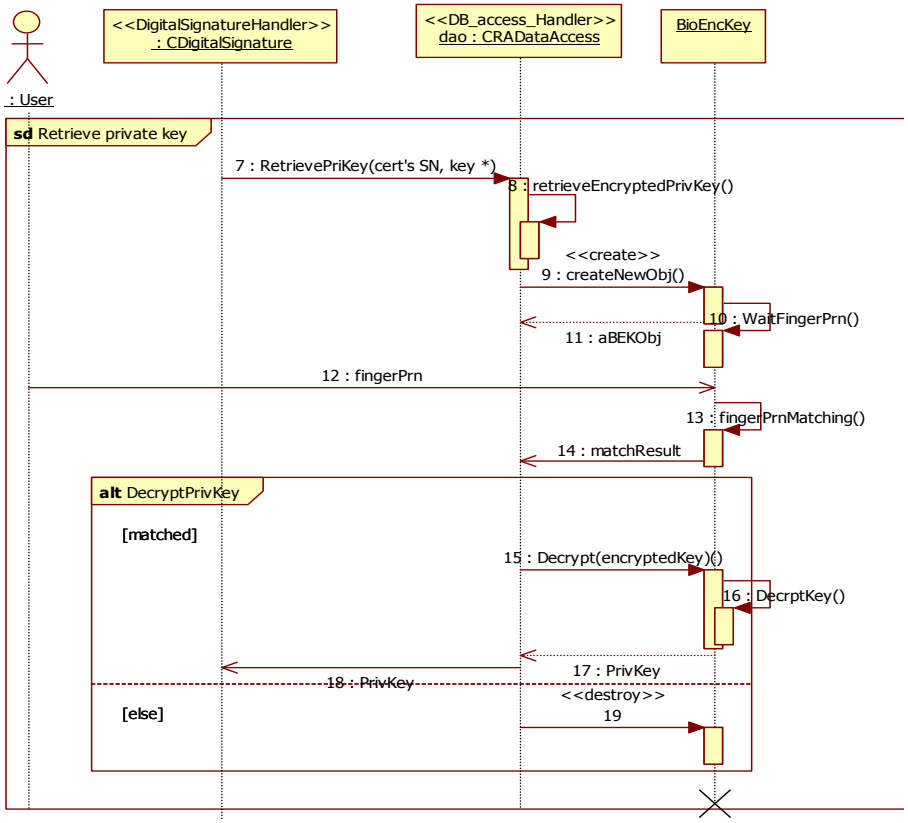
Biểu đồ diễn tiến của ứng dụng được thể hiện tại hình 7.16.

Trong pha lấy khóa, có sử dụng đến đặc trưng vân tay, người chủ của khóa sẽ phải dùng vân tay của mình để giải mã lấy ra khóa cá nhân.

Ảnh vân tay sau khi được xử lý sẽ được trích chọn ra các đặc trưng để đối sánh với vân tay lúc đăng kí người dùng. Nếu quá trình đối sánh thấy khớp thì khóa cá nhân sẽ được giải mã và được lấy ra để sử dụng, trái lại không thể truy xuất được khóa cá nhân.

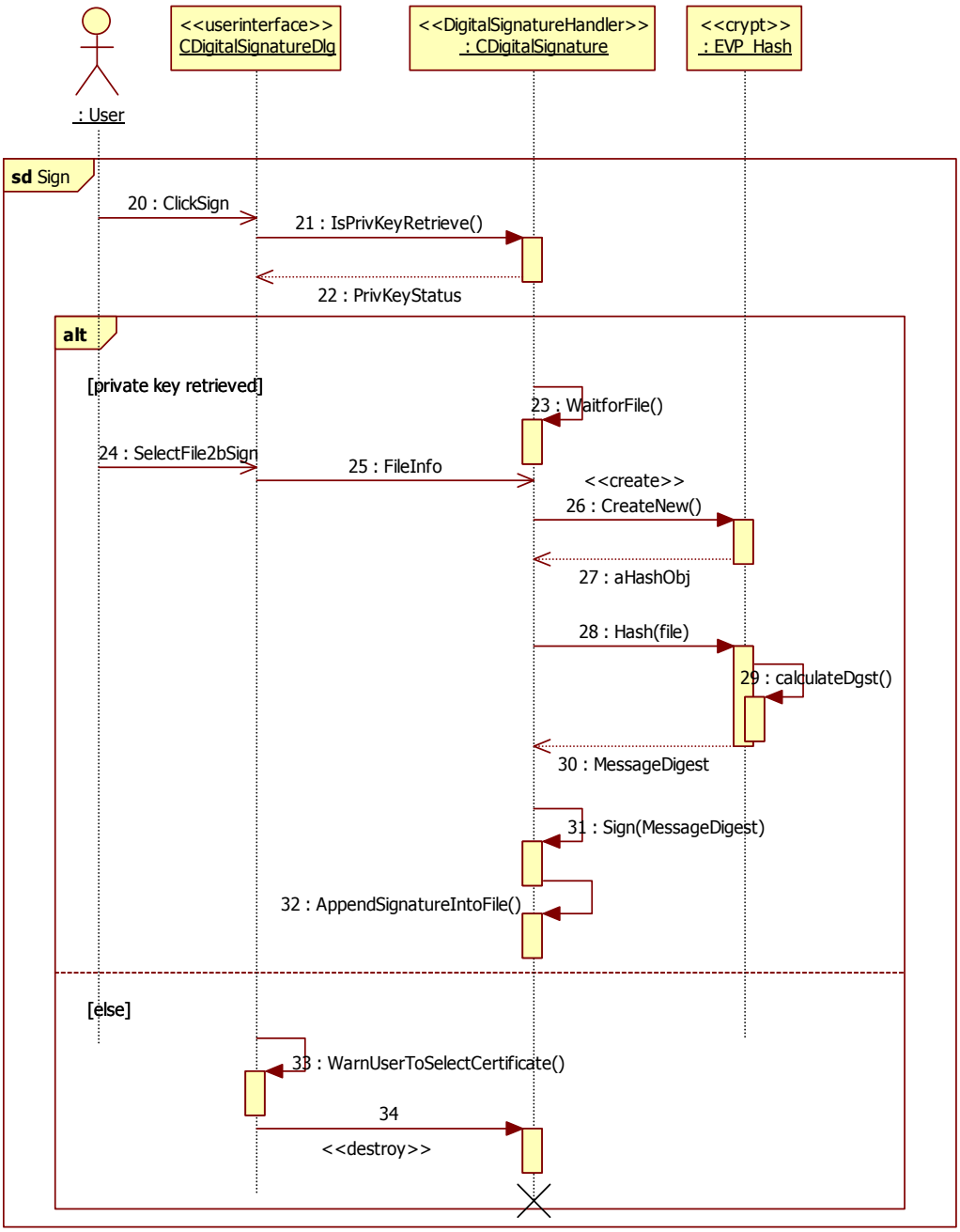


Hình 7.16. Biểu đồ diễn tiến quá trình lấy khóa để kí



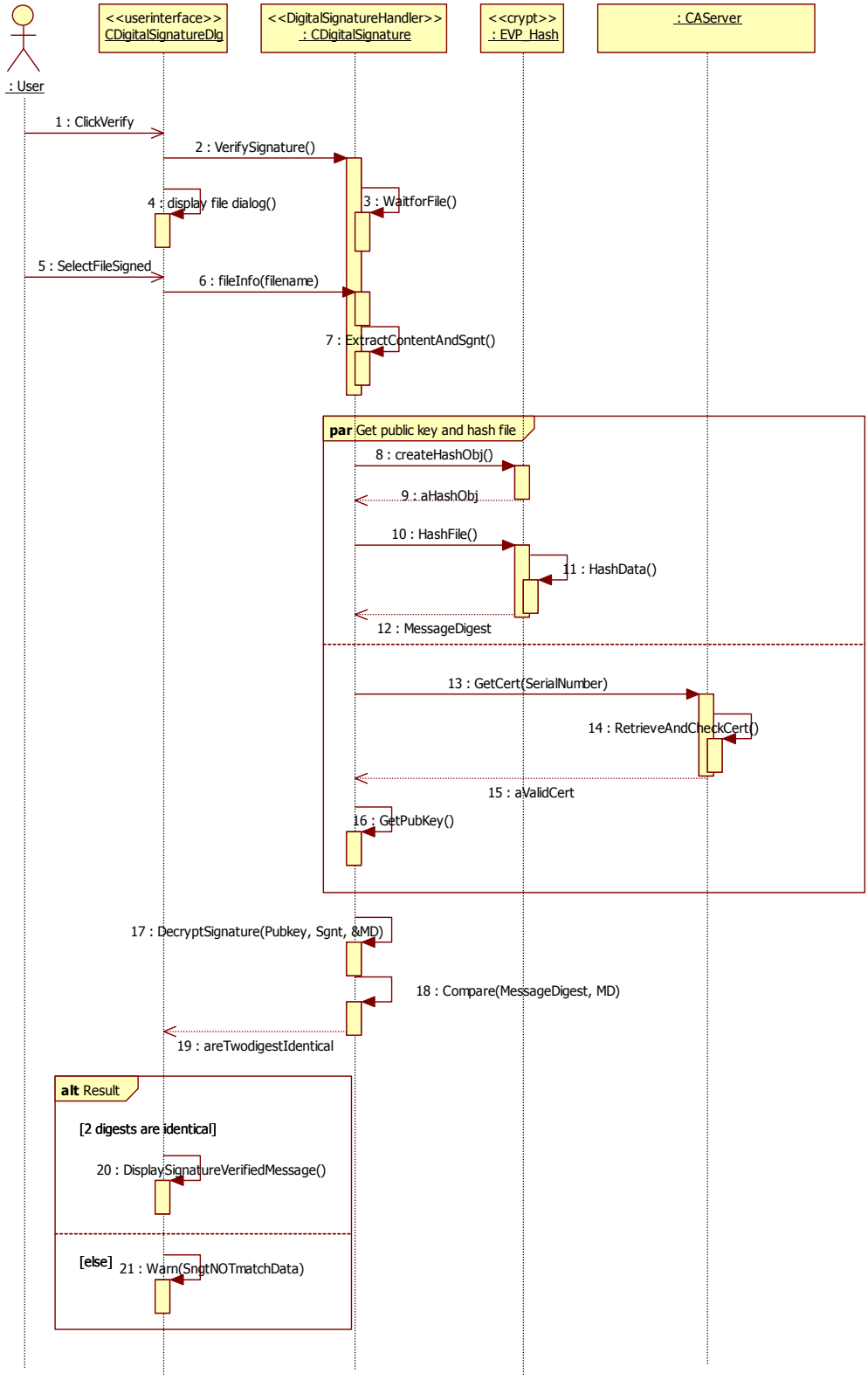
Hình 7.17. Biểu đồ hoạt động truy xuất khóa cá nhân trong ứng dụng chữ kí số

Sau khi lấy được khóa, pha kí diễn ra như đã mô tả trong các mục trên và được thể hiện cụ thể qua biểu đồ diễn tiến sau đây.



Hình 7.18. Biểu đồ diễn tiến công đoạn kí

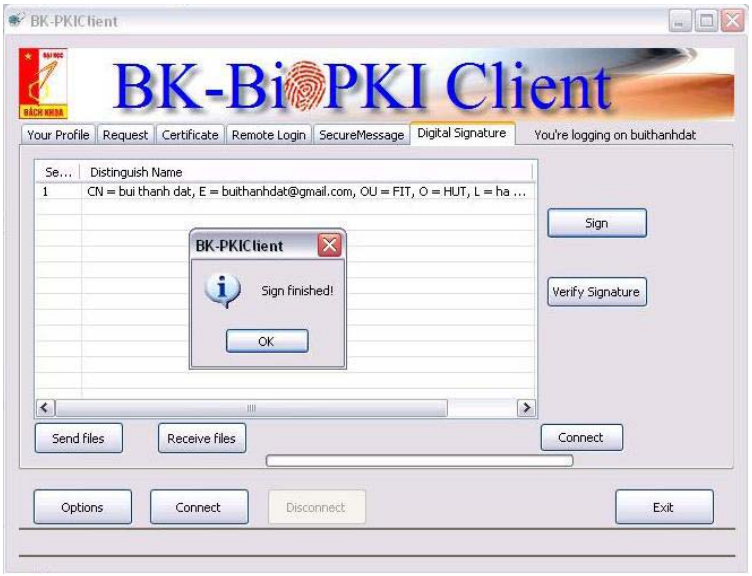
Công đoạn kiểm tra chữ kí không có yếu tố sinh trắc học, biểu đồ cụ thể như sau:



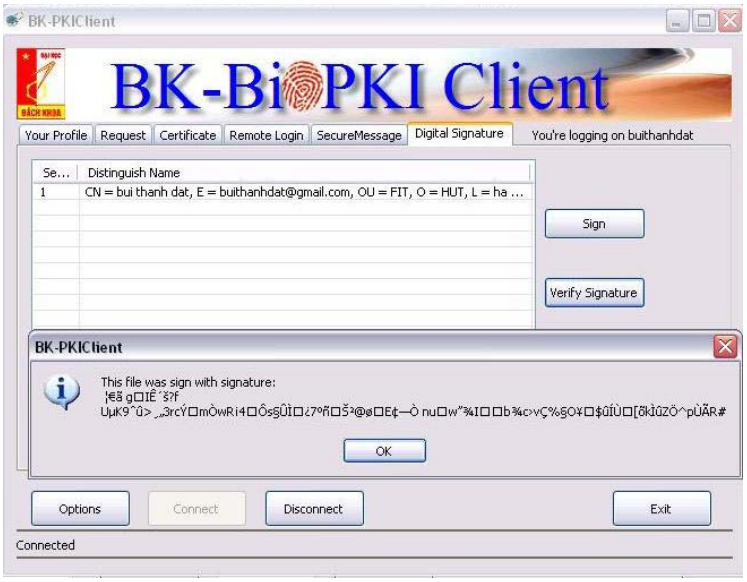
Hình 7.19. Biểu đồ kiểm tra chữ kí số

7.5.6. Thử nghiệm ứng dụng và kết quả

Ứng dụng đã được chạy thử thành công. Ứng dụng đã được xây dựng trên nền tảng hệ thống BK – BioPKI. Trong ứng dụng này, người kí sẽ phải dùng vân tay để truy xuất khóa cá nhân của mình ở pha tạo chữ kí. Người kiểm tra chữ kí lấy chứng chỉ số của người kí thông qua CA để thẩm định chữ kí.



Hình 7.20. Giao diện Kết thúc quá trình ký



Hình 7.21. Chữ kí được lấy ra khi kiểm tra

Nhận xét kết quả:

- Ứng dụng chạy đúng như kịch bản thiết kế ban đầu.
- Có thể phát triển tiếp ứng dụng, bổ sung thêm tùy chọn cho người dùng và cải thiện hiệu năng một số phân hệ trong ứng dụng.

Chương 8.
THIẾT KẾ VÀ XÂY DỰNG CÁC PHẦN MỀM ỨNG DỤNG AN TOÀN THÔNG TIN TRONG HỆ BIOPKI

8.1. Tổng quan các ứng dụng an toàn thông tin

Các ứng dụng trao đổi thông tin an toàn cần đảm bảo 3 yêu cầu: nguồn, thông tin truyền, đích. Khi truyền thông tin đi, nguồn cần đảm bảo rằng chỉ có những trạm đích được cho phép mới có thể truy cập thông tin đã truyền, tất cả các trạm khác đều không thể. Ngược lại khi nhận thông tin, đích cũng cần đảm bảo rằng thông tin này được tạo ra bởi đúng nguồn tin đã định trước. Tất nhiên trong cả hai trường hợp, thông tin nhận được cũng cần được đảm bảo là giống hệt như thông tin đã được truyền đi, không bị thay đổi ở giữa đường truyền.

Xuất phát từ các yêu cầu trên, các ứng dụng an toàn thông tin dựa trên có thể chia làm 3 loại: Ứng dụng mã hóa thông tin đảm bảo thông tin được truyền đến đích, ứng dụng ký thông tin đảm bảo xác thực nguồn tin và ứng dụng kết hợp 2 chức năng trên để tạo một kênh truyền bảo mật.

Trên cơ sở yêu cầu của đề tài, cần xây dựng các ứng dụng thử nghiệm thuộc các dạng trên nhằm mục đích:

- Làm chủ được các ứng dụng của hạ tầng PKI
- Phát triển thành các framework để ứng dụng hạ tầng PKI vào các nội dung cụ thể.

Ngoài ra, khi triển khai ứng dụng BioPKI vào các ứng dụng đã có sẵn để tăng cường tính bảo mật cho các ứng dụng đó, nảy sinh vấn đề tích hợp hệ thống PKI với các hệ thống đã có sẵn này. Để thử nghiệm giải pháp tích hợp, đề tài triển khai một ứng dụng cho phép sử dụng BioPKI để tăng cường bảo mật cho quá trình truy cập từ xa của một dịch vụ tùy ý (đã cài đặt dịch vụ chat, có thể là dịch vụ DB, ...)

Một xu hướng mới xuất hiện trong các hệ thống giao dịch điện tử là đa dạng hóa các phương thức truy cập thông tin. NSD có thể sử dụng các cách thức, các hạ tầng truyền thông khác nhau để có thể truy cập vào các CSDL cũng như các dịch vụ thông tin. Với các đặc điểm, thông số khác nhau của các hạ tầng truyền thông đó, PKI nói chung và BioPKI nói riêng gặp một số khó khăn về tốc độ đường truyền, về khả năng xử lý thiết bị đầu cuối, về kích thước thông điệp, về thời gian đáp ứng, ...

Vì vậy, đề tài đã triển khai thử nghiệm ứng dụng PKI trên nền SMS, cung cấp cơ chế trao đổi thông tin bảo mật an toàn bằng PKI trên nền truyền thông SMS. Ứng dụng này có thể mở rộng cho những hạ tầng truyền thông khác như MMS, CDMA, ...

Trong chương này, đầu tiên ứng dụng ký và mã hóa thông điệp sử dụng các dấu hiệu sinh trắc được trình bày. Tiếp theo là ứng dụng tăng cường bảo mật cho quá trình truy cập từ xa. Cuối cùng là ứng dụng PKISMS truyền thông bảo mật trên nền SMS.

8.2. Ứng dụng ký và mã hóa thông điệp

8.2.1. Phân tích yêu cầu truyền thông tin bảo mật

Ngày nay, thương mại điện tử đóng vai trò rất quan trọng trong các hoạt động kinh tế, xã hội. Có rất nhiều ứng dụng được xây dựng trong lĩnh vực thương mại điện tử với nhiều mục đích khác nhau, như phục vụ cho các ngân hàng, chứng khoán, chính phủ điện tử… Hệ thống PKI được sử dụng để đảm bảo tính bảo mật cho các dịch vụ này. Dựa trên hệ thống PKI, chúng ta có thể phát triển rất nhiều ứng dụng sử dụng mật mã khóa công khai và khóa đối xứng. Một trong những ứng dụng đó là ứng dụng chữ ký số và mã hóa thông điệp.

Phần này sẽ trình bày về việc thiết kế và cài đặt ứng dụng ký và mã hóa. Trong thực tế, để gửi một bức thư an toàn đến người nhận mà đảm bảo tính bí mật và tính không thể từ chối, bức thư đó phải được ký và cho vào phong bì đảm bảo. Điều này cũng được áp dụng trong truyền thông sử dụng khóa công khai để đảm bảo tính xác thực.Trước khi gửi một thông điệp, người gửi phải thực hiện những việc sau:

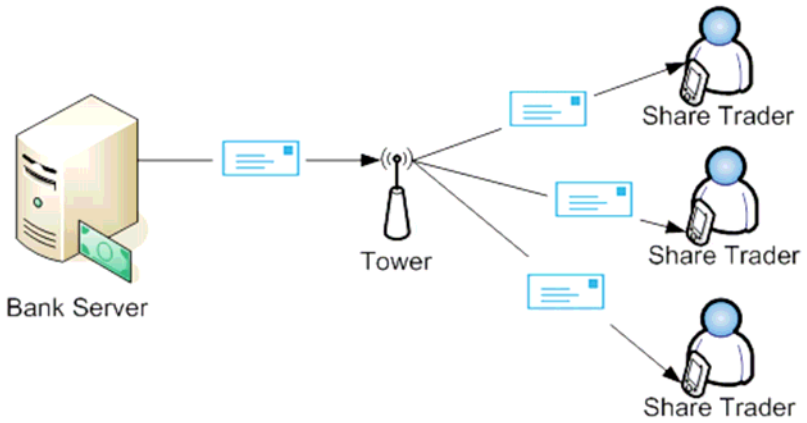
- Ký lên thông điệp đó
- Mã hóa thông điệp đã được ký bằng cách sử dụng một khóa được sinh ngẫu nhiên
- Mã hóa khóa vừa sinh ra bằng khóa công khai của người nhận
- Gửi thông điệp đã được mã hóa đến cho người nhận

Đây chính là cách tiếp cận ký rồi mã hóa thông điệp. Các tính chất được có thể đảm bảo khi sử dụng phương pháp này

- Tính an toàn: Việc ký và mã hóa tạo ra một mức an toàn cao hơn là không kết hợp (kết hợp hai hàm tính toán làm tăng tính phức tạp từ đó làm tăng tính an toàn). Nó đảm bảo tính bí mật và không thể từ chối
- Tính hiệu quả
- Tính bí mật

Nhược điểm của phương pháp:

Trong phương pháp ký và mã hóa này, bên gửi phải sử dụng khóa công khai của bên nhận để mã hóa thông điệp. Điều này sẽ trở nên bất tiện nếu muốn gửi thông điệp đó đến nhiều người cùng một lúc. Ví dụ như một ngân hàng muốn gửi một thông báo đến một vài khách hàng của họ, thì họ phải sử dụng khóa công khai của từng người để mã hóa. Cách tiếp cận này sẽ làm giảm hiệu quả. Để giải quyết vấn đề này, có thể tạo ra một nhóm khóa giữa ngân hàng và khách hàng để sử dụng trong việc phân phối thông điệp cho nhiều người



Hình 8.1. Nhược điểm của ký và mã hóa

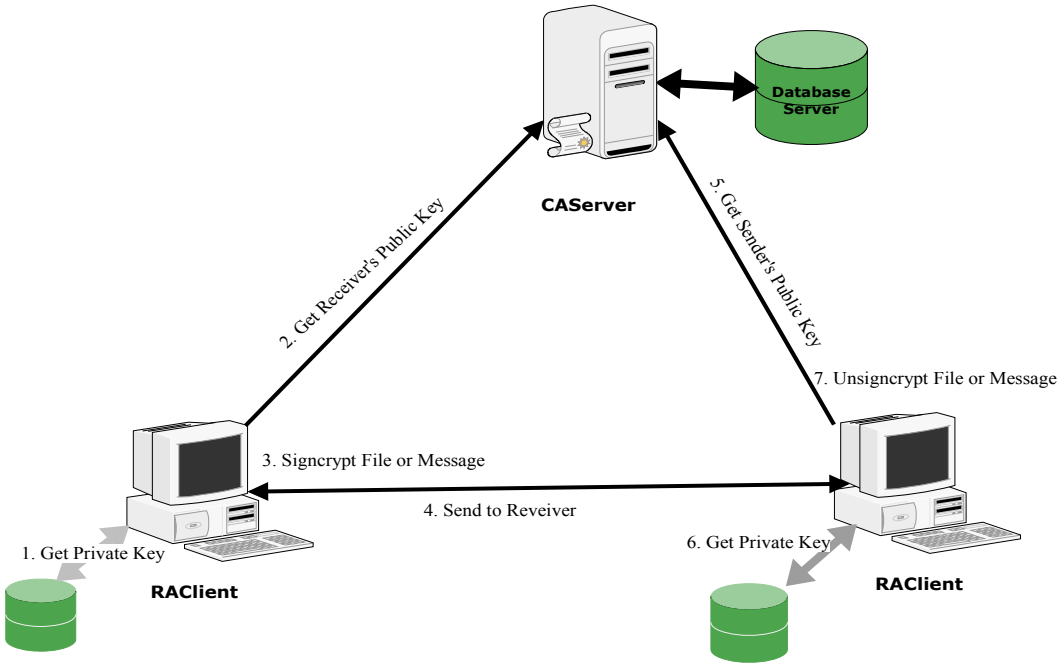
8.2.2. Xây dựng ứng dụng ký và mã hóa thông điệp sử dụng dấu hiệu sinh trắc

8.2.2.1. Mô tả các yêu cầu về chức năng của hệ thống

Chương trình được xây dựng dựa trên hạ tầng khóa công khai đã có, gồm các chức năng cơ bản của một hệ PKI như các chức năng liên quan đến chứng nhận người dùng, yêu cầu chứng chỉ, cấp phát và quản lý chứng chỉ số và các chức năng liên quan đến kết nối giữa RA và CA.

Để có thể mã hóa thông điệp một cách an toàn, tạo và xác thực chữ ký số cho một thông điệp hoặc file thì người sử dụng cần phải được cấp phát một chứng chỉ số tương ứng với từng chức năng sử dụng.

Dưới đây là sơ đồ mô tả hoạt động ký và mã hóa trong hệ thống BK-BioPKi đã được xây dựng:



Hình 8.2. Sơ đồ hoạt động ký và mã hóa trong hệ BioPKI

8.2.2.2. Quá trình mã hóa và giải mã thông điệp

Mã hóa là quá trình chuyển đổi một thông điệp ban đầu thành một thông điệp bí mật mà chỉ có bên gửi và bên nhận mới có thể nhận biết được. Chẳng hạn như Alice muốn gửi thông điệp riêng cho Bob thì Alice phải biết khóa công khai của Bob. Khóa công khai này được thông báo rộng rãi cho mọi người cùng biết, và Bob có thể gửi khóa đó qua mạng mà không phải lo lắng. Sau đó Alice sẽ sử dụng khóa công khai đó để mã hóa thông điệp và gửi cho Bob. Bob nhận được thông điệp của Alice và sử dụng khóa riêng của mình (tương ứng với khóa công khai đó) để giải mã.

8.2.2.3. Chữ ký số và xác thực

Chữ ký số là cơ chế cho phép xác thực một thông điệp, hay nói cách khác nó cho phép chứng minh được thông điệp đó là của chính người gửi tạo nên. Chẳng hạn như Alice muốn tạo chữ ký lên thông điệp mà mình muốn gửi cho Bob thì cô ấy phải sử dụng khóa riêng của mình để mã hóa thông điệp và gửi kèm theo khóa công khai cho Bob. Bob sử dụng khóa công khai của Alice để giải mã, quá trình này chính là để xác thực chữ ký số, có nghĩa là chắc chắn thông điệp đó đã được ký bởi Alice

Trên đây là những nguyên lý minh họa cho quá trình mã hóa/ giải mã và ký/ xác thực chữ ký số. Ta có thể kết hợp việc mã hóa và chữ ký số để đảm bảo tính bí mật và tính xác thực

Việc sử dụng mã hóa đối xứng đóng vai trò rất quan trọng trong hệ thống khóa công khai vì những giải thuật mã hóa bất đối xứng thường chậm hơn rất nhiều so với các giải thuật mã hóa đối xứng. Do vậy cần phải kết hợp sử dụng mã hóa đối xứng và bất đối xứng trong từng trường hợp

Để tạo chữ ký số, cần sử dụng một kỹ thuật đó là sử dụng hàm băm. Kỹ thuật này cho phép tạo ra một thông điệp ngắn gọn từ thông điệp đầy đủ ban đầu. Các giải thuật băm là những giải thuật mã hóa một chiều, rất khó để thu được thông điệp gốc từ thông điệp đã được băm.

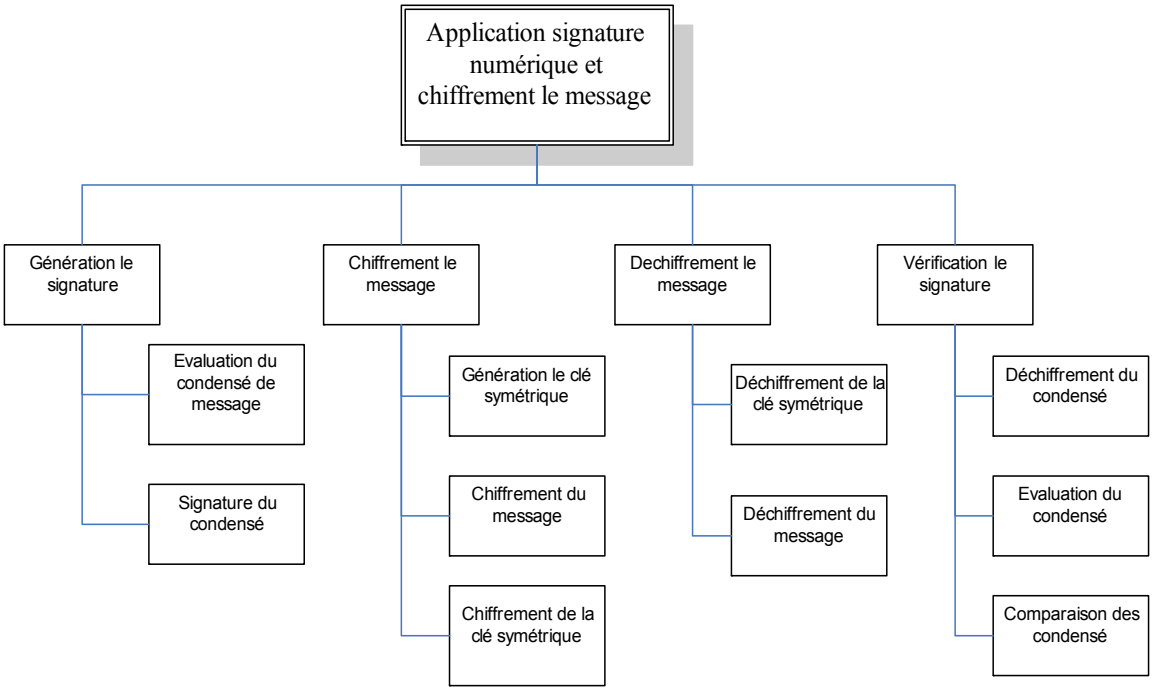
Lý do chính cần phải tạo ra những thông điệp ngắn gọn:

+ Việc gửi kèm nó với thông điệp gốc sẽ giúp cho ta có thể xác định được những lỗi trong thông điệp

+ Nó được ứng dụng để tạo chữ ký số là để thu gọn kích thước chữ ký số cho nhỏ hơn so với thông điệp ban đầu

+ Những giải thuật băm nhanh hơn bất kỳ giải thuật mã hóa nào (kể cả khóa công khai và khóa đối xứng)

8.2.3. Thiết kế chi tiết các chức năng của hệ thống

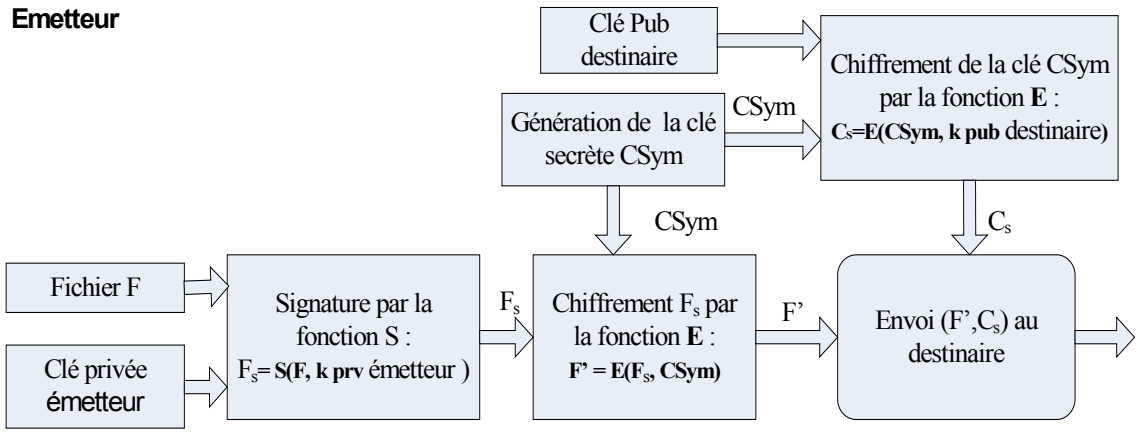


Hình 8.3. Biểu đồ phân cấp chức năng của ứng dụng

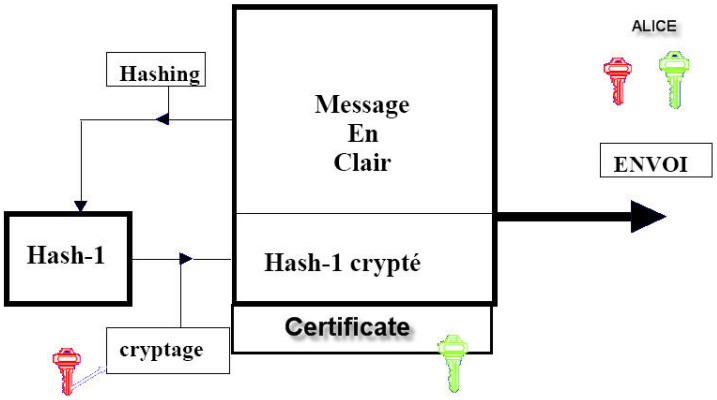
*** Chức năng mã hóa và tạo chữ ký số**

Hình sau mô tả quá trình Alice phải thực hiện để gửi một thông điệp đã được ký và mã hóa cho Bob

***Tạo chữ ký số cho thông điệp, bao gồm 2 bước**:*



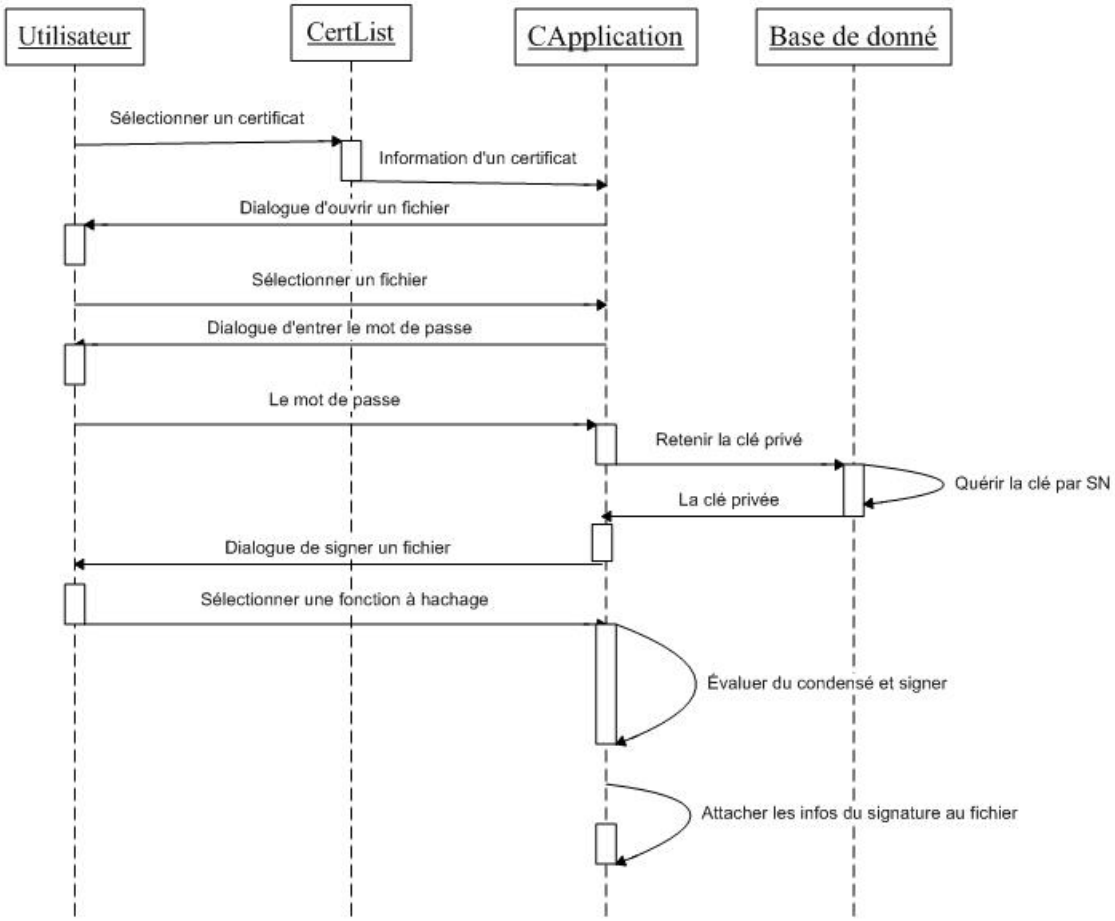
Hình 8.4. Quá trình ký và mã hóa thông điệp gửi đi



Hình 8.5. Quá trình băm chứng chỉ

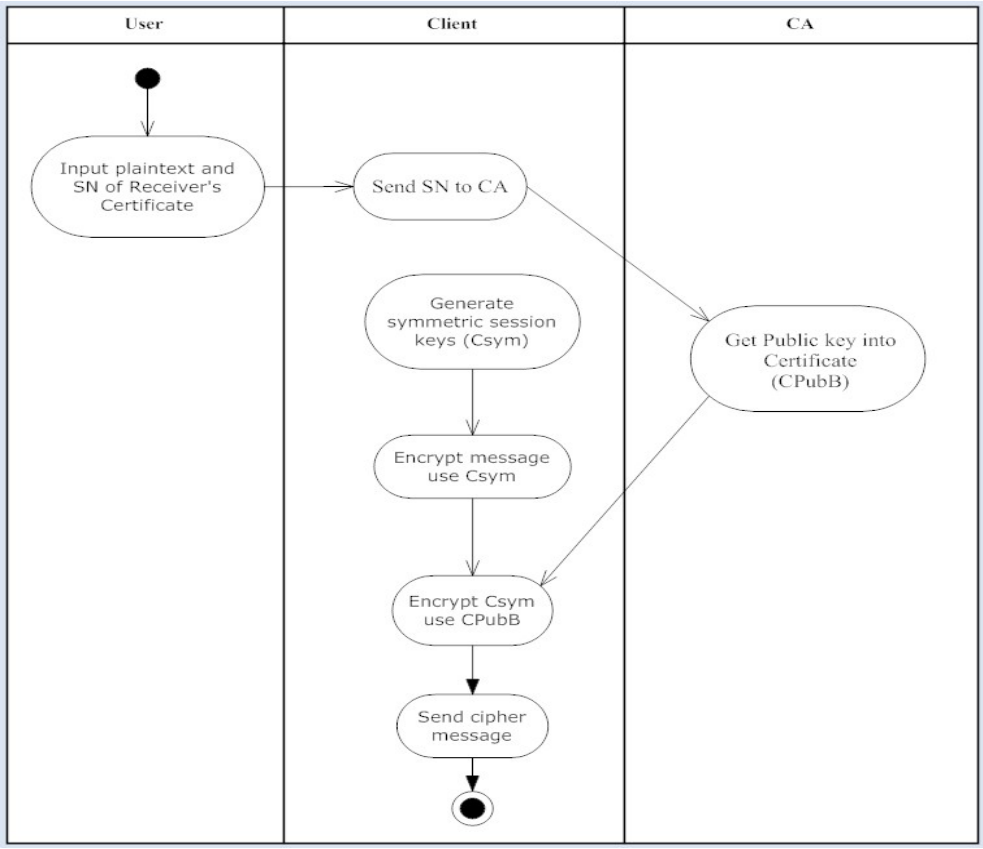
+ Xác định thông điệp băm từ thông điệp gốc: mục đích của việc này là để đảm bảo việc nhận biết thông điệp đó có còn toàn vẹn không.

+ Ký lên thông điệp băm: chữ ký được tạo ra nhờ việc mã hóa thông điệp băm bằng khóa riêng của người gửi. Người ta có thể thấy trong chữ ký số tên của giải thuật băm mà người gửi đã sử dụng. Khóa công khai của người gửi cũng được đính kèm theo chữ ký số. Nhờ có những thông tin này mà bất kỳ ai cũng có thể giải mã và xác thực chữ ký số của người gửi.



Hình 8.6. Giao dịch Quá trình ký và mã hóa

Mã hóa thông điệp: Quá trình mã hóa bao gồm 3 bước:

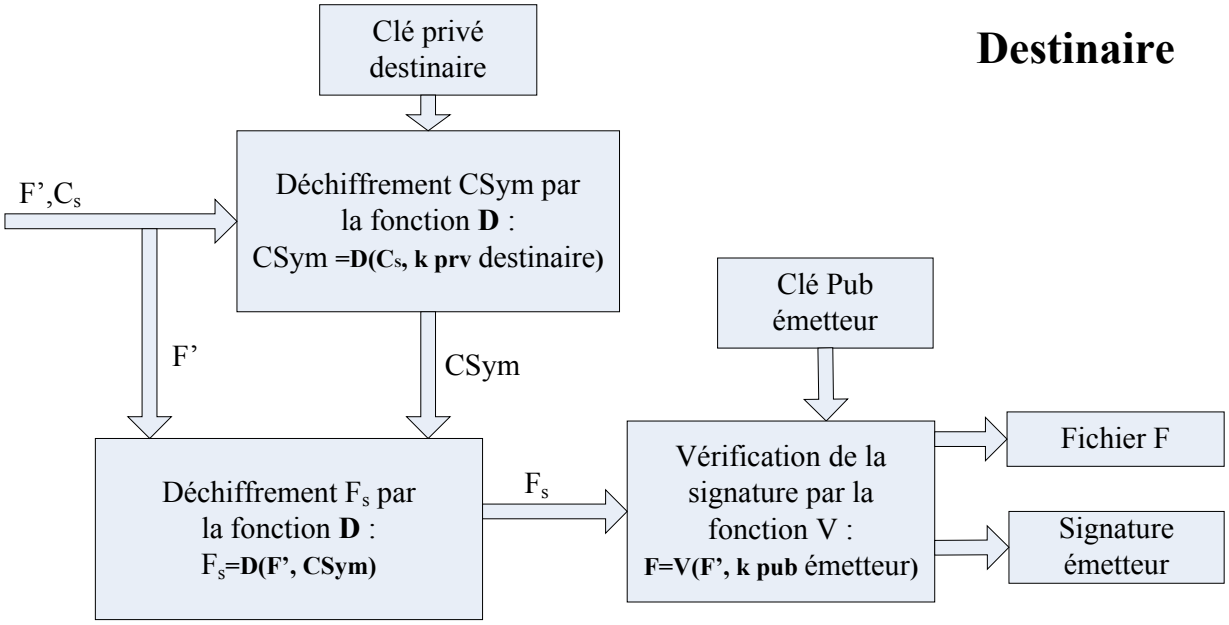


Hình 8.7. Quá trình mã hóa thông điệp

a. Tạo một khóa duy nhất (Csym) để mã hóa và giải mã để sử dụng cho giải thuật mã hóa đối xứng
b. Mã hóa thông điệp: Tất cả các thông điệp (kể cả thông điệp ban đầu và chữ ký số) được mã hóa bằng Csym đã được tạo ở trên
c. Mã hóa khóa đối xứng: Csym sẽ được bên nhận sử dụng để giải mã thông điệp nhận được, do vậy cần thiết phải mã hóa Csym bằng khóa công khai của người nhận. Vì Csym có kích thước khá nhỏ so với thông điệp cần gửi nên việc sử dụng khóa công khai để mã hóa Csym là khả thi, hiệu quả sử dụng của các giải thuật mã hóa bất đối xứng là có thể chấp nhận được

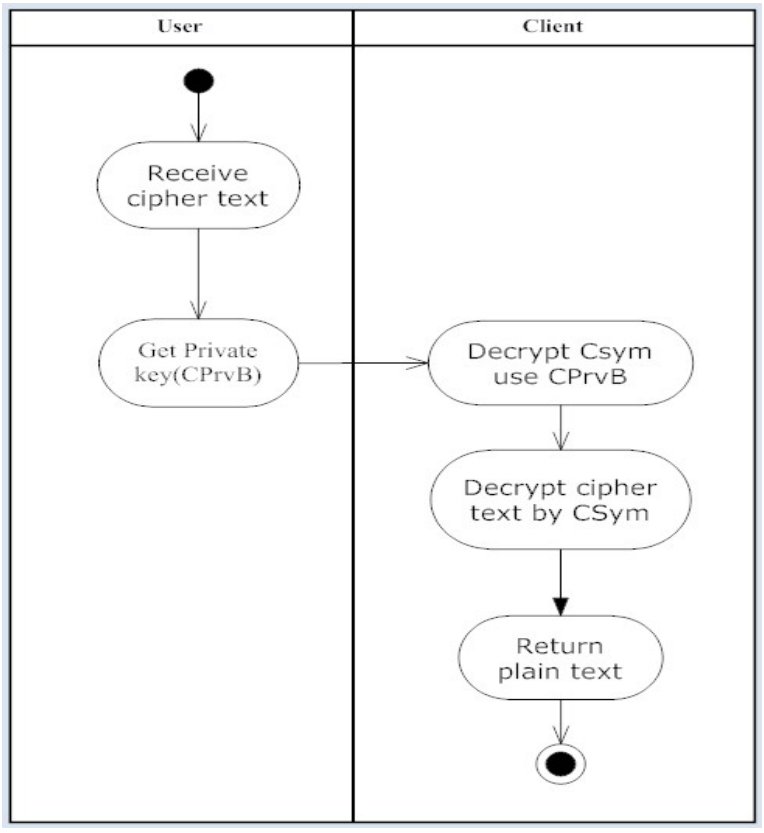
*** Chức năng giải mã và xác thực chữ ký số của một thông điệp**

Hình sau mô tả một dãy các thao tác mà Bob cần thực hiện để giải mã và xác thực thông điệp được gửi từ Alice.



Hình 8.8. Quá trình giải mã và xác thực thông điệp

Quá trình giải mã thông điệp bao gồm các bước sau:

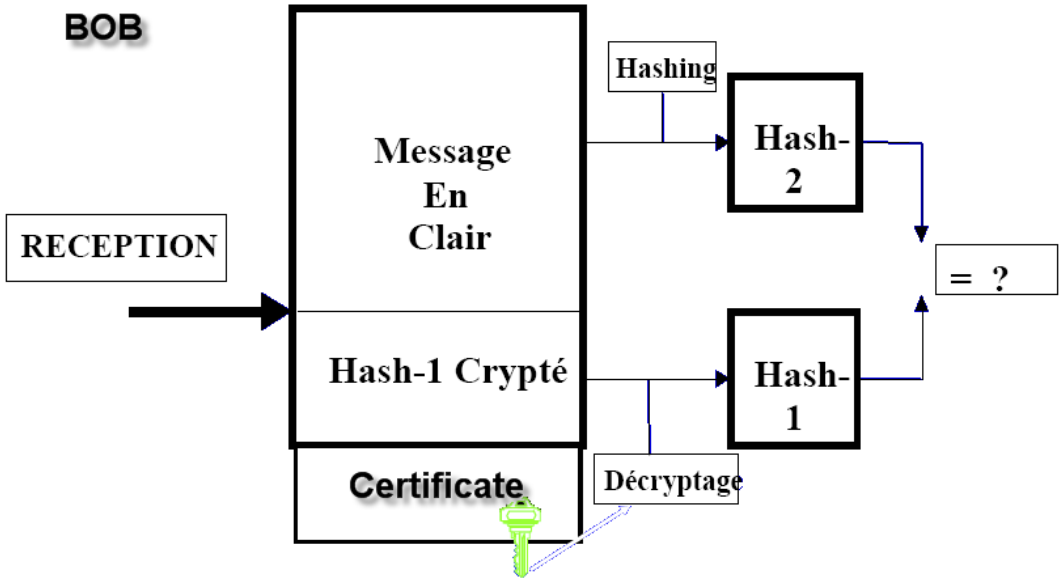


Hình 8.9. Quá trình giải mã thông điệp

+ Giải mã khóa đối xứng: đây là khóa duy nhất được sử dụng để mã hóa thông điệp. Khóa này được mã hóa bằng khóa công khai của người nhận (Bob). Do vậy chỉ có Bob là có thể giải mã Csym và sử dụng nó để giải mã thông điệp

+ Giải mã thông điệp: Thông điệp nhận được (bao gồm cả thông điệp ban đầu và chữ ký số) được giải mã nhờ Csym

Quá trình xác thực chữ ký: Việc xác thực chữ ký bao gồm 3 bước sau:

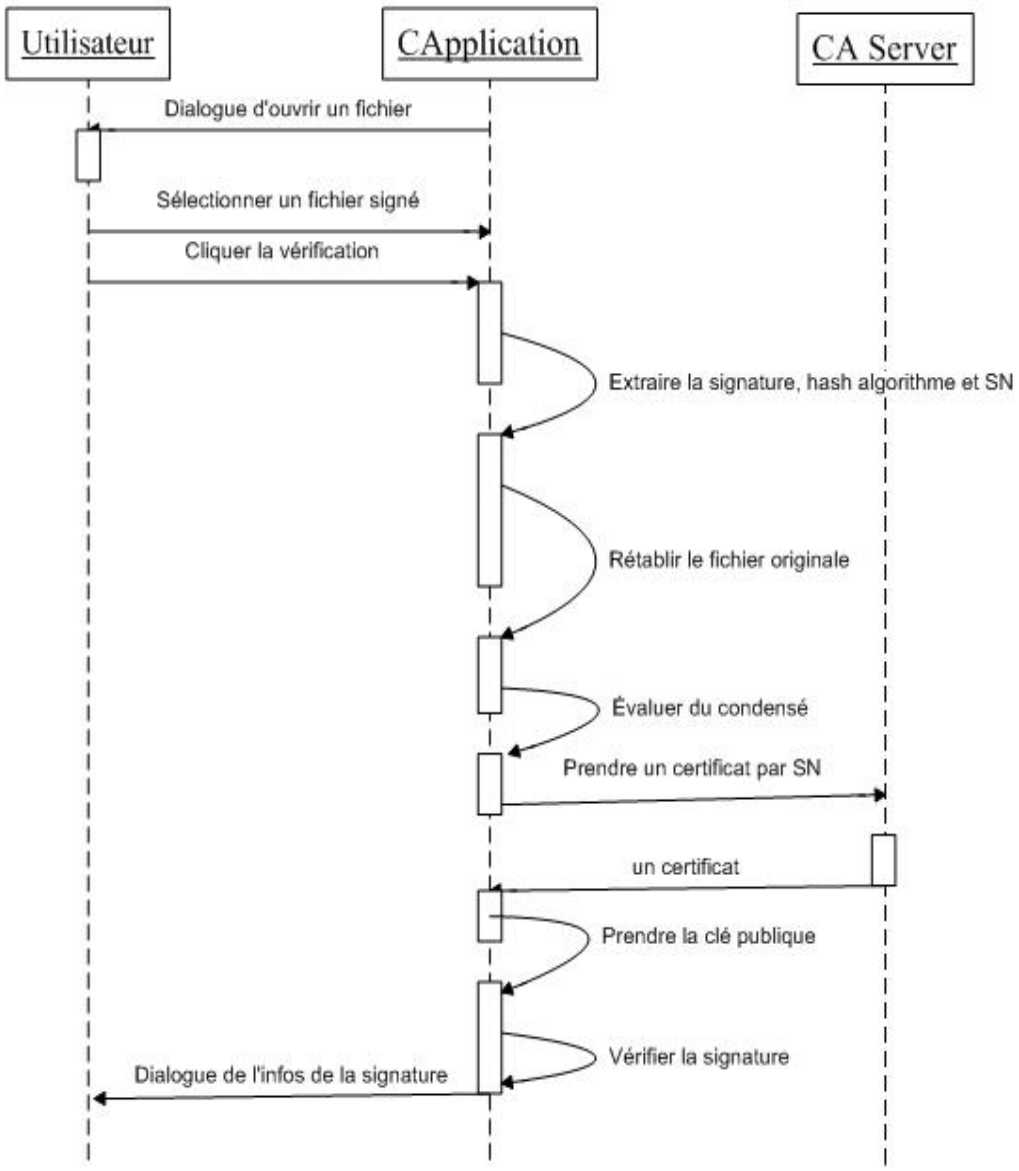


Hình 8.10. Quá trình xác thực chữ ký

a. Giải mã thông điệp băm: thông điệp băm đã được mã hóa nhờ vào khóa riêng của người gửi. Bây giờ nó sẽ được giải mã bằng khóa công khai của người gửi nằm trong thông điệp đó

b. Xác định thông điệp băm từ thông điệp nhận được: như trên đã nói băm là quá trình một chiều, do vậy không thể lấy lại thông điệp gốc từ thông điệp băm, do vậy bên nhận phải thực hiện tạo lại thông điệp băm từ thông điệp nhận được nhờ sử dụng giải thuật băm đã được ghi kèm trong chữ ký số.

c. So sánh hai thông điệp băm: Thông điệp băm vừa được tạo sẽ được so sánh với thông điệp băm được giải mã ở trên. Nếu chúng giống nhau thì chữ ký được xác thực còn nếu khác nhau thì có thể thông điệp đó không được ký bởi người gửi hoặc thông điệp đó bị hỏng, trong cả hai trường hợp thì thông điệp sẽ bị loại bỏ.



Hình 8.11. Biểu đồ lớp của ứng dụng

Hình 8.12.

* Để bảo vệ khóa riêng được an toàn hơn, chương trình đã tích hợp module sinh trắc học vào. Mỗi lần tạo chữ ký số, và giải mã thông điệp, người dùng phải lấy được khóa riêng của mình, thay vì phải nhập password như thông thường, người sử dụng phải thực hiện quét vân tay để lấy ra được khóa cá nhân trong cơ sở dữ liệu.

8.2.4. Các công nghệ sử dụng trong chương trình

Chương trình được xây dựng bằng ngôn ngữ C++, trên môi trường lập trình Visual C++ 7.1, sử dụng các hàm API về mật mã của thư viện OpenSSL

Các module chính của ứng dụng:

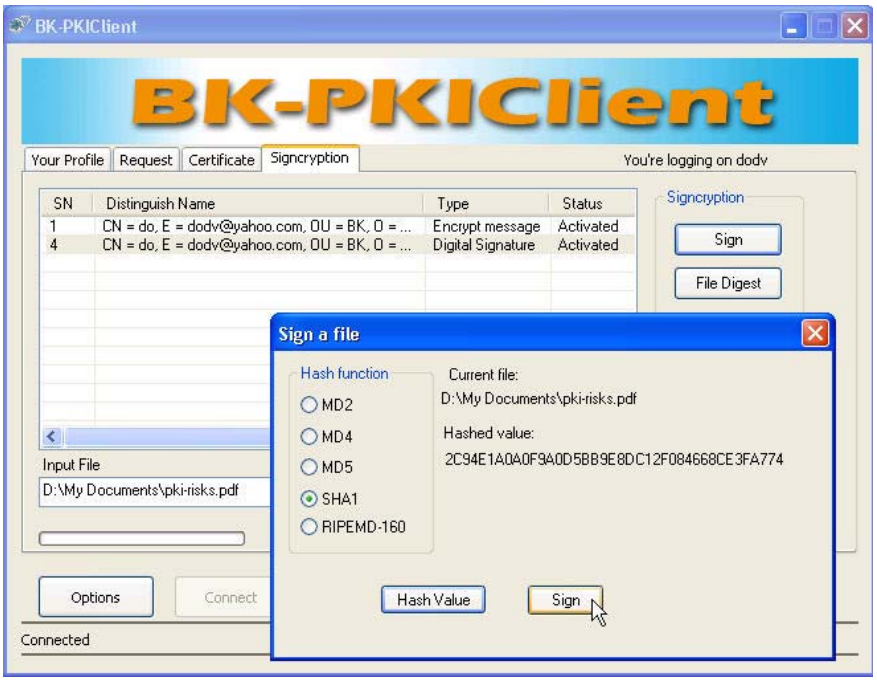
- Module về ký và mã hóa một file: dữ liệu đưa vào là một file có kích thước bất kỳ, sẽ được bên gửi sử dụng khóa riêng để ký, sau đó là mã hóa. File sau khi mã hóa sẽ chứ số Serie của chứng chỉ của người nhận và khóa đối xứng đã được mã hóa.
- Module giải mã và xác thực chữ ký số: thực hiện chức năng giải mã file và khôi phục lại file gốc, sau đó xác thực chữ ký đi kèm với file xem có đúng là do người gửi ký không và trả về thông tin chữ ký đó.

Hình 8.13. Giao diện chính của ứng dụng

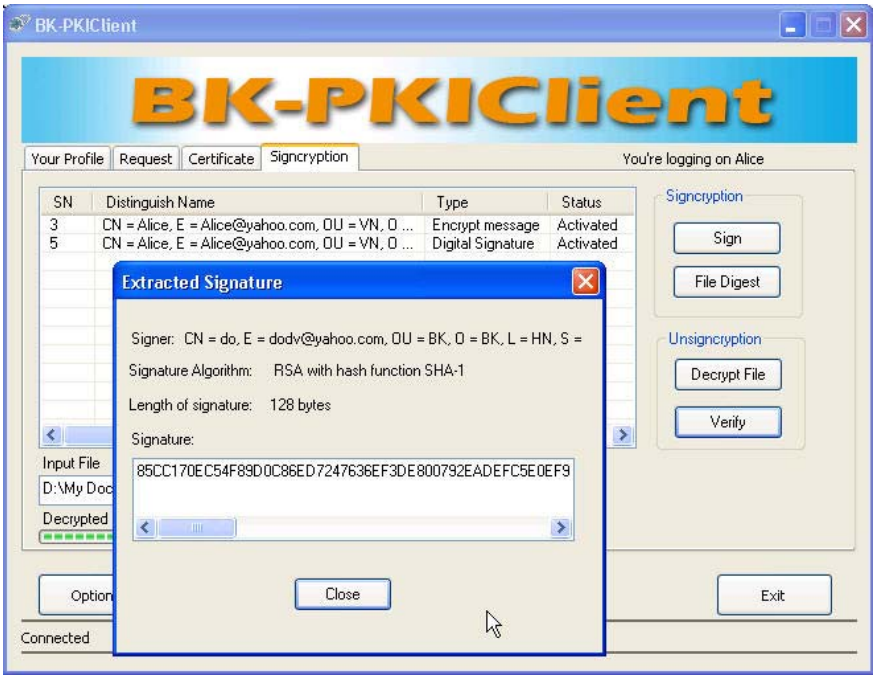
Các lớp chính được cài đặt trong ứng dụng:

- Lớp CertList thể hiện danh sách các chứng chỉ đang hoạt động của người sử dụng. Danh sách này giúp cho người sử dụng lựa chọn chứng chỉ để sử dụng cặp khóa công khai/ khóa riêng
- Lớp DigitalSignature bao gồm các phương thức thực hiện các chức năng ký, mã hóa, giải mã và xác thực chữ ký
- Lớp CEncryptedSymKey cài đặt các hàm để sinh khóa đối xứng, yêu cầu lấy chứng chỉ từ CA dựa vào số serie của chứng chỉ đó. Sau đó sẽ thực hiện mã hóa khóa đối xứng vừa được sinh ra bằng khóa công khai
- Lớp CSignature thực hiện chức năng băm file, sau đó sử dụng khóa cá nhân của người dùng để tạo chữ ký số từ thông điệp băm này

- Lớp CExtractedSignature thể hiện thông tin về chữ ký số sau khi đã được xác thực



Hình 8.14. Giao diện ứng dụng thực hiện chức năng ký



Hình 8.15. Giao diện ứng dụng sử hiển thị thông tin về chữ ký số sau khi đã được xác thực

8.2.5. Thử nghiệm và đánh giá

Ứng dụng ký và mã hóa đã thực hiện được yêu cầu kết hợp hay chức năng ký và mã hóa, tích hợp vào trong hệ thống BK-BioPKI và sử dụng dấu hiệu sinh trắc để lấy khóa cá

nhân. Ứng dụng thực hiện được việc mã hóa và giải mã một cách chính xác, nhanh và đảm bảo tính bảo mật cao. Ứng dụng đã thử nghiệm với các file có độ dài khác nhau

- Với file có kích thước 1MB, thời gian mã hóa và giải mã là 0.12 s
- Với file có kích thước 10MB, thời gian mã hóa và giải mã là 0.8 s
- Với file có kích thước 100MB, thời gian mã hóa và giải mã là 7.11 s

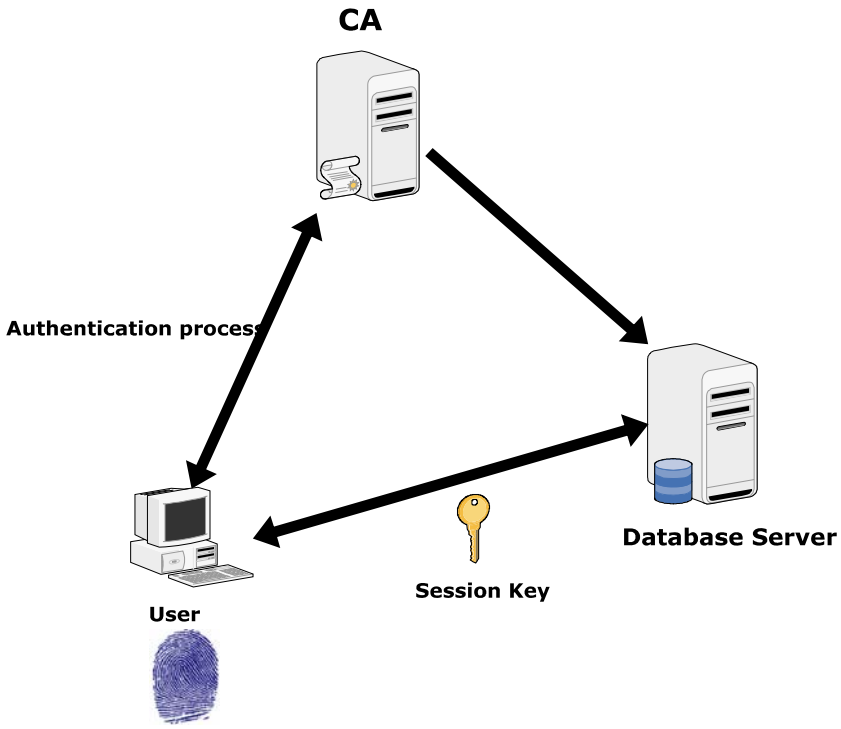
Tuy nhiên, thời gian đó còn phụ thuộc vào tốc độ xử lý của từng máy tính khác nhau.

8.3. Ứng dụng thử nghiệm kiểm soát bảo mật truy cập từ xa

8.3.1. Yêu cầu tăng cường bảo mật truy cập từ xa và giải pháp

Thông thường, trong một mạng máy tính, để có thể thực hiện truy cập từ xa vào một máy chủ CSDL (DBServer), người dùng cần phải có một tài khoản trong DBServer đó với một tên truy nhập và một mật khẩu. Nhưng trên thực tế, mật khẩu này rất dễ bị mất, hay bị lộ, ví dụ trong trường hợp máy tính của người dùng đó bị cài một tiến trình chạy ẩn và đánh cắp thông tin mật khẩu đó. Điều này thực sự rất nguy hiểm, vì khi đó, người dùng sẽ bị kẻ xấu mạo danh, hoặc nguy hiểm hơn, DBServer sẽ bị tấn công.

Ứng dụng tăng cường bảo mật truy cập từ xa sử dụng một mô hình giải pháp kiểm soát truy cập từ xa trong ngữ cảnh hệ thống BK-BioPKI để giải quyết vấn đề trên. Ứng dụng thử nghiệm được xây dựng gồm 3 đối tượng:



Hình 8.16. Mô hình ứng dụng kiểm soát truy cập CSDL từ xa trên mạng.

- CA trong hệ thống BK-BioPKI: ở trong mô hình ứng dụng này, CA đóng vai trò là trung gian xác thực.
- Người dùng muốn thực hiện truy cập từ xa.

- DBServer.

8.3.2. Phân tích và thiết kế ứng dụng thử nghiệm.

Mục đích của ứng dụng:

Ứng dụng được xây dựng với các mục đích sau:

- Xác thực chính xác người dùng muốn truy cập từ xa vào máy chủ CSDL.
- Tạo 1 phiên giao dịch an toàn giữa người dùng và DBServer.
- Ngay khi phiên giao dịch kết thúc, khóa phiên cần phải được xóa bỏ và trở nên vô nghĩa.

Các chức năng ứng với các đối tượng được mô tả qua biểu đồ UseCase sau:

Các đối tượng tham gia trong kịch bản ứng dụng:

- Người dùng: là đối tượng muốn truy cập từ xa vào máy chủ CSDL. Đầu tiên, đối tượng phải xác định được chính xác máy chủ muốn truy cập. Ngoài ra, người dùng còn phải đưa thông tin về sinh trắc học vân tay lên cho DBServer.
- CA: Đối tượng này đóng vai trò trung gian xác thực. CA cần phải xác thực chính xác người dùng. CA cần phải tự sinh khóa phiên cho phiên giao dịch giữa người dùng và DBServer.
- Máy chủ CSDL: Sau khi đã nhận được kết quả xác thực của CA, máy chủ sẽ đồng ý cho người dùng truy cập trong phiên giao dịch an toàn tương ứng.

Điều kiện thực hiện truy cập từ xa:

Để có thể thực hiện truy cập từ xa, cần phải thỏa mãn một số điều kiện sau:

- Người dùng cần phải có chứng chỉ kiểu “truy cập từ xa” trong hệ thống BK-BioPKI.
- Để có được chứng chỉ này, các đặc trưng vân tay của người đó phải được lưu trữ ở CA. (các đặc trưng này được gửi lên CA trong quá trình yêu cầu chứng chỉ).

Ngoài ra, cần có những cơ sở về hệ thống như sau:

- Bộ thư viện OpenSSL bao gồm các hàm về mã hóa, giải mã Blowfish và các hàm có chức năng tạo kênh mật SSL.
- Hệ thống cần có hệ quản trị CSDL MySQL.

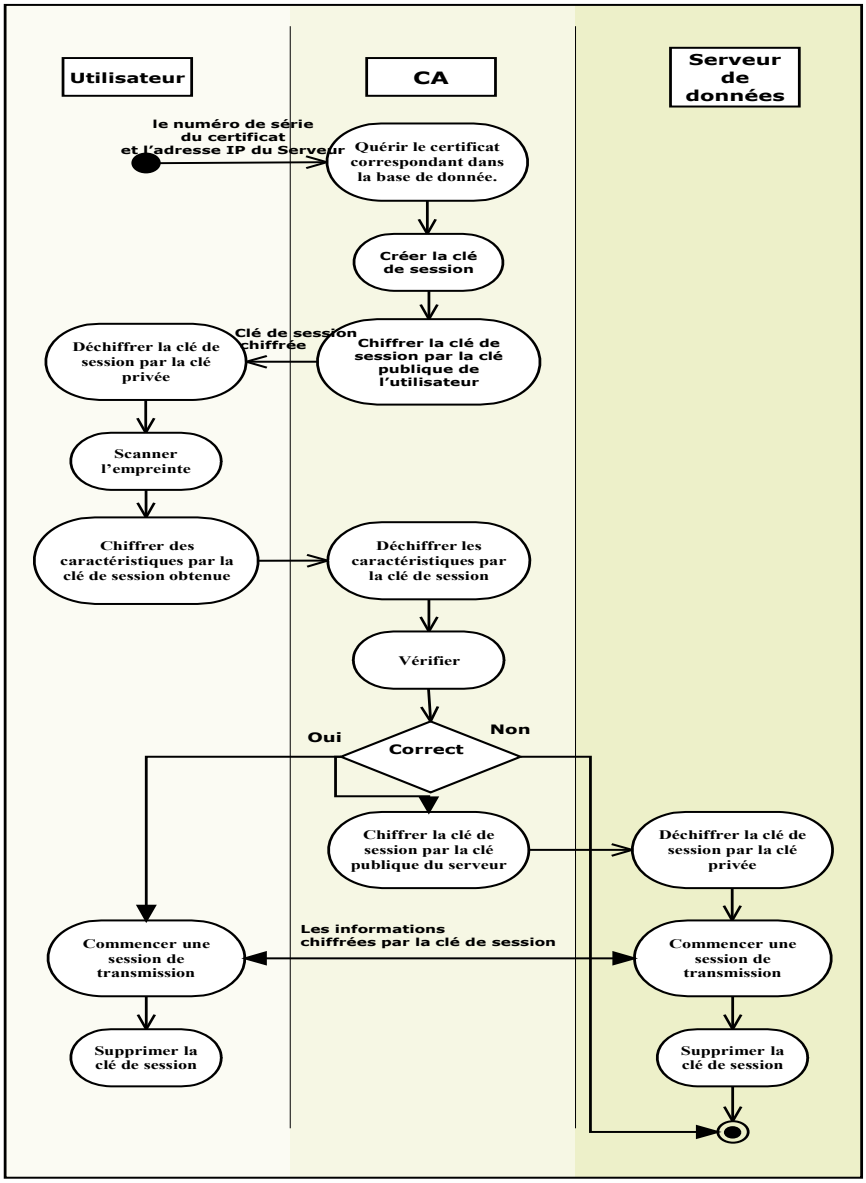
Tiến trình xác thực:

- CA sinh ra một khóa phiên cho phiên giao dịch giữa User và DBServer.
- Người dùng phải gửi các đặc trưng vân tay lên cho CA để thực hiện thẩm định.
- CA thực hiện quá trình thẩm định vân tay số:
    - Nếu thành công: cho phép người dùng truy cập vào DBServer.
    - Nếu không thành công: dừng tiến trình và từ chối truy cập của người dùng.

Trong trường hợp kết quả thẩm định thành công, người dùng được phép truy cập vào DBServer trong một phiên giao dịch an toàn.

Khi phiên giao dịch này kết thúc, khóa phiên được xóa bởi CA.

8.3.3. Kịch bản ứng dụng, kịch bản thử nghiệm và kết quả thử nghiệm



Hình 8.17. Kịch bản ứng dụng.

Các bước lần lượt của mô hình kịch bản hoạt động được mô tả như sau:

1. Người dùng gửi yêu cầu truy cập từ xa lên CA, có kèm theo số serialnumber của chứng chỉ của mình.
2. CA nhận được yêu cầu, truy vấn trong CSDL của mình, tìm được chứng chỉ tương ứng, đồng thời lấy được khóa công khai của chứng chỉ đó.
3. CA sinh ra một khóa phiên, mã hóa khóa phiên đó bằng khóa công khai vừa lấy ra được, và gửi lại cho người dùng.

4. Người dùng nhận được, dùng khóa cá nhân của mình, giải mã lấy ra được khóa phiên.
5. Người dùng thực hiện quét vân tay, dùng module enrollement để trích chọn ra được đặc trưng, và mã hóa đặc trưng vân tay bằng khóa phiên vừa thu được, và gửi lên cho CA.
6. CA dùng khóa phiên, giải mã ra được đặc trưng vân tay, sau đó truy vấn trong CSDL lấy ra được đặc trưng vân tay tương ứng của người dùng đó đã có từ pha xin cấp chứng chỉ. CA thực hiện thẩm định 2 tập đặc trưng này, đưa ra kết quả.
7. Nếu kết quả là không chấp nhận, CA gửi kết quả từ chối cho người dùng, đồng thời kết thúc tiến trình. Nếu kết quả là chấp nhận, CA mã hóa khóa phiên bằng khóa công khai của DBServer và gửi cho DBServer.
8. DBServer dùng khóa riêng của mình để giải mã ra được khóa phiên.
9. Phiên giao dịch giữa User và DBServer bắt đầu được thực hiện với mỗi bên đều đã có khóa phiên.
10. Khi phiên giao dịch này kết thúc, khóa phiên bị xóa đi.

Triển khai chương trình:

Các hàm liên quan đến chứng chỉ:

Các hàm sử dụng	Mô tả
X509Certificate GetCertificate(POSITION pos)	Thu nhận chứng chỉ trong CertList
EVP_Pkey GetPrivateKey(int serialnumber)	Lấy khóa cá nhân trong chứng chỉ có số SN là serialnumber.
EVP_Pkey GetPublicKey(X509Certificate Cert)	Lấy khóa công khai từ chứng chỉ

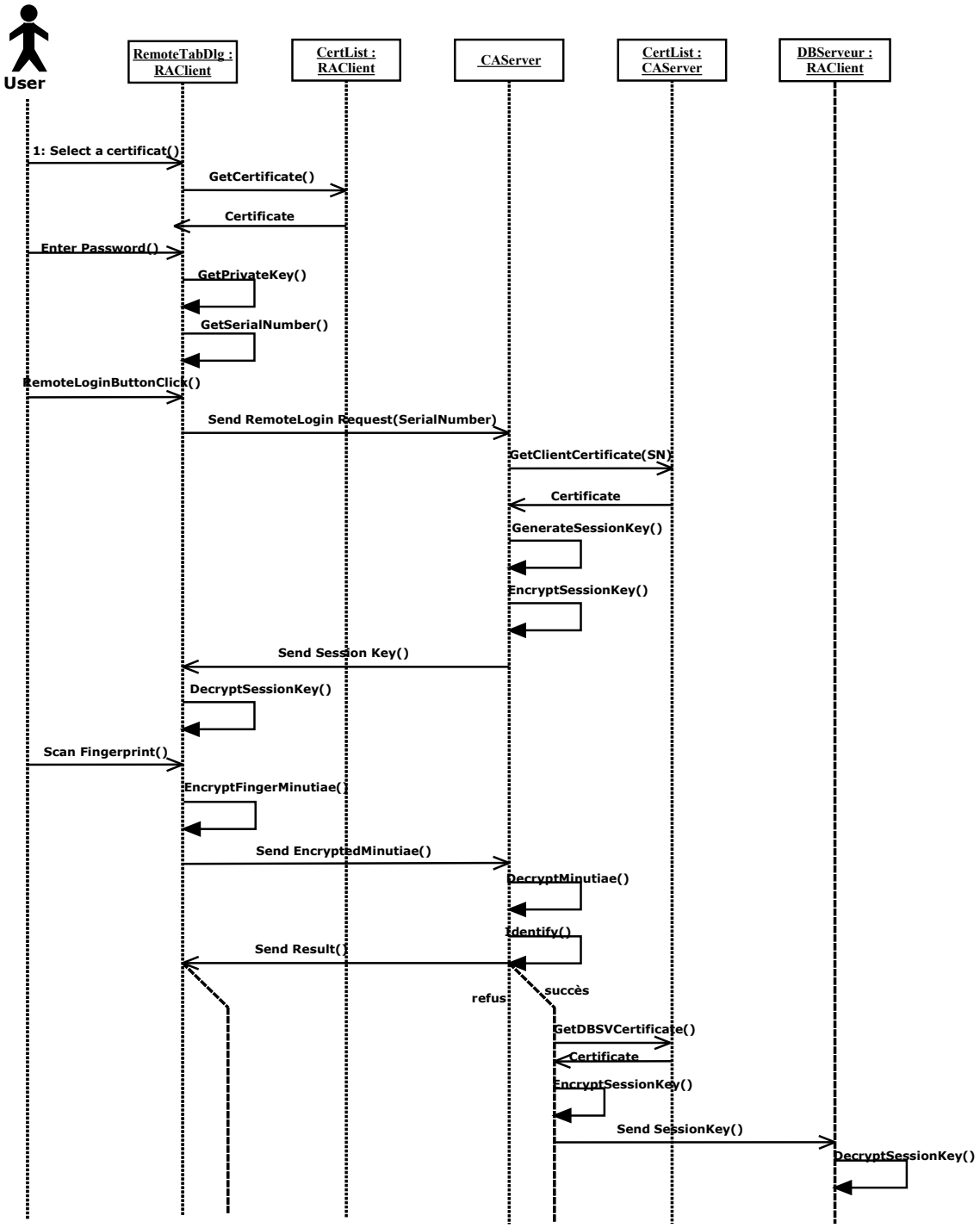
Các hàm liên quan đến mã hóa, giải mã:

Các hàm sử dụng	Mô tả
SKey GenerateSessionKey()	Sinh khóa phiên
char* EncryptSessionKey(SKey* sk,EVP_Pkey* Pk)	Mã hóa khóa phiên
SKey DecryptSessionKey(char* buf,EVP_Pkey* pk)	Mã hóa khóa phiên bằng khóa cá nhân.
char* EncryptFingerMinutiae(Minutiae* mn,SKey sk)	Mã hóa đặc trưng vân tay bằng khóa phiên.
Minutiae* DecryptMinutiae(char* buf, SKey sk)	Giải mã đặc trưng vân tay bằng khóa phiên

Các hàm giao tiếp giữa 3 đối tượng

Các hàm sử dụng	Mô tả
void SendRemoteLoginRequest(int sn,int id)	Người dùng gửi yêu cầu truy cập đến CA
void SendSessionKey(char* sk)	Gửi khóa phiên đã mã hóa
void SendEncryptedMinutiae(char* mn)	Gửi đặc trưng đã mã hóa.

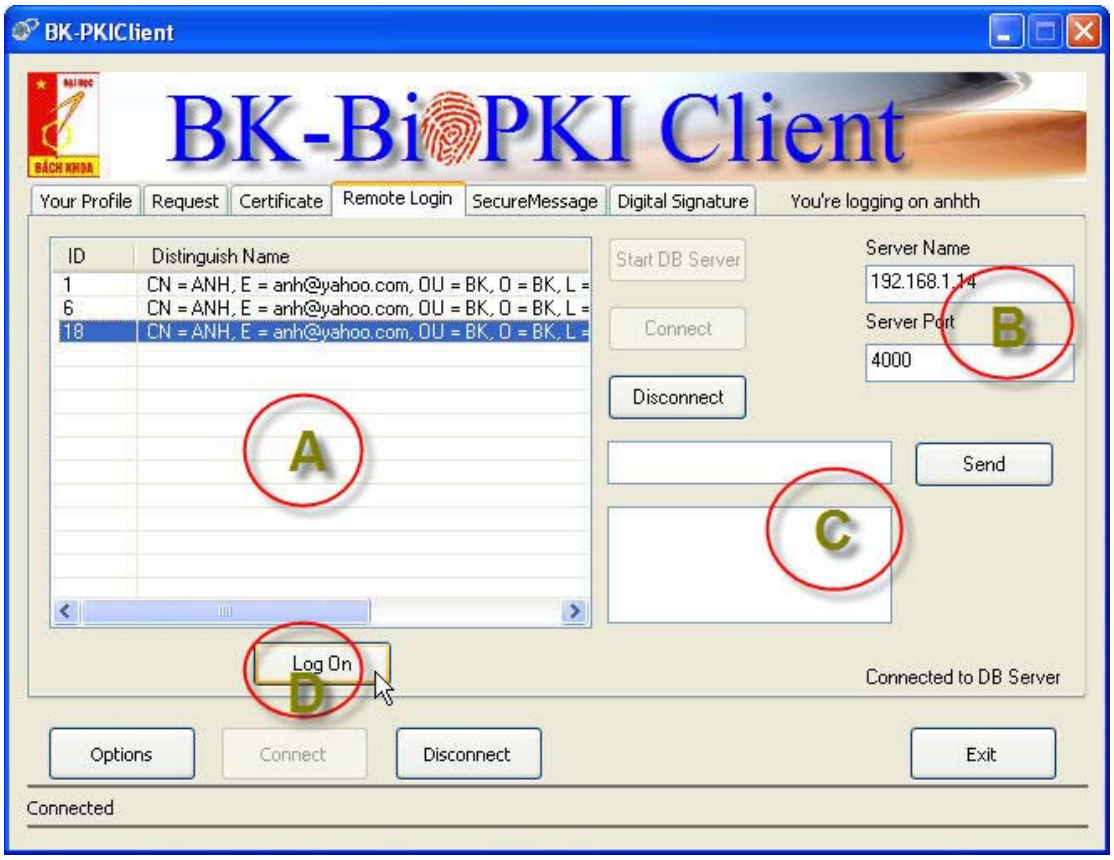
Để hiểu rõ hơn cách sử dụng các hàm, chúng ta quan sát biểu đồ sequence sau đây:



Hình 8.18. Biểu đồ sequence của ứng dụng.

Triển khai giao diện chương trình:

Giao diện chương trình được xây dựng với mục đích người dùng thật dễ sử dụng. Chương trình là 1 Tab trong giao diện chính của chương trình RA_Client.



Hình 8.19. Giao diện ứng dụng.

Giao diện chương trình gồm có 4 phần chính sau:

- A: Danh sách các chứng chỉ có kiểu truy cập từ xa.
- B: Thành phần xác thực máy chủ CSDL.
- C: Bộ phận để test giao dịch giữa DBServer và người dùng.
- D: Phím “Logon” để thực hiện truy cập từ xa.

Đầu tiên, người dùng chọn chứng chỉ muốn dùng để thực hiện truy cập từ xa, sau đó xác thực DBServer cần truy cập đến, và chọn phím Logon.

Nếu thành công, người dùng sẽ nhận được thông báo sau:

Hình 8.20. Thông báo truy nhập thành công.

Thử nghiệm.

Ứng dụng xác thực truy cập từ xa này đã được thử nghiệm trong môi trường mạng LAN của phòng thí nghiệm liên mạng của khoa CNTT trường ĐH BKHN. Ứng dụng đã được tích hợp vào chương trình RA_Client của hệ thống BK-BioPKI.

Kết quả thử nghiệm.

Qua các thử nghiệm, kết quả thu được là:

- DBServer trong hệ thống BK-BioPKI đã được bảo vệ một cách an toàn.
- Với kịch bản trên, ứng dụng có thể tránh được phần lớn các phương thức tấn công.
- Thời gian thực hiện xác thực nhanh.

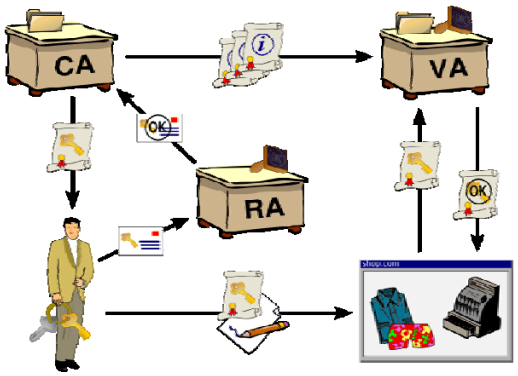
8.4. Ứng dụng an toàn trao đổi thông tin trên SMS

8.4.1. Yêu cầu của ứng dụng

Các giải pháp bảo mật thông tin bao gồm bảo đảm 3 yêu cầu: đảm bảo thông tin được truyền chính xác, đảm bảo thông tin được truyền đến đúng đích tin mong muốn và đảm bảo thông tin được nhận từ đúng nguồn tin. 3 yêu cầu này được thực hiện dựa trên việc mã hóa thông tin.

Mã hóa khóa đối xứng thực hiện việc mã hóa và giải mã bằng cùng một khóa chung. Các giải thuật mã hóa khóa đối xứng thường dùng là DES, RSA, ... Nhược điểm lớn nhất của mã hóa khóa đối xứng là việc trao đổi khóa giữa nguồn và đích cần có một kênh truyền bảo mật riêng.

Để khắc phục nhược điểm trên, hệ thống mật mã hóa khóa công khai và bí mật ra đời. Nguyên tắc cơ bản của phương pháp mã hóa này là quá trình mã hóa giải mã sử dụng một cặp khóa, trong đó từ khóa này rất khó (đòi hỏi một khối lượng tính toán lớn) mới có thể suy ra được khóa còn lại. Một trong 2 khóa được gọi là khóa bí mật, chỉ có duy nhất chủ sở hữu của khóa được biết, khóa còn lại là khóa công khai, được phổ biến cho tất cả các thực thể có thể tham gia truyền tin. Bài toán phổ biến khóa đã được giải quyết.



Hình 8.20

Để có thể sử dụng khóa bí mật và khóa công khai một cách hiệu quả, cần có một hệ thống chung cho tất cả các thực thể tham gia vào truyền tin. Hệ thống này cần quản lý các liên hệ giữa khóa công khai và các thực thể. Mối liên hệ này được biểu diễn bằng các chứng chỉ (certificat). Một chứng chỉ xác nhận mối liên hệ giữ một khóa công khai với một thực thể tham gia truyền tin. Liên hệ này được xác thực bởi thực thể chứng thực (Certificate Authority). Hệ thống để quản lý các chứng chỉ để truyền tin gọi là hạ tầng cơ sở truyền tin khóa công khai (Public Key Infrastruture) có các chức năng cơ bản là quản lý các yêu cầu tạo chứng chỉ, xác thực sử dụng các chứng chỉ, quản lý các chứng chỉ. 2 chức năng

đầu tiên được thực hiện bởi RA, việc quản lý chứng chỉ được thực hiện bởi CA. Liên hệ giữa các CA trong một hệ thống PKI có thể được triển khai theo các mô hình đơn CA, phân cấp hoặc mô hình CA xí nghiệp.

Với sự phát triển của ngành viễn thông, các hệ thống nói trên không chỉ sử dụng hạ tầng truyền thông Internet hoặc Intranet thông thường để hoạt động, mà còn sử dụng các hạ tầng truyền thông đặc biệt như GPRS, SMS, MMS, CDMA, ... Các hạ tầng truyền thông này thường bị hạn chế bởi khả năng truyền tin, khả năng xử lý thông tin của các thiết bị đầu cuối. Việc bảo mật thông tin trên các hạ tầng truyền thông đặc biệt được tiến hành bằng cách: i. dựa vào phần cứng của hạ tầng truyền thông; ii. xây dựng giao thức truyền thông dựa trên PKI cho phù hợp với hạ tầng.

Giải pháp được trình bày ở đây giải quyết vấn đề đã nêu theo cách tiếp cận (ii). Giải pháp được thực hiện trên hạ tầng truyền tin SMS và có khả năng ứng dụng trên các hạ tầng truyền thông khác.

8.4.2. Giải pháp truyền thông tin cậy bằng SMS

Hệ thống ứng dụng cơ sở hạ tầng khóa công khai bảo mật thông tin tin nhắn được xây dựng trên cơ sở lấy hạ tầng khóa công khai làm nền cho ứng dụng truyền thông tin tin nhắn có mã hóa. Khách hàng sử dụng hệ thống mã hóa khóa công khai để tạo ra cặp khóa công khai - bí mật cho mình. Và cơ sở hạ tầng khóa công khai dựa trên hệ thống mã hóa khóa công khai để tiến hành việc cấp phát và chứng thực khóa công khai cho khách hàng.

Trên thực tế thì với các thiết bị có tài nguyên và tốc độ tính toán lớn thì việc mã hóa, chuyển thông tin ứng dụng cơ sở hạ tầng khóa công khai sẽ diễn ra rất đơn giản. Khi đó A muốn chuyển một thông điệp cho B thì A chỉ cần mã hóa thông điệp của mình cần gửi bằng khóa công khai của B. Khi đó chắc chắn chỉ có B mới có khả năng giải mã và thông tin đã được chuyển di một cách an toàn. Tuy nhiên, với các thiết bị như điện thoại di động thì việc mã hóa cả nội dung văn bản bằng mã khóa công khai của bên nhận bằng thuật toán mã hóa khóa công khai là khó khăn. Nguyên nhân là do tốc độ sử lý hạn chế của điện thoại, ngoài ra với thuật toán mã hóa bất đối xứng thì thời gian thực hiện mã hóa là tương đối lớn. Do đó, việc áp dụng trực tiếp mã hóa sử dụng khóa công khai là không khả thi.

Chính từ các hạn chế trên mà nhóm nghiên cứu đề xuất một phương thức trao đổi thông tin như sau:

- Để làm giảm thời gian mã hóa bằng hệ thống mã hóa công khai sử dụng khóa công khai của người nhận, chúng ta sẽ sử dụng mã hóa bất đối xứng
- Do mã hóa bất đối xứng cần có một khóa bí mật để mã hóa thông điệp cần gửi, chính vì vậy chúng ta phải phát sinh một khóa phiên để mã hóa thông tin cần gửi.

Giao thức truyền thông tin tin nhắn có mã hóa sẽ được tiến hành như sau:

Giả sử bên A muốn gửi cho bên B một văn bản cần mã hóa, đầu tiên bên A sẽ phát sinh một khóa phiên, sau đó bên A sẽ mã hóa nội dung thông tin cần gửi bằng khóa phiên đấy với thuật toán mã hóa đối xứng. Khóa phiên được mã hóa hai lần bằng thuật toán mã hóa khóa công khai với khóa bí mật của bên A và khóa công khai ở bên B. Sau đó bên A sẽ

gửi văn bản và khóa được mã hóa cho bên B. Bên B dựa vào khóa công khai của bên A và khóa bí mật của mình để giải mã khóa phiên. Qua đó giải mã nội dung văn bản.

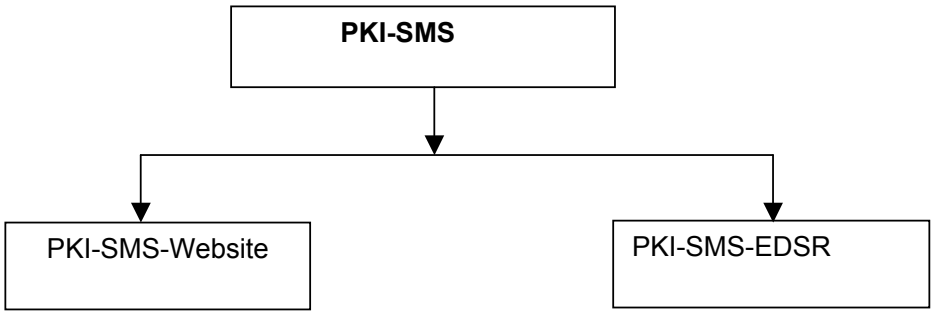
Giải pháp kết hợp này được xem là hợp lý, việc mã hóa văn bản có kích thước lớn sẽ được tiến hành thông qua thuật toán mã hóa đối xứng, việc mã hóa khóa phiên sẽ được tiến hành dựa trên cơ sở hạ tầng khóa công khai.

Do đó, hệ thống đã kết hợp được cơ sở hạ tầng khóa công khai trong việc bảo mật thông tin tin nhắn.

8.4.3. Phân tích thiết kế ứng dụng

Hệ thống ứng dụng cơ sở hạ tầng khóa công khai trong bảo mật thông tin SMS đảm bảo sự an toàn trong việc truyền thông tin bằng tin nhắn SMS. Hệ thống cho phép khách hàng có thể đăng ký giấy chứng thực, kiểm tra chứng thực đã được nhà thẩm quyền ký thông qua giao thức ứng dụng không dây(WAP). Hệ thống được xây dựng gồm hai phần: PKI-SMS-Website và PKI-SMS-EDSR (chương trình cho phép mã hóa, giải mã, gửi và nhận tin nhắn SMS trên điện thoại di động).

Hệ thống được xây dựng trên nền tảng ngôn ngữ java và cơ sở dữ liệu Oracle. Hệ thống Website được xây dựng trên nền tảng Spring. Sau đây là biểu đồ phân cấp hệ thống



Hình 8.21. Biểu đồ phân cấp hệ thống PKI-SMS

Khó khăn trong việc xây dựng hệ thống PKI-SMS

- **Độ dài tin nhắn SMS:** Như chúng ta đã biết thì việc tin nhắn SMS có độ dài tối đa chỉ là 160 ký tự. Hơn nữa trong giao thức đã đề cập đến ở trên thì chúng ta cần phải chuyển cả nội dung tin nhắn và khóa phiên được mã hóa.

  Do độ dài hạn chế của tin nhắn nên tạo ra rất nhiều khó khăn trong quá trình xác định các thông số đầu vào cho hệ thống PKI-SMS(như kích thước khóa phiên, kích thước nôi dung tin nhắn, kích thước khóa công khai…)
- Ngoài ra, do vấn đề **an toàn trong từng phiên giao dịch** nên kích thước khóa phiên, khóa công khai cũng không được phép quá nhỏ. Bởi khi đó thì việc bẻ khóa sẽ trở nên dễ dàng hơn rất nhiều.
- Một yếu tố cuối cùng không thể không nhắc đến đó là vấn đề **tài nguyên hạn chế của điện thoại di động**. Với những chiếc điện thoại có tài nguyên hạn chế thì việc

mã hóa và giải mã với các thuật toán phức tạp, kích thước khóa lớn trở nên vô cùng khó khăn và bất khả thi.

Chính từ các yếu tố trên nên việc xây dựng hệ thống PKI-SMS gặp phải rất nhiều khó khăn trong việc lựa trọn thuật toán mã hóa khóa công khai, thuật toán mã hóa đối xứng, khích thước khóa phiên và kích thước khóa công khai-bí mật.

Chính vì vậy, hệ thống PKI-SMS được xây dựng với sự lựa chọn các thuật toán và kích thước khóa như sau:

- **Thuật toán mã hóa khóa công khai RSA:** Thuật toán mã hóa khóa công khai RSA dựa trên độ khó của bài toán phân tích một số ra thừa số nguyên tố. Đây là thuật toán hay được sử dụng nhất hiện nay và nó đã chứng minh được tính ổn định cao.

  Để đảm bảo an toàn cho hệ thống mã hóa sử dụng phương pháp mã hóa khóa công khai RSA thì số n(module) phải đủ lớn. Tại thời điểm năm 2005, số lớn nhất có thể được phân tích ra thừa số nguyên tố có độ dài 663 bít với phương pháp phân tán trong khi khóa của RSA có độ dài từ 512,1024 tới 2048 bít. Với khóa 4096 bít thì hầu như không có khả năng bị phá vỡ trong tương lai gần.

  Do đó, người ta thường cho rằng RSA đảm bảo an toàn với điều kiện *n* được chọn đủ lớn. Nếu *n* có độ dài 256 bít hoặc ngắn hơn, nó có thể bị phân tích trong vài giờ với máy tính cá nhân dùng các phần mềm có sẵn. Nếu n có độ dài 512 bít, nó có thể bị phân tích bởi vài trăm máy tính tại thời điểm năm 1999. Để đảm bảo an toàn đối với hệ thông PKI-SMS thì kích thước khóa tối ưu nên chọn là 4096 bít.

  Tuy nhiên việc lựa chọn này chỉ hợp lý đối với các thiết bị có tài nguyên lớn. Việc mã hóa và giải mã đối với khóa 4096 bít được thử nghiệm với điện thoại K750i của Sony Ericssion với kích thức nội dung văn bản cần mã hóa chỉ là 8 byte là không thể thực hiện. Tài nguyên của điện thoại không cho phép việc mã hóa nội dung thông tin bằng thuật toán mã hóa khóa công khai với kích thước khóa là 4096 bít.

  Chính vì vậy mà hệ thống PKI-SMS sẽ sử dụng kích thức khóa công khai là **512 bít** cho thuật toán mã hóa RSA. Việc lựa chọn thông qua thử nghiệm trên điện thoại K750i cho thời gian mã hóa văn bản 8 byte chỉ mất 3s. Đây là khoảng thời gian chấp nhận được đối với điện thoại di động.

- **Thuật toán mã hóa nội dung thông tin tin nhắn**: do thuật toán mã hóa bất đối xứng, cụ thể là thuật toán mã hóa khóa công khai RSA mất rất nhiều thời gian để tiến hành việc mã hóa và giải mã nên việc mã hóa nội dung thông tin được tiến hành thông qua thuật toán mã hóa đối xứng DES.

  Việc lựa chọn thuật toán mã hóa đối xứng DES là do độ dài 56 bit của khóa là nhỏ. Chính vì vậy việc mã hóa sẽ diễn ra trong khoảng thời gian rất nhanh. Hiện nay,khóa DES bị phá trong trong thời gian ngắn nhất vẫn là 24 giờ, trong khi đó với việc phiên giao dịch của chúng ta chỉ diễn ra trong vòng chưa đến 10 giây. Điều này cho phép phiên giao dịch sẽ diễn ra với tính an toán cao đồng thời giản tối đa các tính toán phức tạp trên thiết bị điện thoại di động.

- **Kích thước khóa phiên**: Kích thước khóa phiên được lựa chọn là 8 byte(4 ký tự) là hợ lý. Bởi nó không gây ra sự khó chịu cho khách hàng đồng thời đảm bảo được tổng thời gian mã hóa khóa phiên bằng thuật toán mã hóa khóa công khai RSA và mã nội dụng tin nhắn bằng thuật toán DES là chấp nhận được.

Từ các lý luận trên, hệ thống PKI-SMS sẽ được xây dựng với các thành phần sau:

- Thuật toán mã hóa khóa công khai được lựa chọn là RSA
- Kích thước cặp khóa công khai- bí mật được lựa chọn là 512 bít
- Thuật toán mã hóa nội dung tin nhắn được lựa chọn là DES
- Kích thước khóa phiên là 8 byte

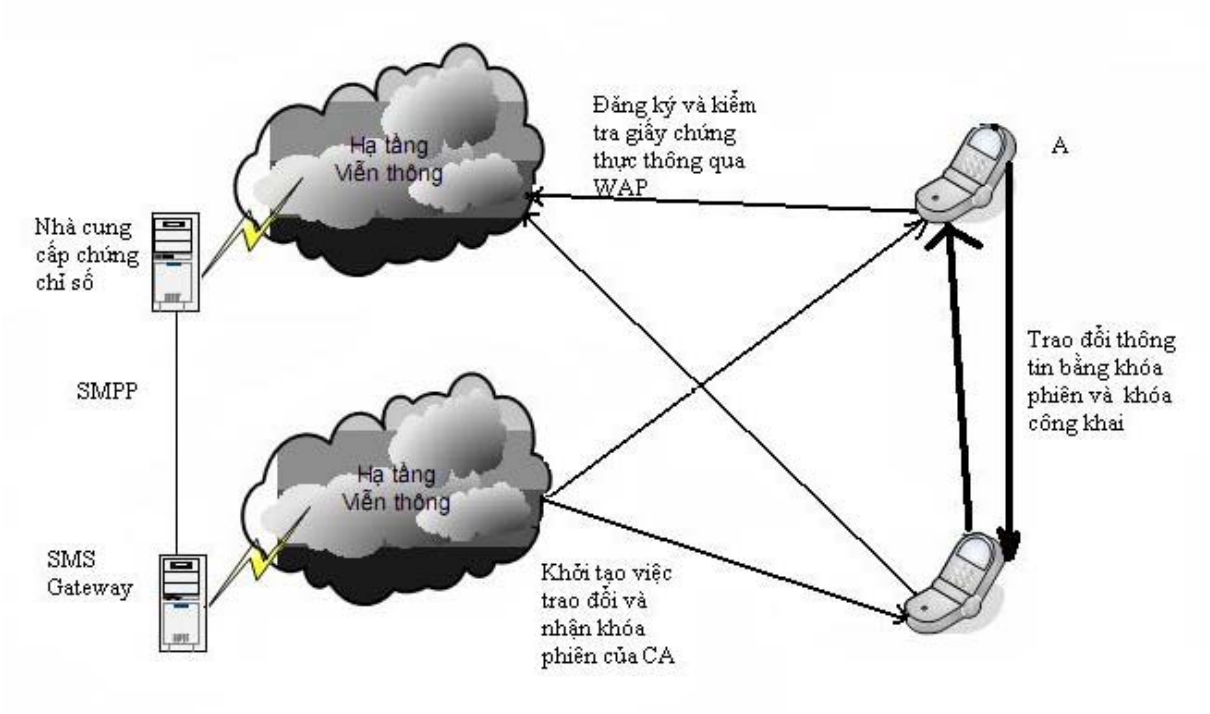
Hệ thống PKI-SMS sẽ được xây dựng gồm hai phần, phần PKI-SMS-Website và PKI-SMS-EDSR.

Việc tách hệ thống ra thành hai phần là do khó khăn trong vấn đề tạo khóa, đăng ký và chứng thực trên điện thoại với thuật toán RSA là rất khó khăn. Nguyên nhân là do giấy chứng thực khóa công khai cấp bao gồm nhiều trường, kích thước tương đối lớn. Việc chứng thực giấy chứng nhận khóa công khai đối với điện thoại di động lại gặp vấn đề vè tài nguyên. Khi kích thước đầu vào lớn thì việc chứng thực lại bất khả thi trên điện thoại.

Tuy nhiên, do điện thoại ngày nay có khả năng kết nối Intener bằng giao thức WAP thông qua việc cài đặt GPRS nên vấn đề đã được giải quyết. Vì vậy, hệ thống đã được chia thành hai phần.

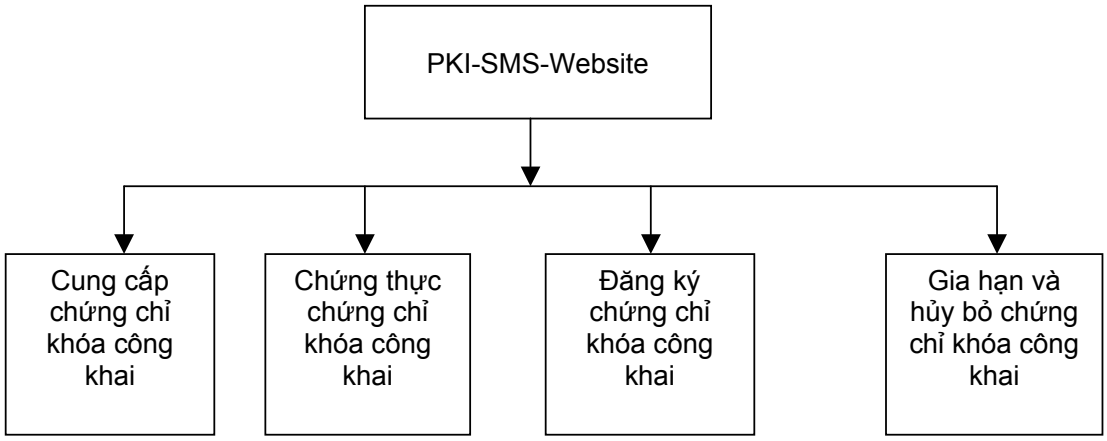
- Phần PKI-SMS-Website được dùng để đăng ký và chứng thực giấy chứng nhận khóa công khai(được viết bắng Spring framework theo chuẩn WAP)
- Phần PKI-SMS-EDSR được viết bắng ngôn ngữ J2me của Java với thư việc mã hóa nguồn mở bouncycastle

Mô hình hệ thống

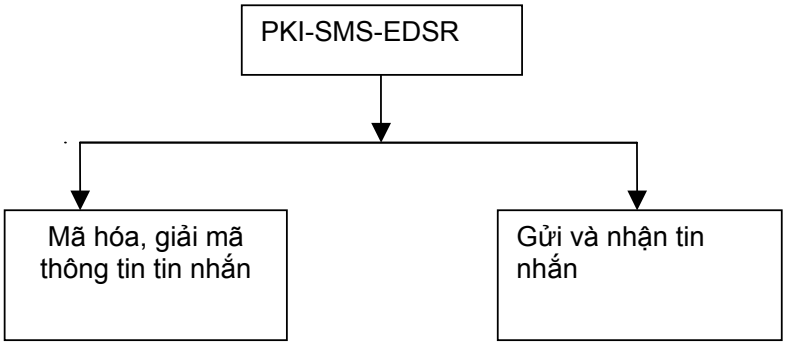


Hình 8.22. Mô hình hệ thống PKI-SMS

Biểu đồ phân cấp chức năng



Hình 8.23. Biểu đồ chức năng PKI-SMS-Website



Hình 8.24. Biểu đồ chức năng PKI-SMS_EDSR

Chi tiết các chức năng

Tên chức năng	Loại	Mô tả
1.1 Cung cấp chứng chỉ khóa công khai	Web Form	Hiện thị thông tin về chứng chỉ khóa công khai
1.2 Chứng thực chứng chỉ khóa công khai	Web Form	Hiện thị kết quả chứng thực khóa công khai
1.3 Đăng ký chứng chỉ khóa công khai	Web Form	Hiện thị thông tin đăng ký chứng chỉ khóa công khai
1.4 Gia hạn và hủy bỏ chứng chỉ khóa công khai	Web Form	Hiện thị thông tin về tình trạng và thời hạn của chứng chỉ khóa công khai
2.1 Mã hóa, giải mã thông tin tin nhắn	Service	Cung cấp chức năng mã hóa và giải mã nôi dung tin nhắn trên điện thoại di động
2.2 Gửi và nhận tin nhắn	Service	Cung cấp chức năng gửi và nhận tin nhắn trên điện thoại di động

Thiết kế cơ sở dữ liệu

Các bảng trong cơ sở dữ liệu

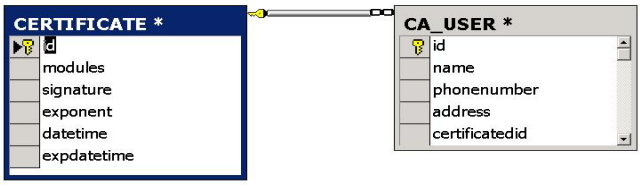
CERTIFICATE (Giấy chứng thực khóa công khai)

Tên trường	Kiểu dữ liệu	Cho phép để trắng	Khóa chính	Ghi chú
ID	INTEGER	Không	Có	
MODULE	VARCHAR (500)	Không	Không	Module công khai
SIGNATURE	VARCHAR (500)	Không	Không	Chữ ký của nhà thẩm quyền lên giấy chứng thực
EXPONENT	VARCHAR (500)	Không	Không	Số mũ công khai
DATETIME	DATE	Không	Không	Ngày khách hàng đăng ký giấy chứng thực khóa công khai
EXPDATETIME	DATE	Không	Không	Ngày hết hạn của giấy chứng thực

CA_USER ()

Tên trường	Kiểu dữ liệu	Cho phép để trắng	Khóa chính	Ghi chú
ID	INTEGER	Không	Có	
NAME	VARCHAR (100)	Không	Không	
PHONENUMBER	VARCHAR (20)	Không	Không	
ADDRESS	VARCHAR (500)	Không	Không	
CERTIFICATEID	INTEGER	Không	Không	

Mô hình quan hệ giữa các bảng



8.4.4. Đánh giá và thử nghiệm

Chức năng thiết kế

Cấp chứng thực khóa công khai

Hệ thống PKI-Website cho phép người dùng đăng ký khóa công khai thông qua giao thức ứng dụng không dây(WAP)

Chứng thực khóa công khai

Hệ thống PKI-Website cho phép người dùng chứng thực khóa công khai thông qua giao thức ứng dụng không dây(WAP)

CA ký giấy chứng thực khóa công khai

Hệ thống PKI-Website được dùng để CA ký xác nhận của mình thông qua thuật toán mã hóa khóa công khai RSA với khóa bí mật của CA.

Mã hóa và giải mã thông tin

Chương trình PKI-SMS-EDSR cho phép người dùng thực hiện việc mã hóa, truyền và giải mã tin nhắn

Kịch bản thử nghiệm

Thiết bị: Điện thoại Sony Ericssion K750i, Nokia N72

Dữ liệu

+Dữ liệu ngắn: PKISMS

+Dữ liệu dài: PKISMS TEST PROGRAM

+Kích thước khóa 512 bít

+Kích thước khóa 1024 bít

+Kích thước khóa 4096 bít

+Kích thước khóa phiên 8 byte

+Kích thước khóa phiên 16 byte

Tính năng kỹ thuật

Tốc độ truyền tin

Tốc độ truyền tin nhắn phụ thuộc vào nhà cung cấp dịch vụ. Thời gian truyền tin mất từ 3->4 giây.

Kết quả thực nghiệm

Với điện thoại SonyEricssion K750i thì kết quả được thể hiện qua bảng sau:

	Kích thước khóa 512 bít, Khóa phiên 8 byte	Kích thước khóa 1024 bít, Khóa phiên 8 byte	Kích thước khóa 2048 bít, Khóa phiên 8 byte	Kích thước khóa 512 bít, Khóa phiên 16 byte	Kích thước khóa 1024, Khóa phiên 16 byte	Kích thước khóa 4096 bít, Khóa phiên 16 byte
Tốc độ mã hóa	3s		Bộ mô phỏng không thực hiện được	3s		Bộ mô phỏng không thực hiện được
Tốc độ giải mã	2s		Bộ mô phỏng không thực hiện được	2s		Bộ mô phỏng không thực hiện được
Độ dài tin nhắn tối đa	7 ký tự			7 ký tự		
Độ dài tin nhắn sau mã hóa	145 ký tự	273 ký tự >160		145 ký tự	273 ký tự >160	
Kết luận	Có thể	Không thể dùng	Không thể dùng	Có thể	Không thể dùng	Không thể dùng

Với điện thoại Nokia N72 kết quả cũng tương tự Sony Ericssion K750i và được thể hiện qua bảng sau:

	Kích thước khóa 512 bít, Khóa phiên 8 byte	Kích thước khóa 1024 bít, Khóa phiên 8 byte	Kích thước khóa 2048 bít, Khóa phiên 8 byte	Kích thước khóa 512 bít, Khóa phiên 16 byte	Kích thước khóa 1024, Khóa phiên 16 byte	Kích thước khóa 4096 bít, Khóa phiên 16 byte
Tốc độ mã hóa	3s		Bộ mô phỏng không thực hiện được	3s		Bộ mô phỏng không thực hiện được
Tốc độ giải mã	2s		Bộ mô phỏng không thực hiện được	2s		Bộ mô phỏng không thực hiện được
Độ dài tin nhắn tối đa	7 ký tự			7 ký tự		
Độ dài tin nhắn sau mã hóa	145 ký tự	273 ký tự >160		145 ký tự	273 ký tự >160	
Kết luận	Có thể	Không thể dùng	Không thể dùng	Có thể	Không thể dùng	Không thể dùng

8.5. Kết chương

Các ứng dụng được xây dựng và thử nghiệm cho thấy có thể ứng dụng hệ thống BioPKI vào các ứng dụng cơ bản của hệ thống PKI. Dấu hiệu sinh trắc có thể được sử dụng để bảo vệ khóa cá nhân bí mật như trong trường hợp ứng dụng mã hóa và ký thông điệp. Dấu hiệu này có thể được sử dụng để tăng cường khả năng xác thực trong các hệ thống đã có sẵn cơ chế bảo mật.

Trong các ứng dụng đã đề cập, việc thu thập và xử lý dấu hiệu sinh trắc dừng ở mức cục bộ, không có CSDL chung để lưu trữ các dấu hiệu sinh trắc. Như vậy các thiết bị đầu cuối phải có khả năng xử lý tương đối cao (các thử nghiệm cho thấy thời gian xử lý với các thao tác sinh trắc thông thường khoảng vài giây, nếu các thiết bị có khả năng tính toán kém hơn sẽ không đảm bảo thời gian đáp ứng.

Một hướng phát triển trong tương lai là chuyển một số thao tác xử lý sinh trắc thành tập trung, tạo thành một hệ thống thực sự. Ứng dụng PKI-SMS chuẩn bị sẵn cho khả năng này, với việc thực hiện PKI trên hệ thống truyền thông đặc biệt với tốc độ truyền tin và khả năng xử lý của các thiết bị đầu cuối hạn chế.

Phần IV. TỔNG HỢP CÁC KẾT QUẢ VÀ KẾT LUẬN

1. Các kết quả đạt được của đề tài theo các sản phẩm đã ghi trong thuyết minh nhiệm vụ.

1.1. Tóm tắt các yêu cầu khoa học đối với sản phẩm tạo ra (kết quả dạng II và III)

Tên sản phẩm:

Hệ thống an ninh thông tin dựa trên mã sinh trắc học Bio-PKI (gọi tắt là Hệ thống an ninh thông tin Bio-PKI), bao gồm:

- Kết quả giải pháp tích hợp đặc trưng vân tay với mã bảo mật trong hệ PKI thành hệ BioPKI.
- Kết quả thử nghiệm Prototype về hạ tầng hệ thống BioPKI để thẩm định vân tay trong hệ BioPKI.
- Kết quả phần mềm máy tính cho hệ thống BioPKI, phân hệ sinh trắc bao gồm: phần mềm phân hệ mã hóa khóa sinh trắc học vân tay BioPKI và phần mềm xác thực thẩm định vân tay.
- Các báo cáo: Báo cáo phân tích hệ thống và hướng xây dựng ứng dụng trong xác thực thâm định vân tay và điều khiển truy nhập trong hệ BioPKI; Các báo cáo định kỳ và báo cáo tổng hợp đề tài.

1.2 Kết quả các sản phẩm dạng các báo cáo đã đăng ký

- Đảm bảo đầy đủ số lượng các báo cáo định kỳ

- Đảm bảo đầy đủ số lượng về các sản phẩm báo cáo đã đăng ký đã được tổng hợp trong báo cáo bao gồm :

Báo cáo khảo sát phân tích và xây dựng phương án giải pháp hệ thống an ninh thông tin Bio-PKI (chương 1, 2, 3 ,4)

Báo cáo phân tích và thiết kế hệ thống an ninh sinh trắc học Bio-PKI (chương 5, 6, 7)

Báo cáo các ứng dụng thử nghiệm (chương 8)

1.3 Kết quả các sản phẩm đã đăng ký

Đảm bảo đầy đủ số lượng các sản phẩm dạng đã ghi trong thuyết minh và trong hợp đồng, gồm có:

1.3.1. Kết quả về giải pháp tích hợp đặc trưng vân tay với mã bảo mật trong hệ PKI thành hệ thống BioPKI

Đề tài đã đề xuất mô hình giải pháp tích hợp đặc trưng vân tay với hạ tầng khóa công khai thành hệ thống BioPKI, được trình bày trong chương 4 và chương 7 của báo cáo này.

Mô hình hệ thống BioPKI bao gồm các thành phần hệ thống sau:

- Hệ thống lõi hạ tầng khóa công khai PKI: Hệ thống lõi PKI được xây dựng theo mô hình kiến trúc CA với đầy đủ các thành phần chức năng cơ bản của hê PKI bao gồm:
  - CA (Certificate Authority): Bộ phận thẩm quyền phát hành các chứng chỉ và chứng thực các chứng chỉ
  - RA (Registration Authority): Bộ phận thẩm quyền đăng ký chứng chỉ,
  - Certificate Holder- User: người sử dụng trong hệ thống PKI, chủ thể chứng chỉ,
  - Digital Certificate Distribution System: Hệ thống phân phối chứng chỉ số, kho chứa

  Hệ thống lõi PKI được thiết kế và lập trình trên môi trường bộ thư viện mã nguồn mở OpenSSL, theo chuẩn X509. Trong mô hình hệ BioPKI hiện nay RA có vai trò quản lý người dùng, lưu trữ khóa cá nhân được bảo mật bằng sinh trắc vân tay. Toàn bộ các giao thức và các giao dịch cơ sở giữa RA và CA được thiết kế và cài đặt làm cơ sở để tích hợp hệ sinh trắc tạo vào máy người sử dụng (users)
- Hệ thống thẩm định xác thực sinh trắc vân tay (Fingerprint Biometric System)
  dùng sinh trắc vân tay sống được lấy trực tuyến từ thiết bị scanner. Hoạt động của hệ thống sinh trắc gồm 2 pha chức năng: Đăng ký (enrollement), thẩm định xác thực (verification)
- Mô hình tích hợp thẩm định trắc vân tay sống trực tuyến vào hệ lõi hạ tầng khóa công khai (gọi tên là BK-BioPKI), bao gồm 2 phân hệ sinh trắc sau:
  - Phân hệ thẩm định xác thực trực tuyến vân tay người dùng được tích hợp vào quá trình đăng nhập hệ thống BioPKI thay password, các dấu đặc trưng vân tay được mã hóa và lưu trữ tại máy user (được gọi là Phân hệ sinh trắc 1)
  -Phân hệ sinh trắc vân tay kết hợp với quá trình mật mã và sử dụng chứng chỉ số trong hệ Bio PKI, sinh khóa sinh trắc để mã hóa bảo mật khóa cá nhân của người dùng trong hệ thống (đươc gọi là Phân hệ sinh trắc 2). Phần mềm phân hệ sinh trắc 2 được tích hợp vào hệ BioPKI tại máy user, được quản lý bởi RA và xác thực bởi CA (chi tiết của mô hình tích hợp sẽ được trình bày trong chương 5 và chương 7 báo cáo này)

1.3.2 Kết quả thiết kế và xây dựng thử nghiệm hệ thống BioPKI (Prototype) kết hợp thẩm định xác thực vân tay sống, trực tuyến. (Trình bày trong các chương 5, 6, 7)

- Giải pháp công nghệ thiết kế, triển khai hệ thống BK-BioPKI và tích hợp mã sinh trắc học vân tay vào hạ tầng PKI, xác thực sinh trắc vân tay trong hệ thống BioPKI

- Phân tích thiết kế toàn bộ hệ thống BK-BioPKI (prototype): Đã phân tích thiết kế và xây dựng cài đặt thử nghiệm một hệ thống BioPKI (tên gọi BK-BioPKI) thẩm định xác thực vân tay sống lấy trực tuyến từ thiết bị Scanner thông dụng. Hệ thống BK-BioPKI hoạt động trên môi trường mạng PTN tại khoa CNTT – ĐHBK HN. Toàn bộ hệ thống được xây dựng cài đặt trên cơ sở công cụ bộ thư viện OpenSSL và ngôn ngữ C++ kết hợp Matlab

1.3.3 Kết quả phần mềm máy tính cho hệ thống BioPKI: phần mềm hệ sinh trắc bao gồm: phần mềm phân hệ mã hóa khóa sinh trắc học vân tay BioPKI và phần mềm xác thực thẩm định vân tay (trình trong các chương 5 và 7)

Đề tài đã xây dựng và cài đặt toàn bộ phần mềm cho hệ thống BK-BioPKI bao gồm các bộ phần mềm sau:

- ***Bộ phần mềm cơ sở hệ lõi PKI*** đảm bảo được các chức năng cơ bản của một cơ sở hạ tầng khóa công khai PKI với CA đơn: tạo yêu cầu xin cấp chứng chỉ, cấp phát chứng chỉ, quản lý, gia hạn chứng chỉ và hủy bỏ chứng chỉ.
- **Bộ phần mềm hệ thẩm định xác thực vân tay sống, trực tuyến gồm các chức năng chủ yếu**:
  + Phần mềm đăng ký sinh trắc học vân tay BioPKI
  + Phần mềm mã hóa
  + Phần mềm xác thực thẩm định vân tay BioPKI

  Bộ phần mềm sinh trắc trong hệ thốngBioPKI được xây dựng thành 2 phân hệ thống sinh trắc tương ứng với mô hình kết hợp 2 phân hệ sinh trắc vào các hoạt động trong hệ BioPKI.
- Bộ phần mềm tích hợp hệ thống an ninh sinh trắc học Bio-PKI: Thực hiện tích hợp hệ thẩm định xác thực vân tay vào hoạt động các giao dịch đăng nhập, xin cấp chứng chỉ và sử dụng chứng chỉ trong hệ thống. Các hình vẽ dưới đây trình bày 2 sơ đồ diễn tiến lập trình trong số nhiều sơ sồ diễn tiến đã được thiết kế và thực hiện các bước trong các giao dịch hoạt động trong hệ thống BioPKI.
- Chương trình thử nghiệm sinh trắc lòng bàn tay: Cài đặt thuật toán trích chọn đặc trưng, thẩm định xác thực sinh trắc lòng bàn tay và thử nghiệm với CSDL ảnh lòng bàn tay (xem chi tiết phần phụ lục Báo cáo tổng hợp.

1.3.4 Phần mềm thử nghiệm ứng dụng

Đề tài đã xây dựng thử nghiệm 3 kịch bản ứng dụng an toàn bảo mật thông tin trong môi trường hệ thống BK-BioPKI (trình bày chi tiết trong chương 7 và chương 8 của báo cáo tổng hợp), gồm có:

- Xác thực chữ ký số
- Ký và mã hóa bảo mật thông điệp
- Kiểm soát bảo vệ truy cập vào CSDL trên mạng

Các kịch bản này đã được thiết kế chi tiết, được lập trình cài đặt và thủ nghiệm trong môi trường mạng của hệ thống BK-BioPKI tại PTN.

1.3.5 Các kết quả thực nghiệm trong phòng thí nghiệm

a/ Mô tả kịch bản thử nghiệm

Hiện nay toàn bộ hệ thống tích hợp BK-BioPKI được xây dưng trong môi trường mạng trong PTN theo cấu hình đã trình bày ở trên. Tại các máy người sử dụng, dùng thiết quét vân tay

Futronic's FS82 USB 2.0 Fingerprint để lấy vân tay sống trực tuyến dùng cho 2 pha của hệ thống: pha đăng ký và pha thẩm định xác thực liên quan đến chứng chỉ.

Quá trình thử nghiệm hệ thống bao gồm 2 nội dung chủ yếu: Thử nghiệm các hoạt động giao dich trong hệ thống BK-BioPKI thông qua các ứng dụng và thử nghiệm đánh giá thống kê thực nghiệm các tham số chất lượng hệ thống thông qua các độ đo tỷ số từ chối sai FRR (False Rejection Rate) và tỷ số chấp nhận sai FAR (False Acceptance Rate)

Tính toán thực nghiệm các tham số đánh giá hệ thống (%):

$$\text{Tỷ số từ chối sai} \quad \text{FRR} = \frac{So\ truong\ hop\ loai\ bo\ sai}{Tong\ so\ truong\ hop}$$

$$\text{Tỷ số chấp nhận sai} \quad \text{FAR} = \frac{So\ truong\ hop\ chap\ nhan\ sai}{Tong\ so\ truong\ hop}$$

a. Thử nghiệm các giao dịch cơ sở trong hệ BK-BioPKI và đánh giá mức độ trơn của các hoạt động giao dịch trong hệ thống:

- Thực hiện các quá trình cài đặt CA và RA (5 lần) để kiểm tra mức độ lỗi trong chương trình.
- Đăng ký người sử dụng: 10 người. Kiểm tra các lỗi phát sinh trong quá trình từ lúc đăng ký người dùng vào hệ thống đến khi lấy được chứng chỉ.
- Thống kê các lỗi nếu xảy ra trong quá trình thực hiện giao dịch

- ***Thử nghiệm các ứng dụng và đánh giá thực nghiệm thamg số chất lượng thẩm định xác thực sinh trắc vân tay trong hoạt động hệ BK-BioPKI***

Trong mỗi hoạt động hệ sinh trắc bao gồm 2 pha : Đăng ký và thẩm định xác thực sinh trắc. Theo mô hình giải pháp hệ BK-BioPKI đã trình bày ở trên, hệ sinh trắc bao gồm 2 phân hệ kết hợp: phân hệ thẩm định sinh trắc đăng nhập đầu vào và phân hệ thẩm định sinh trắc để giải mã truy xuất lấy khóa cá nhân (private key) để thực hiện các giao dịch: ứng dụng chữ ký số hoặc ứng dụng bảo mật thông điệp

- Thử nghiệm thẩm định sinh trắc trong hoạt động đăng nhập vào hệ thống:
  - Thực hiện lấy mẫu của 10 người sử dụng
  - Để đánh giá tỷ số chấp nhận sai FAR : với mỗi người dùng, thử nghiệm với 10 mẫu vân tay không dùng để đăng ký
  - Để đánh giá tỷ số từ chối sai FRR : mỗi người thử nghiệm đăng nhập 10 lần sau khi đã đăng ký vân tay, dùng vân tay đăng ký để thử nghiệm và đo số trường hợp sai
- Thử nghiệm thẩm định xác thực sinh trắc vân tay người dùng đề truy xuất lấy khóa cá nhân và thực hiện ứng dụng chữ ký số: sinh khóa sinh trắc BEK bảo mật khóa cá nhân.
  - 5 người sử dụng yêu cầu được cấp phát chứng chỉ và sau đó dùng chứng chỉ đề thực hiện chữ ký số.

- Đánh giá thực nghiệm các tham số chât lượng thẩm định khóa sinh trắc để truy xuất khóa cá nhân:

- Đánh giá tỷ số chấp nhận sai FAR: với mỗi người dùng, thử nghiệm với 10 mẫu vân tay khác mẫu vân tay đã dùng để đăng ký đề thử nghiệm xác thực và đo số lần chấp nhận sai

- Để đánh giá tỷ số từ chối sai FRR: mỗi người thử nghiệm 10 lần thẩm định xác thực dùng vân tay đăng ký để thử nghiệm truy xuất khóa cá nhân và đo số trường hợp sai

b/ Kết quả thực nghiệm

- ***Kết quả thực nghiệm đánh giá quá trình thẩm định sinh trắc trong hoạt động đăng nhập (login)***

Số lần thực hiện	Số từ chối sai/ Số chấp nhận sai	Tỷ số từ chối sai FRR(%)	Tỷ lệ chấp nhận sai FAR (%)
100	23	23	
100	19		19

Bảng 1: Kết quả thực nghiệm Tỷ lệ FRR và FAR khi đăng nhập

- ***Kết quả thực nghiệm đánh giá quá trình thẩm định sinh trắc để truy xuất lấy khóa cá nhân dung trong hoạt động chữ ký số***

Số lần thực hiện	Số từ chối sai/ Số chấp nhận sai	Tỷ số từ chối sai FRR(%)	Tỷ lệ chấp nhận sai FAR (%)
100	23	23	
100	14		14

Bảng 2: Kết quả thực nghiệm Tỷ lệ FRR và FAR khi xác thực khóa sinh trắc vân tay song trực tuyến đề giải mã truy xuất khóa cá nhân trong hoạt động ký chữ ký số

Khi thử nghiệm tăng số mẫu vân tay trong quá trình đăng ký (ví dụ lây 3 mẫu vân tay khi đăng ký thay cho lấy 1 mẫu trong thử nghiệm trên) thì tỷ số lỗi FRR được cải thiện giảm xuống khoảng 12% - 10%, tuy nhiên thời gian tính lại tăng lên.

- ***Kết quả thử nghiệm độ trơn trong hoạt động của hệ thống và tính thực nghiệm tỷ số các lỗi phát sinh***

Kết quả cho thấy hầu hết các giao dịch của hệ thống (từ cài đặt CA, RA, đăng nhập, yêu cầu cấp chứng chỉ, chữ lý số, truy nhất khoa cá nhân) đã hoạt động đầy đủ các chức năng đã thiết kê PKI, không xảy ra lỗi, hoạt động trơn tru đặc biệt là các kết nối giữa CA-RA (các giao dịch về chứng chỉ) và giữa các RA với nhau (chữ ký số)

Số lần cài đặt	Số lần lỗi	Tỉ lệ (%)
5	5	0

Bảng 3 . Kết quả đánh giá quá trình cài CA

Số lần cài đặt	Số lần lỗi	Tỉ lệ (%)
5	5	0

Bảng 4. Kết quả đánh giá quá trình cài RA

- Tuy nhiên trong quá trình thực hiện cho thấy có một số lần còn lỗi xảy ra trong quá trình đăng ký vân tay khi tạo yêu cầu (request) để gửi lên CA. Đây là lỗi quá trình đăng ký sinh trắc (enrollment) vân tay người dùng vào yêu cầu và là lỗi liên quan đến thuật toán sinh trắc. Lỗi này hoàn toàn có thể khắc phục được thông qua việc cải thiện thuật toán trích chọn đặc trưng và chương trình xử lý sinh trắc.

Đánh giá kết quả thực nghiệm

Qua các kết quả thử nghiệm trong phòng thí nghiệm về hệ thống BK-BioPKI có thể cho thấy toàn bộ hệ thống nền tảng lõi PKI được thực hiện tốt, hoạt động khá hoàn thiện , các giao dịch từ cài đặt, cấp chứng chỉ, xác thực chứng chỉ, nhìn chung hoạt động ổn định và không có lỗi. Các chức năng của một hệ thống BioPKI được thực hiện tương đối hoàn chỉnh và đảm bảo các hoạt động xác thực sinh trắc vân tay sống trong hệ thống BK-BioPKI ở các mức khác nhau. Hoạt động toàn bộ hệ thống BK-Biopki đã được kiểm nghiệm qua các thực nghiệm với các sinh trắc vân tay sống trực tuyến và đạt bước đầu khả quan. Điều đó đã kiểm nghiệm thực tế mô hình giải pháp hệ thống BioPKI đề xuất và quá trình phân tích thiết kế hệ thống đã đạt kết quả tốt.

Tuy nhiên, về đánh giá các tham số hiệu năng hệ thống vẫn còn có lỗi ở quá trình sinh trắc, thể hiện lỗi do xử lý chưa hết các trường hợp ngoại lệ. Thực nghiệm với vân tay sống cho thấy tỷ số lỗi FRR và FAR trong cả 2 quá trình hoạt động xác thực sinh trắc tỷ lệ lỗi vẫn còn tương đối cao. Đó chính là vấn đề cần tiếp tục cải tiến về hệ thẩm định xác thực sinh trắc

Trong điệu kiện cấu hình hệ thống trong môi trường phòng thú nghiệm, thời gian thực hiện thuật toán còn lớn (khoảng gần 40s). Hiệu năng về thời gian xử lý sinh trắc còn chậm thể hiện chủ yếu do phần tích hợp các thuật toán sinh trắc (viết bằng Matlab) vào hệ PKI chỉ ở mức mô hình tích hợp.

2. Kết quả phối hợp với Malaysia.

2.1. Đặc điểm quá trình hợp tác

- Về tiến độ thời gian bắt đầu thực hiện nhiệm vụ nghị định thư của 2 phía Malaysia và Việt Nam có sự chênh lệch: Nhiệm vụ của phía Malaysia đã thực hiện từ 2005, thực hiện trước một năm so với nhiệm vụ của phía Việt Nam.

- Khi nhiệm vụ phía Việt Nam chính thức bắt đầu thì phía Malaysia đang là giai đoạn cuối của nhiệm vụ đề tài phía Malaysia đề xuất trong nhiệm vụ hợp tác Nghị định thư và phía Malaysia đã kết thúc đề tài này 2006.

- Phía bạn tiếp tục nghiên cứu về lĩnh vực này và từ 6-2007 phía Malaysia có kinh phí thực hiện đề tài thứ hai (theo tài liệu bạn cung cấp, thời gian của đề tài tiếp theo này là từ 15/6/2007 đến 30/5/2008), bởi vậy đến 5/2007 phía bạn mới xúc tiến tiếp tục các hoạt động trao đổi hợp tác qua mail.

- Chủ nhiệm đề tài phía Malaysia có thay đổi, hiện nay là ông Dr. Ong Thian Song, Giám đốc điều hành trung tâm nghiên cứu CBB

- Phía Malaysia tiếp tục nhiệt tình trong hợp tác thực hiện nhiệm vụ NĐT với Viêt Nam.

- Phía bạn chưa thực hiện cử đoàn ra sang Việt Nam như đã dự kiến vì lý do kinh phí của phía bạn.

2.2. Các hoạt động phối hợp nghiên cứu

- Phía MMU tổ chức Hội thảo trao đổi phối hợp nghiên cứu 2 bên tại Malaysia trong thời gian 20-21/ 9/ 2007 để xúc tiến tăng cường hợp tác, gặp gỡ trao đổi cụ thể và phối hợp các công việc nghiên cứu của cả hai bên

MMU-HUT Joint Seminar, 20th - 21th September 2007

CBB-FIST, Multimedia University (Melaka Campus), Malaysia

- Phía Đại học Bách khoa Hà nội đã tham gia trình bày 3 báo cáo trao đổi nghiên cứu tại hội thảo này, bao gồm:
    - H.Lan Nguyen, “BioPKI based information security system using fingerprint biometric authentication”
    - Q.Trung HA, “Using online fingerprint authentication to protect private key for digital signature”.
    - H.Lan Nguyen and Q.Trung Ha, “BioMetric verification based remote authentication”
- Tháng 12/ 2007 và tháng 5/2008: Theo kế hoạch đã duyệt, phía VN đã cử 2 đoàn công tác sang Malaysia làm việc phối hợp nghiên cứu về hệ thống thẩm định sinh trắc (chi tiết đã nêu trong báo cáo ở phần phụ lục)
- Kết quả nghiên cứu phối hợp là trao đổi về phương án, xây dựng mô hình và trao đổi các thuật toán, hiện chưa có sự trao đổi kết hợp phần mềm cụ thể nào trong hệ BK-BioPKI hiên nay
- Để thực hiện được trao đổi phần mềm hoặc tích hợp kết quả 2 bên, theo đề nghị của phía trường MMU cần chuẩn bị để ký bản cam kết (MMA) giữa MMU và HUT (ĐHBK HN). Hiện nay cho đến tháng 12-2008, hai bên đã trao đổi bản thảo và đợi điều kiện để ký. Cho đến nay, phía MMU chưa có đoàn sang ĐHBK HN vi lý do kinh phí và thời gian.
- Hai bên MMU và HUT đã nhất tiếp tục phát triển Hợp tác với Malaysia trong thời gian tới trong khuôn khổ đề tài KC0111 tiếp tục nghiên cứu phát triển hệ thống BioPKI trong giai đoạn tiếp từ 2008-2009.

2.3. Tiếp tục phát triển Hợp tác với Malaysia

Về hợp tác với Malaysia từ 6/2007 đến 6/2008 (xem trình bày chi tiết ở phụ lục báo cáo này) nhiệm vụ hợp tác nghiên cứu đã tiến hành theo mức độ trao đổi tích hợp các kết quả về phương án và phối hợp thực hiện phát triển phần mềm của cả 2 phía.

Hiện nay cả 2 bên (ĐHBK HN và MMU) đã thảo luận và đề nghị tiếp tục nghiên cứu phát triển hệ thống BioPKI trong giai đoạn tiếp từ 2008-2009.

3. Các kết quả khác

3.1 Đào tạo thạc sĩ

- ***Theo hướng của đề tài cho đến nay đã có 6 luận văn Thạc sĩ bảo vệ tốt nghiệp***:

  1. Trần Tuấn Vinh Khóa 2003-2005 đã bảo vệ 2006
     Tên luận văn: "Nghiên cứu giải pháp an ninh thông tin dựa trên hướng tiếp cận sinh trắc học kết hợp mã công khai PKI với đặc điểm sinh trắc vân tay"

  2. Nguyễn Anh Tài Khóa 2004-2006 đã bảo vệ 2006
     Tên luận văn: "Nghiên cứu phương pháp thẩm định xác thực sinh trắc chữ ký viết tay ứng dụng trong giao dịch điện tử"

  3. Vũ Thanh Thắng Khóa 2005-2007 đã bảo vệ 12- 2007
     Tên luận văn: "Nghiên cứu thuật toán mã hóa bảo mật nâng cao AES và xây dựng ứng dụng thuật toán dựa trên công nghệ nhúng"

  4. Lê Quang Tùng Khóa 2006-2008 đã bảo vệ 11- 2008
     Tên luận văn: "Xây dựng giải pháp ứng dụng xác thực sinh trắc học trong cơ sở hạ tầng khóa công khai dựa trên hệ thống OpenCA"

  5. Lê Trần Vũ Anh Khóa 2006-2008 đã bảo vệ 11- 2008
     Tên luận văn: "Nghiên cứu giải pháp ứng dụng hạ tầng khóa công khai PKI trong hệ thống thanh toán điện tử liên ngân hàng"
  6. Hà Tiến Dũng Khóa 2006-2008 đã bảo vệ 11- 2008
     Tên luận văn: "Hệ mật khóa công khai và chữ ký số"

- ***Các đồ án kỹ sư tốt nghiệp ngành CNTT- ĐHBK HN đã thực hiện theo hướng đề tài***: Một số lượng đông đảo khoảng 20 đồ án tốt nghiệp của sinh viên các khóa (K46, K47, K48) có trong danh sách tham gia đề tài (Phần I) đã bảo vệ tốt nghiệp Kỹ sư CNTT – ĐHBK HN đạt kết quả khá và giỏi.

3.2. Các bài báo khoa học

[1] Thi Hoàng Lan NGUYEN, Thi Thu Hăng NGUYEN "*An Approach to Protect Private Key using Fingerprint Biometric Encryption Key in BioPKI based Security System*", bài báo đá được nhận đê trình bày và sẽ đăng trong kỷ yếu Hội nghị quốc tế: IEEE-10th International Conference on Control, Automation, Robotics and Vision (ICARCV 2008), December 17-20, 2008 in Hanoi, Vietnam.

[2] Nguyễn Thị Hoàng Lan, Bùi Thành Đạt, Lê Tiến Dũng, "X*ây dựng hệ thống an ninh thông tin dựa trên sinh trắc vân tay và hạ tầng khóa công khai BioPKI*", Trình bày tại Hội thảo Quốc gia lần thứ tư về Nghiên cứu phát triển và ứng dụng Công nghệ thông tin và Truyền thông ICT.rda' 2008, Hà Nội 8- 9/8/2008 (bài báo đang chỉnh sửa theo ý kiến của phản biện để đăng trong Kỷ yếu)

[3] Nguyễn Thị Hoàng Lan, Trần Hải Anh, "*Một giải pháp thẩm định vân tay trực tuyến trong hệ thống BK-BioPKI và ứng dụng kiểm soát truy cập từ xa*", Trình bày tại Hội thảo Quốc gia lần thứ tư về Nghiên cứu phát triển và ứng dụng Công nghệ thông tin và Truyền

thông ICT.rda' 2008, Hà Nội 8- 9/8/2008 (bài báo đang chỉnh sửa theo ý kiến của phản biện để đăng trong Kỷ yếu)

[4]. Nguyễn Thị Hoàng Lan, Hoàng Trần Đức, "Về một ứng dụng mã hóa bảo mật thông điệp trong hệ thông BK-BioPKI", Trình bày tại Hội thảo Quốc gia lần thứ tư về Nghiên cứu phát triển và ứng dụng Công nghệ thông tin và Truyền thông ICT.rda' 2008, Hà Nội 8-9/8/2008.

[5]. Hà Quốc Trung, Nguyễn Trung Dũng, *"Trao đổi thông tin an toàn và bảo mật trên hạ tầng SMS"***,** Trình bày tại Hội thảo Quốc gia lần thứ tư về Nghiên cứu phát triển và ứng dụng Công nghệ thông tin và Truyền thông ICT.rda' 2008, Hà Nội 8- 9/8/2008.

[6]. Nguyễn Linh Giang, Vũ Ngọc Hà, *"Một giải pháp kết hợp chứng chỉ sinh trắc vào hệ thống PKI",* Trình bày tại Hội thảo Quốc gia lần thứ tư về Nghiên cứu phát triển và ứng dụng Công nghệ thông tin và Truyền thông ICT.rda'2008, Hà Nội 8- 9/8/2008.

3.3 Hội thảo mở rộng

Đề tài đã tổ chức 1 hội thảo mở rộng báo cáo kết quả của đề tài với các nội dung sau đã thông báo như sau:

XEMINAR

Hệ thống an ninh thông tin BioPKI dựa trên sinh trắc học vân tay kết hợp với cơ sở hạ tầng khóa công khai PKI

Đề tài KHCN theo nghị định thư hợp tác với Malaysia về "Hệ thống an ninh thông tin dựa trên sinh trắc học Bio-PKI (Bio-PKI Based Information Security System), Khoa Công nghệ thông tin ĐHBK HN, tổ chức Xeminar trình bày các chuyên đề về các kết quả nghiên cứu của Đề tài.

Thời gian : 8h30, ngày thứ sáu 20/ 6/ 2008.

Địa điểm : Phòng hội thảo C10, Đại học Bách khoa Hà Nội

Số 1 Đại Cồ Việt, Hai Bà Trưng, Hà Nội

Nội dung Xeminar gồm các chuyên đề:

- Giải pháp an ninh dựa trên sinh trắc học (Biometric) và mô hình hệ thống an ninh thông tin BK-BioPKI
- Phân tich xây dựng hạ tầng hệ thống PKI, hệ cơ sở để tích hợp sinh trắc học
- Thiết kế xây dựng phân hệ sinh trắc sinh vân tay: sinh khóa sinh trắc và thẩm định xác thực sinh trắc vân tay trực tuyến
- Thiết kế xây dựng prototype hệ thống BK-BioPKI trên cơ sở tích hợp phân hệ sinh trắc vân tay vào hệ PKI trong môi trường mạng phòng thí nghiệm.
- Một số kịch bản ứng dụng thử nghiệm về bảo mật an toàn thông tin trên cơ sở hệ thống BK-BioPKI: Chữ ký số, mã hóa bảo mật thông điệp, bảo mật tin nhắn SMS, kiểm soát truy cập từ xa.

- Kết quả hợp tác với Malaysia.

KÍNH MỜI TOÀN THỂ CÁC QUÍ VỊ QUAN TÂM ĐẾN DỰ VÀ ĐÓNG GÓP Ý KIẾN CHO ĐỀ TÀI

4. Tóm tắt về sử dụng kinh phí

Toàn bộ báo cáo về kinh phí đề tài sẽ được trình bày chi tiết trong báo cáo tài chính, phần dưới đây chỉ nêu tóm tắt về sử dụng kinh phí của đề tài

- Khoản 1. Thuê khoán chuyên môn: đã thanh toán xong. Tổng kinh phí đã thanh toán là 374.950.000 VNĐ (*Ba trăm bảy mươi tư triệu chín trăm năm mươi nghìn đồng)*
- Khoản 2. Nguyên vật liệu, vật tư, năng lượng: đã thanh toán xong. Tổng kinh phí đã thanh toán là 62.035.160 VNĐ (*Sáu mươi hai triệu không trăm ba mươi lăm ngàn một trăm sáu mươi đồng*)
- Khoản 3. Thiết bị, máy móc chuyên dùng: đã thanh toán xong bao gồm: 1 Server IBM, 1 UPS 6KVA, các thiết bị quét để nhận dạng vân tay FX3000. Tổng kinh phí đã thanh toán là 177.735.000 VNĐ (*Một trăm bảy mươi bảy triệu bảy trăm ba mươi lăm ngàn đồng*)
- Khoản 4. Đoàn ra: đã thanh toán xong. Tổng kinh phí đã thanh toán là 88.807.170 VNĐ (*Tám mươi tám triệu tám trăm linh bảy nghìn một trăm bảy mươi đồng*)
- Khoản 5. Đoàn vào: vì lý do phía bạn chưa vào, đã đề nghị và được chuyển kinh phí sang thuê khoán chuyên môn kinh phí là 25.000.000 VNĐ (*Hai mươi lăm triệu đồng*)
- Khoản 6. Chi khác: đã thanh toán xong (trừ phần chi phí đánh giá, kiểm tra, nghiệm thu xin đề nghị tạm ứng trước, sẽ quyết toán sau). Tổng kinh phí là 96.442.000 VNĐ *(Chín mươi sáu triệu bốn trăm bốn mươi hai nghìn đồng)*
- Tổng kinh phí của toàn bộ đề tài đã thanh toán và tạm ứng là **789,969,330** VNĐ (*Bảy trăm tám mươi chín triệu chín trăm sáu mươi chín nghìn ba trăm ba mươi đồng)*

5 . Kết luận và hướng phát triển

5.1. Nhận xét đánh giá chung

- **Đề tài đã hoàn thành nhiệm vụ đã đề ra** đảm bảo về số lượng và chất lượng đã đăng ký về các sản phẩm KHCN. Toàn bộ hệ thống đã được thử nghiệm đạt kết quả bước đầu trong môi trường mạng phòng thí nghiệm. Tuy nhiên kết quả thử nghiệm cho thấy tỷ lệ lỗi xác thực vân tay sống còn lớn, đây là một trong các vấn đề mấu chốt phải tiếp tục nghiên cứu cải thiện trong thời gian tới.

- **Đề tài đã phát triển** cụ thể hơn các nội dung dưới đây so với nội dung đã đăng ký về phần mềm máy tính:

- Về phần mềm tích hợp sinh trắc trong hệ thống: hệ thống BK-BioPKI đã xây dựng bao gồm 2 phân hệ sinh trắc kết hợp 2 giải pháp sinh trắc trong hệ BioPKI
- Về phần mềm thử nghiệm ứng dụng: hiện nay đã xây dựng và thử nghiệm 3 kịch ứng dụng an toàn bảo mật thông tin trong mụi trường hệ thống BK-BioPKI gồm: Xác thực chữ ký số; Ký và mã hóa bảo mật thông điệp; Kịch bản thử nghiệm kiểm soát bảo vệ truy nhập CSDL trên mạng.
- Về sinh trắc lòng bàn: Đã xây dựng thử nghiệm 1 chương trình trích chọn đặc trưng và thẩm định sinh trắc lòng bàn tay, sử dụng ảnh lòng ban tay lấy từ CSDL.

- **Tính mới, tính sáng tạo của đề tài**: hướng nghiên cứu BioPKI là vấn đề đang được quan tâm trên thế giới, các tài liệu và hệ thông an ninh thông tin dựa sinh trắc học hiện chưa nhiều và thường đóng kín do yêu cầu bảo mật. Kết quả của đề tài đã đóng góp tính mới trên mô hình giải pháp tích hợp hệ thống BioPKI thẩm định xác thực sinh trắc vân tay sống. Đó là hệ BioPKI thống mới, cho đến hiện nay dựa trên các thông tin đã công bố, đây là những kết quả đầu tiên nghiên cứu ở Việt Nam về lĩnh vực này

5.2. Về tiến độ thực hiện

- Để tăng cường có hiệu quả trong hợp tác với Malaysia và để đề tài có điều kiện thử nghiệm và hoàn thành tốt nhiệm vụ theo nghị định thư, đề tài đã làm văn bản đề nghị xin phép được điều chỉnh ra hạn thời gian thực hiện tài đến 6/2008 trong điều kiện toàn bộ kinh phí đã được duyệt, không bổ sung thêm kinh phí, như vậy thời gian thực hiện đề tài là tròn 24 tháng như dự kiến.
- Nhiệm vụ đề tài đã được phép của Bộ KHCN, theo có công văn số 3397/BKHCN-XHTN, ký ngày 27/12/2007 cho phép gia hạn thời gian thực hiện nhiệm vụ đề tài đến 6/2008, như vậy đề tài có điều kiện thời gian đầy đủ 24 tháng để thực hiện như dự kiến ban đầu.
- Đề tài đã hoàn thành các công việc nghiên cứu theo đúng kế hoạch đã được phép đến 6-2008. Kết quả nghiên cứu của đề tài đã được trình bày trong Hội thảo mở rộng báo cáo kết quả nghiên cứu đã được tổ chức và thông báo trên mạng vào 20- 6-2008.

5.3 Hướng phát triển

- Đề tài đã đạt các kết quả khả quan trọng bước đầu phòng thí nghiệm, mở ra một triển vọng nghiên cứu phát triển mới có ý nghĩa về hệ thống an ninh thông tin dựa trên sinh trắc học BioPKI và ứng dụng thực tế
- Kết quả của đề tài nhiệm vụ nghị thư là cơ sở để được tiếp tục theo hướng nghiên cứu BioPKI trong giai đoạn tiếp theo trong khuôn khổ Đề tài KC0111.
- Các hướng phát triển nghiên cứu trong thời gian tới trong Đề tài KC0111

- Xây dựng hệ lõi PKI theo các công nghệ và chuẩn công nghiệp OpenCA đề phù hợp với các khả năng sẽ triển khai hệ hạ tầng khóa công khai PKI ở Việt Nam
- Nghiên cứu phát triển mô hình BioPKI với xác thực đa sinh trắc
- Xây dựng hệ tích hợp hệ thống BioPKI trên cơ sở hệ lõi PKI OpenCA
- Thiết kế hệ xác thực sinh trắc sử dụng công nghệ nhúng (Etoken USB)
- Khảo sát và xây dựng các ứng dụng thực tế để có thể đưa hệ thống ra ứng dụng.

TÀI LIỆU THAM KHẢO

[1] PhD Alex Stoianow, PhD Ann Cavoukian, "***Biometric Encryption: A positive – Sum Technology that Achieves Strong Authentication, Security AND Privacy***", Information and Privacy Commissioner/Ontario, March 2007.

[2] William Stallings. "***Cryptography and Network Security Principles and Practices, Fourth Edition***". Prentice Hall, November 16, 2005

[3] F. Hao, R. Anderson, J. Daugman, "***Combining cryptography with biometrics effectively***", Computer Laboratory - University of Cambridge, No. 640, 7-2005.

[4] Martin Drahanský, "***Biometric Security System Fingerprint Recognition Technology***", PhD thesis, Brno University of Technology, Czech Republic, March 2005.

[5] Yoshifumi Ueshige, "***A Study on Biometrics Authentication in BioPKI***", Institute of Systems & Information Technologies, KYUSHU, 2005

[6]. Michael Goh Kah Ong, Tee Comie, Andrew Teoh Beng Jin, David Ngo Chek Ling, "***An automated palmprint recognition system***", Journal of Image Vision Computing, No.23, pp 501-515, Jan. 2005.

[7] Uludag, Anil K. Jain et al "***Biometric Cryptosystems: Issues and Challenges***", Proceedings of the IEEE, Vol.92, No. 6, pp. 948-960, June 2004..

[8] Anil K. Jain and Arun Ross, "***Multibiometric Systems***", Journal Communications of the ACM", Vol. 47, No. 1 2004.

[9] K. Delac, M.Grgic, "***A survey of biometric recognition methods***", 46th International Symposium Electronics in Marine, ELMAR-2004, Zadar, Croatia. pp 1-6, June 2004.

[10] D.Maltoni, D.Maio, A.K.Jain, S.Prabhakar, "***Handbook of Fingerprint Recognition***", Springer, New York, 2003.

[11]. Suranjan Choudhury, Kartik Bhatnagar and Wasim Haque, "***Public Key Infrastructure Implementation and Design***". M&T Books, 2002.

[12]. C.Adam, S.Lloyd, "***Understanding PKI: Concept, Standard and Develoyment Consideration***", 2nd ed. , Addition Wesley 2002.

[13] Parvathi Ambalakat, "*Security of Biometric Authentication Systems*", 21st Computer Science Seminar SA1-T1-1, 2002.

[14] F. Hao, C.W. Chan, "***Private key generation from on-line handwritten signatures***," Information Management & Computer Security - Nanyang Technological University, Singapore, 2002.

[15] Yuliang He, Jie Tian, Xiping Luo, Tanghui Zhang. "***Image enhancement and minutiae matching in fingerprint verification***", Pattern Recognition Letter, 2002.

[16] Pravir Chandra, Matt Messier, John Viega. "***Network Security with OpenSSL***", O'Reilly 2002.

[17]: Sharath Pankanti, Salil Prabhakar, and Anil K.Jain, "***On the Individuality of Fingerprints***", IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp. 805-812, 2001.

[18] Carl Ellison, Bruce Schneier. "***Ten Risks of PKI***". Computer Security Journal Volume XVI, Number 1, 2000.

[19] Serge Aumont, Roland Dirlewanger, Olivier Porte. "***L'accès sécurisé aux données***". JRES 1999.

[20] Lin Hong, Yifei Wan, Anil Jain, Fingerprint Image Enhancement, "***Algorithm and Performance Evaluation***", IEEE transaction on Pattern Analysis and Machine Intelligence, vol. 20, no. 8, pp.777-789, May 1998.

[21] Recommendation X.800. "***Security architecture for open systems interconnection for CCITT***". ITU, 1991

[22] O'Reilly - ***Network Security with Open SSL***

[23] OpenSSL, http://www.openssl.org

[24] MySQL: http://www.mysql.com

[25] Wikipedia, the free encyclopedia: http://en.wikipedia.org

PHỤ LỤC

PHỤ LỤC A. Hướng dẫn sử dụng

PHỤ LỤC B. Tài liệu kỹ thuật phát triển hệ thống

MỤC LỤC

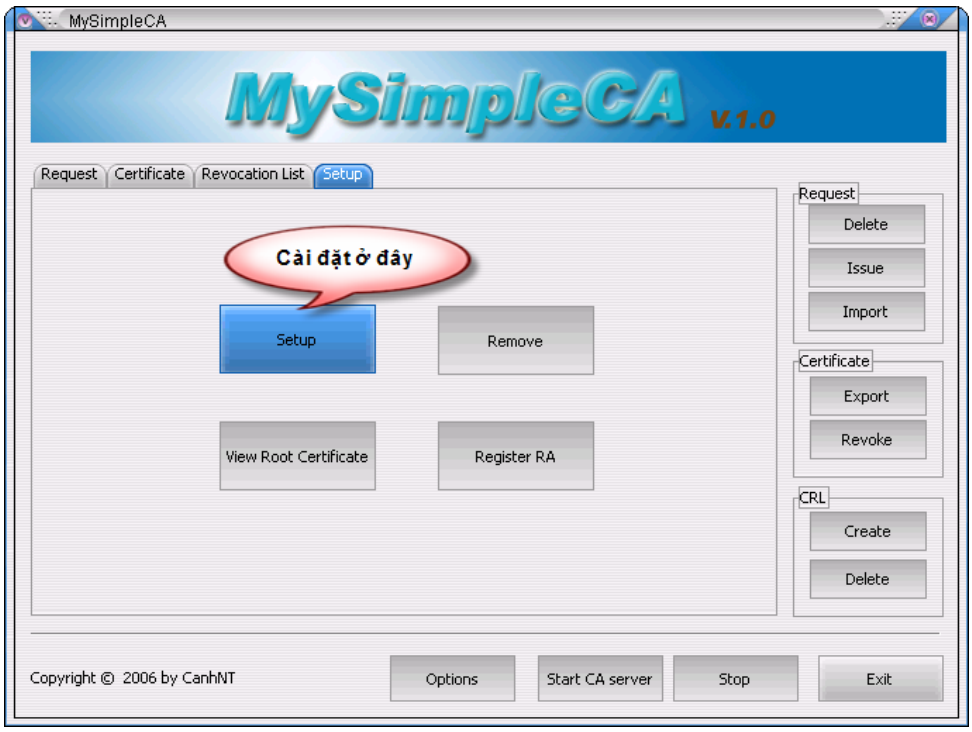
1. CÀI ĐẶT.

1.1. Yêu cầu cấu hình

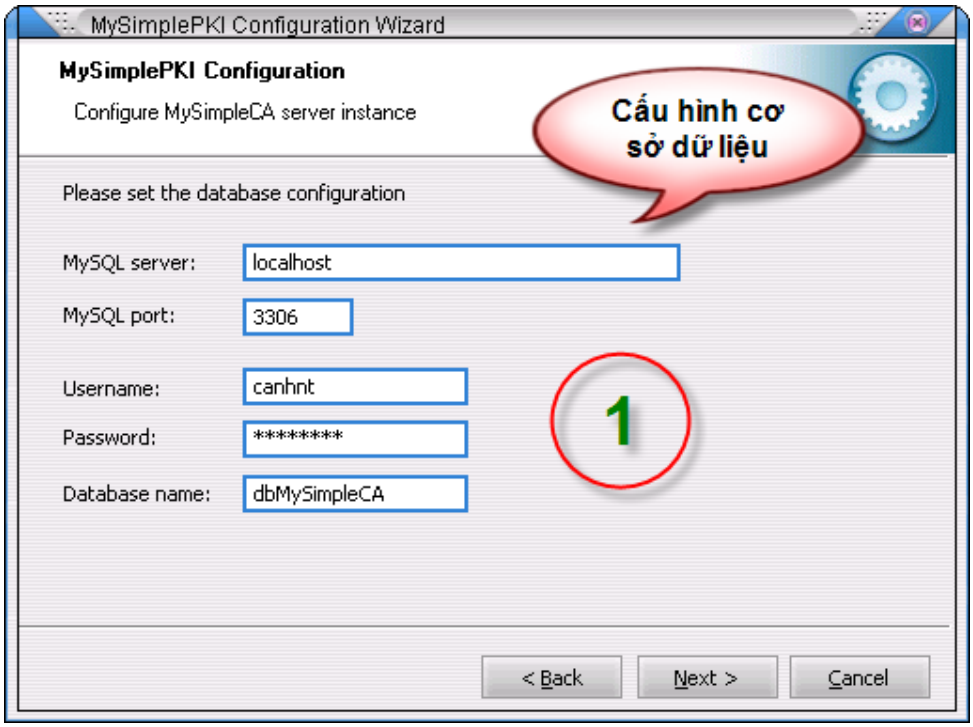
- Microsoft Windows 2000/XP/2003
- MySQL version 5.02 trở lên

1.2. Cài đặt MySimpleCA

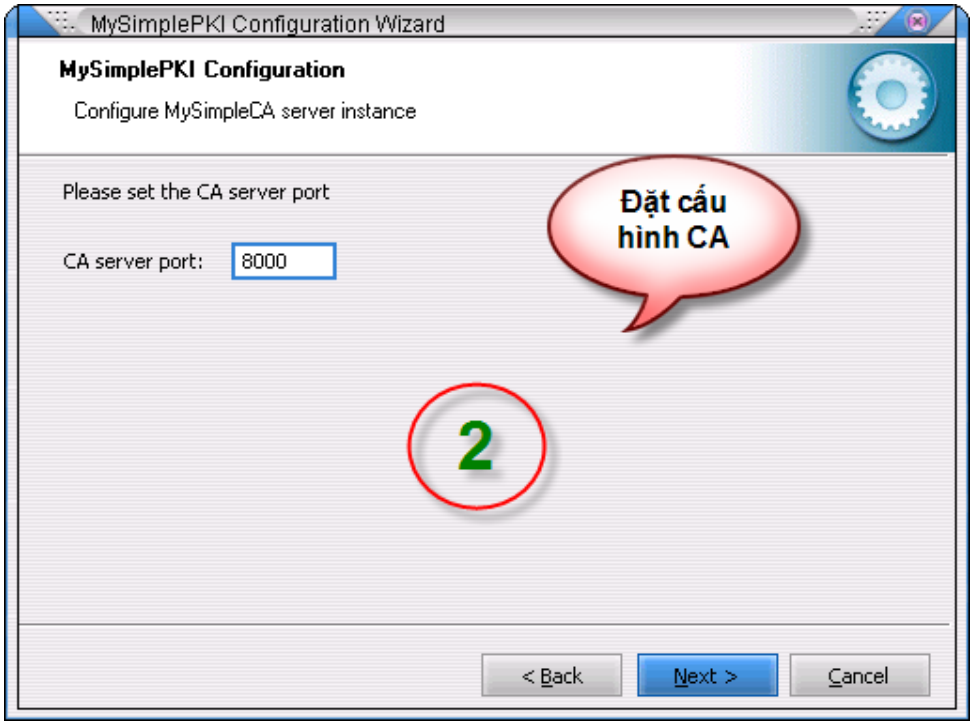
- Khởi động chức năng Setup Wizard của MySimpleCA:



- Tiếp theo, thực hiện các bước trong Setup Wizard
    - Cấu hình cơ sở dữ liệu:
    - MySQL server: địa chỉ máy chủ dịch vụ MySQL
    - MySQL port: cổng dịch vụ MySQL
    - Username: tên tài khoản MySQL
    - Password: mật khẩu cho tài khoản MySQL
    - Databasse name: tên cơ sở dữ liệu sẽ tạo



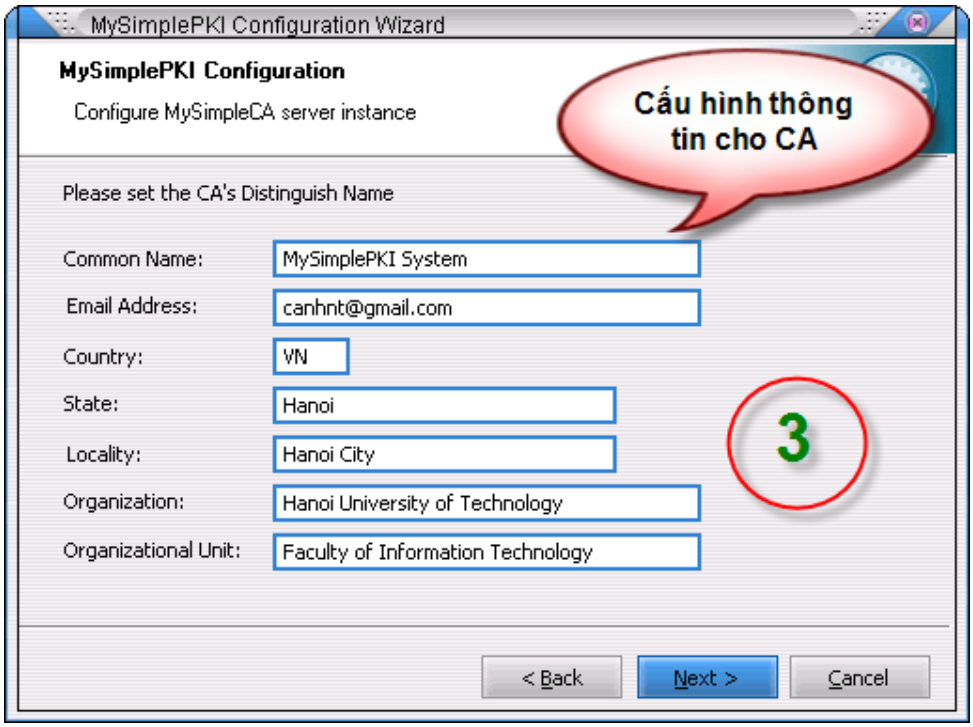
- Cấu hình cổng dịch vụ của CA: đây là cổng mà CA server chờ kết nối từ RA.



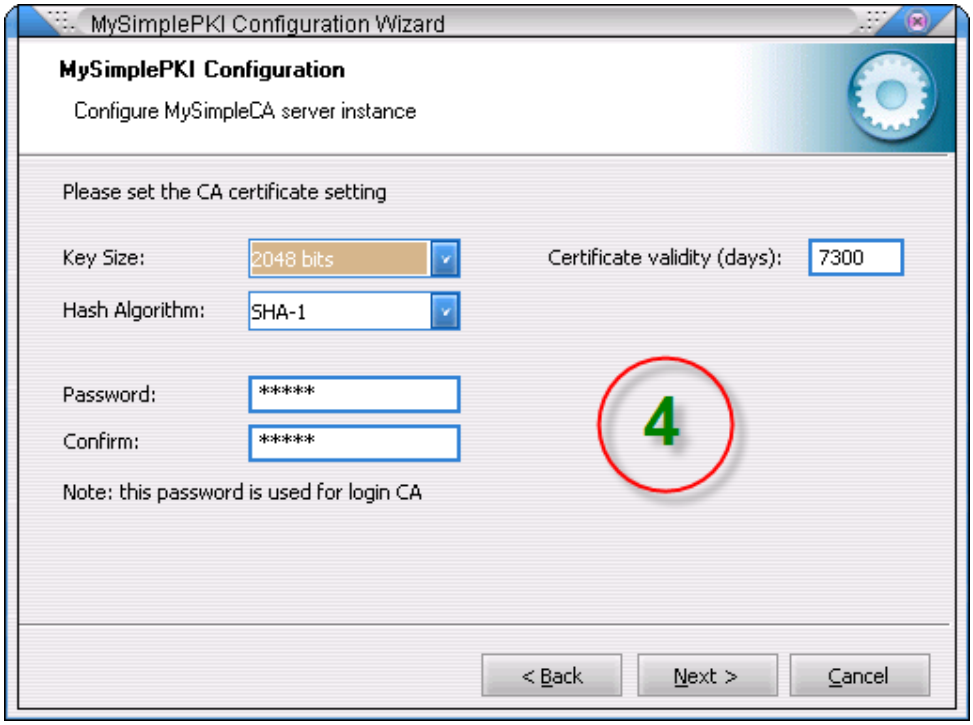
- Đặt các thông tin bên trong chứng nhận số gốc:

- Common Name: tên CA
- Email Address: địa chỉ thư điện tử.
- Country: mã quốc gia, chỉ được 2 ký tự. Ví dụ: VN, JP, US, UK, AU…

- State: tên tỉnh thành, bang.
- Locality: tên địa phương
- Organization: tên tổ chức
- Organizatioal Unit: tên đơn vị trong tổ chức.



- Cấu hình khóa cho chứng nhận số gốc và đặt mật khẩu quản trị

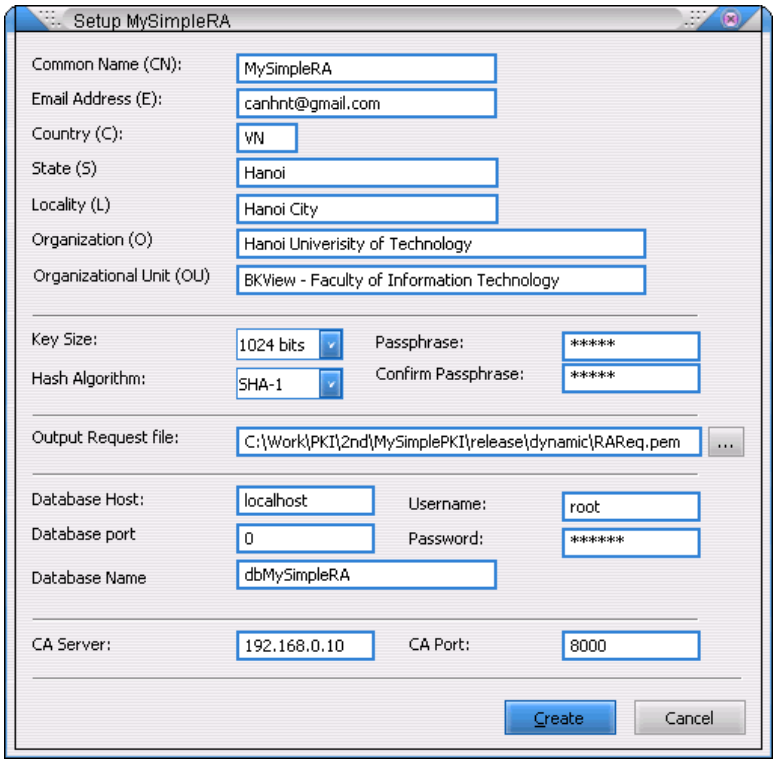


Sau khi hoàn thành các bước cài đặt, cần khởi động lại chương trình.

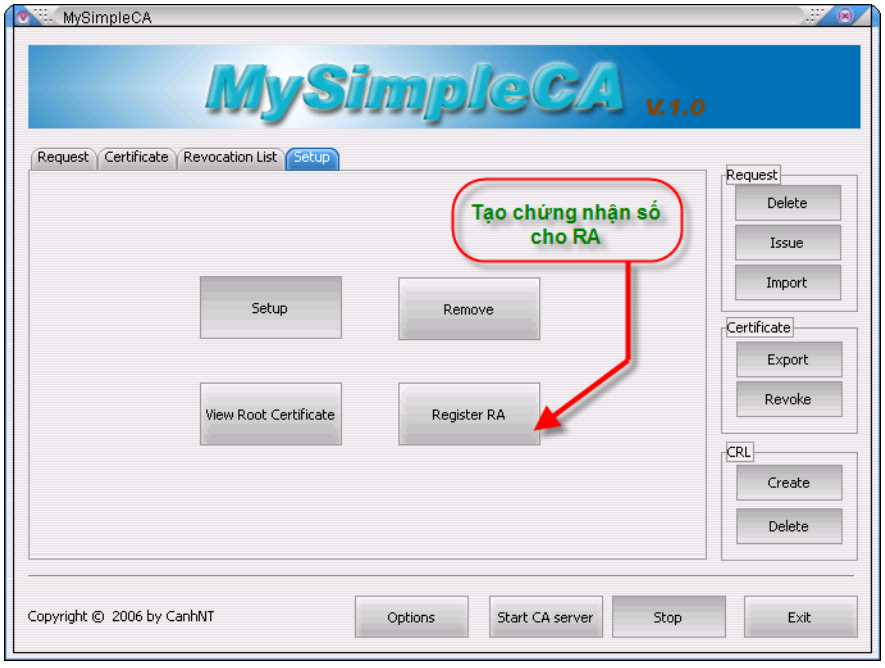
1.3. Cài đặt MySimpleRA

Cài đặt MySimpleRA tiến hành các bước như sau

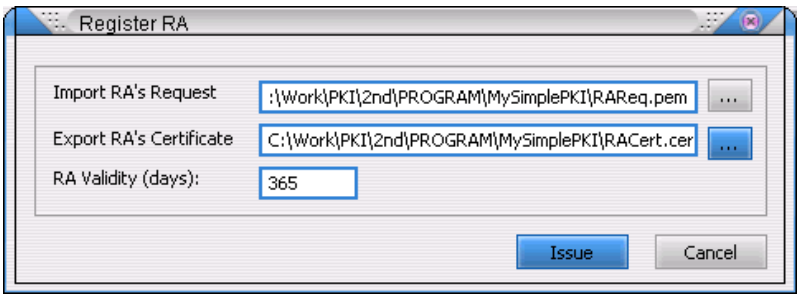
- Cấu hình cho chương trình: thông tin định danh, cặp khóa công khai/cá nhân, cơ sở dữ liệu..



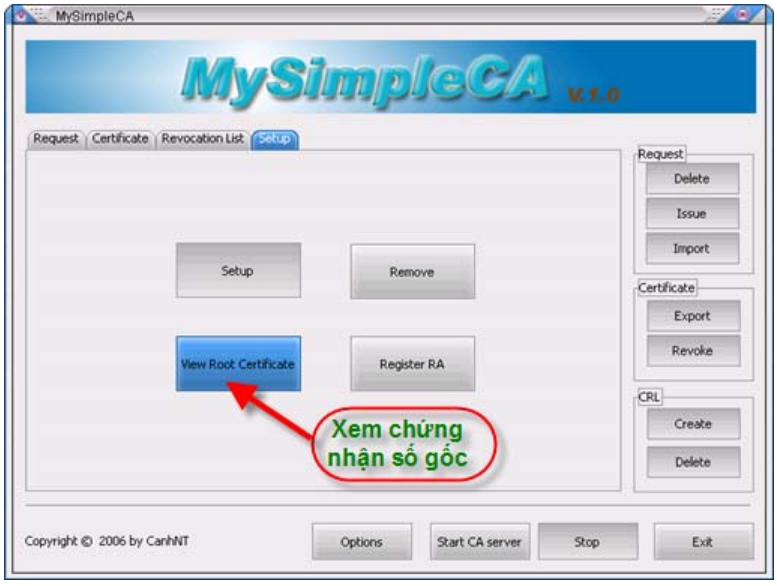
- Đăng ký RA với CA: gửi file request của RA tới CA để CA tạo chứng nhận số tương ứng. Tại CA, tạo chứng nhận số cho RA như sau

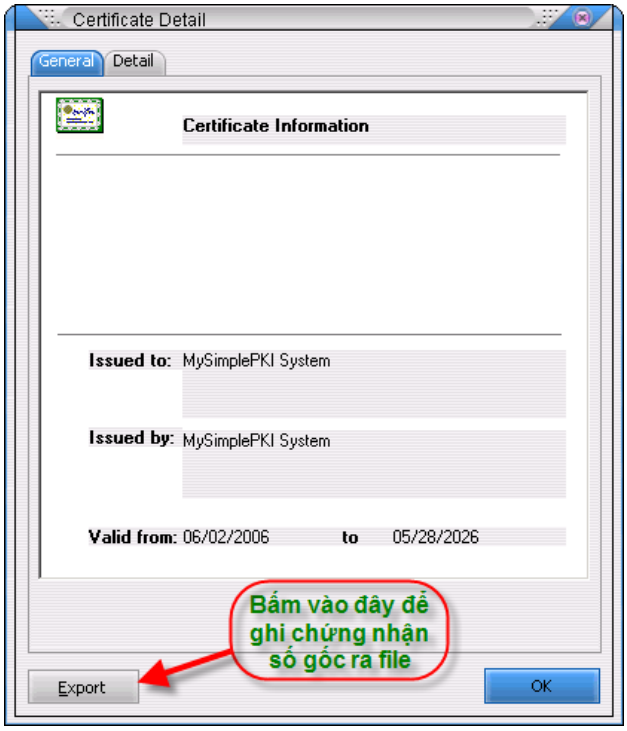


Nhập file đăng ký của RA và ghi kết quả ra file chứng nhận số của RA.

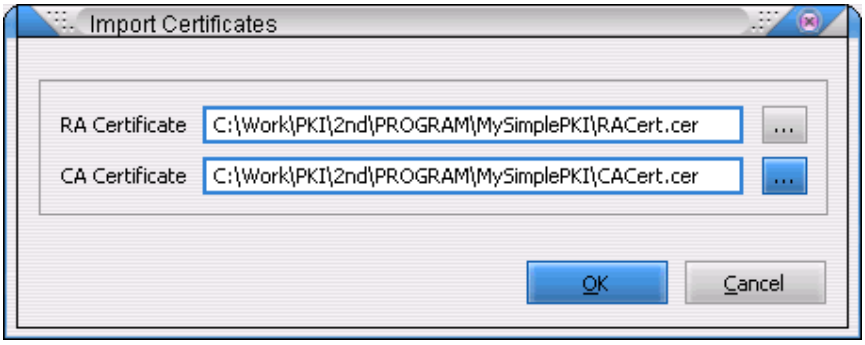


Lấy chứng nhận số gốc của CA để dùng cho cấu hình RA:





Đọc các chứng nhận số của RA và CA từ file để cấu hình cho MySimpleRA:

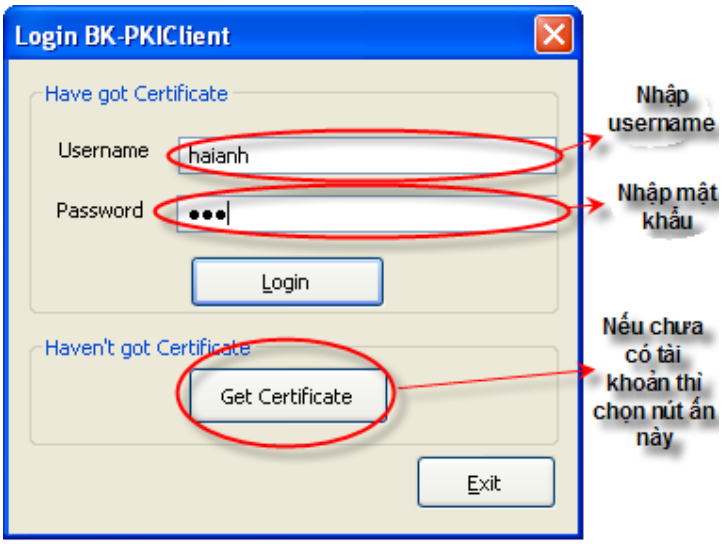


Sau khi nhập các chứng nhận số RA và CA, quá trình cài đặt cho MySimpleRA hoàn tất.

2. ĐĂNG NHẬP:

2.1. Ở RA:

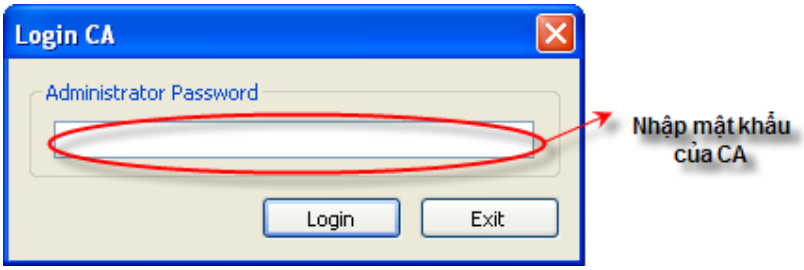
Đầu tiên sẽ có form yêu cầu nhập username và password:



Người dùng sẽ nhập username và mật khẩu, nếu nhập sai liên tiếp 3 lần thì chương trình sẽ tự thoát.

2.2. Ở CA.

Đối với chương trình CA, người dùng chỉ cần nhập mật khẩu của CA (lúc Setup đã chọn, và mặc định là “admin”).

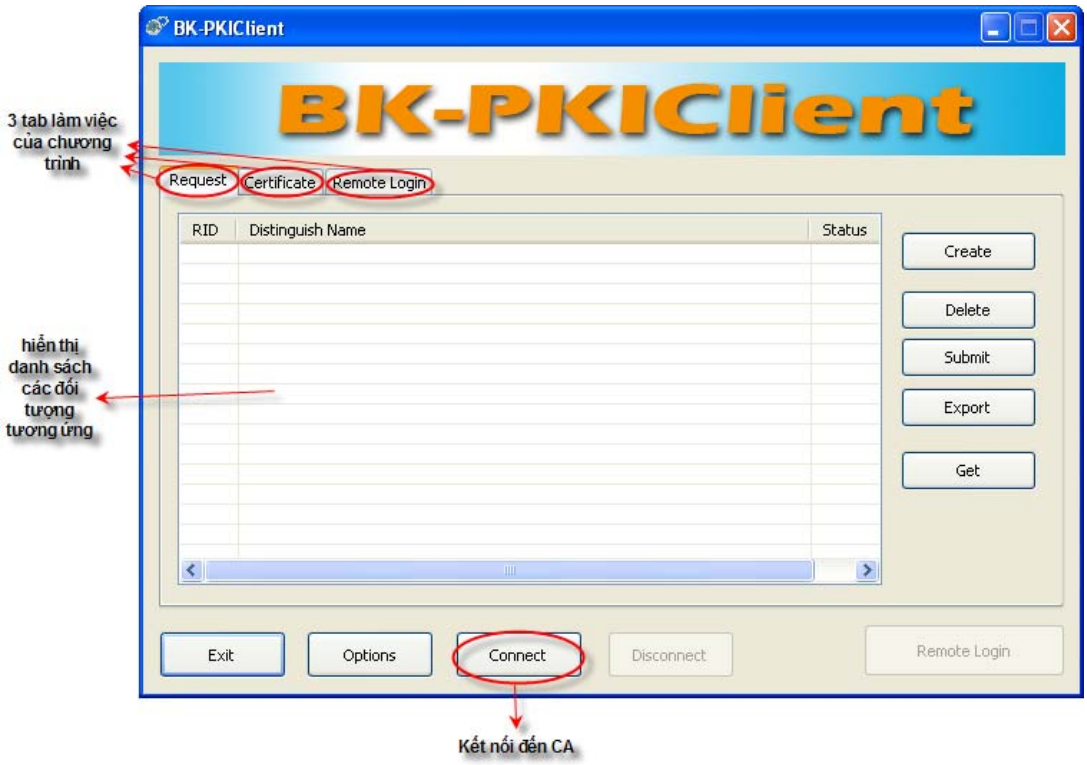


3. SỬ DỤNG CHƯƠNG TRÌNH CHÍNH:

3.1. Chương trình RA:

Giao diện của chương trình được chia ra thành các TAB tương ứng, hiện tại đang có 3 TAB là:

- Request: Dùng để quản lý các yêu cầu của các Client.
- Certificate: Dùng để quản lý các chứng chỉ của Client.
- Remote Login: Dùng để thực hiện ứng dụng truy cập từ xa



Đầu tiên, để kết nối với chương trình CA, người dùng cần phải chọn nút Connect. Sau khi chọn, chương trình sẽ được kết nôi với chương trình CA, nhưng chương trình sẽ báo lỗi nếu chương trình của CA chưa để chế độ "nghe" (chấp nhận các kết nối đến nó).

3.1.1. Làm việc với các yêu cầu.

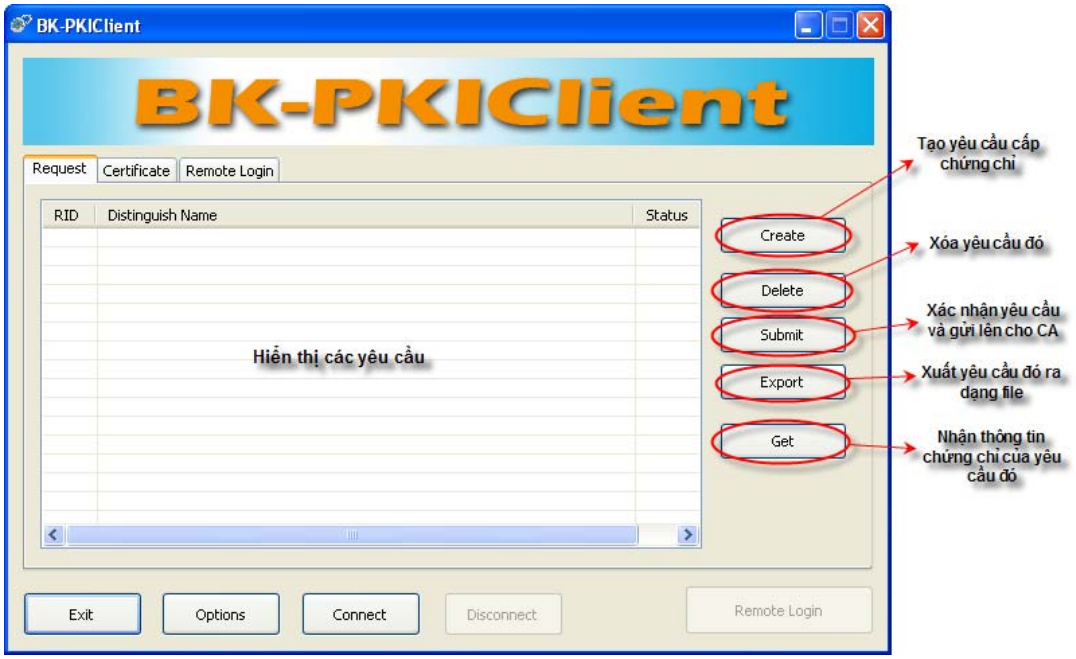
Để làm việc với các Request, người dùng chọn Tab Request.

Các chức năng ứng với Tab Request người dùng có thể chọn là:

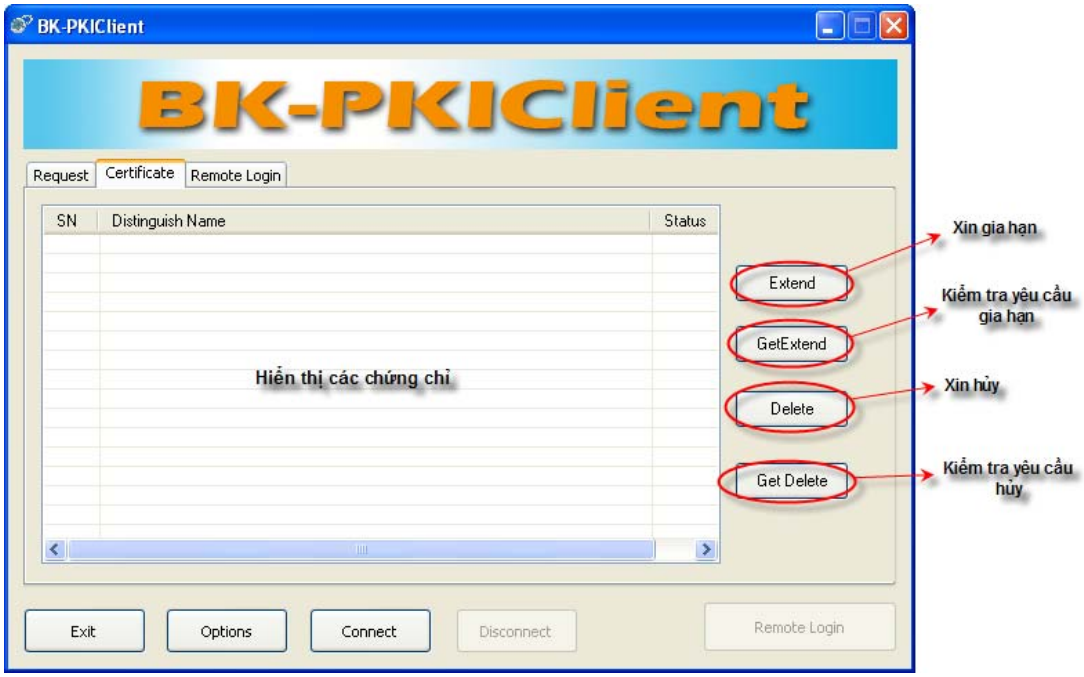
- Tạo yêu cầu chứng chỉ: Khi chưa có chứng chỉ hoặc muốn tạo thêm chứng chỉ người dùng chọn chức năng này. Khi đó chương trình sẽ hiển thị ra các cửa sổ để yêu cầu người dùng nhập thông tin, hoàn tất quá trình tạo yêu cầu cấp chứng chỉ.
- Xóa yêu cầu: Nếu phát hiện ra yêu cầu vừa tạo chưa chính xác, người dùng có thể chọn chức năng này để hủy yêu cầu đó.

- Xác nhận yêu cầu và gửi lên cho CA: Sau khi đã chắc chắn về tính đúng đắn của yêu cầu, người dùng chọn chức năng này để chương trình RA gửi yêu cầu lên cho CA.
- Xuất yêu cầu ra file: Dùng để xuất 1 yêu cầu ra file.
- Nhận thông tin chứng chỉ: Người dùng sẽ chọn chức năng này để kiểm tra xem yêu cầu vừa gửi lên đã được CA đồng ý chưa, nếu đã được chấp nhận thì lập tức người dùng sẽ có được chứng chỉ ứng với yêu cầu đó.

Giao diện của chương trình ứng với TAB Request:



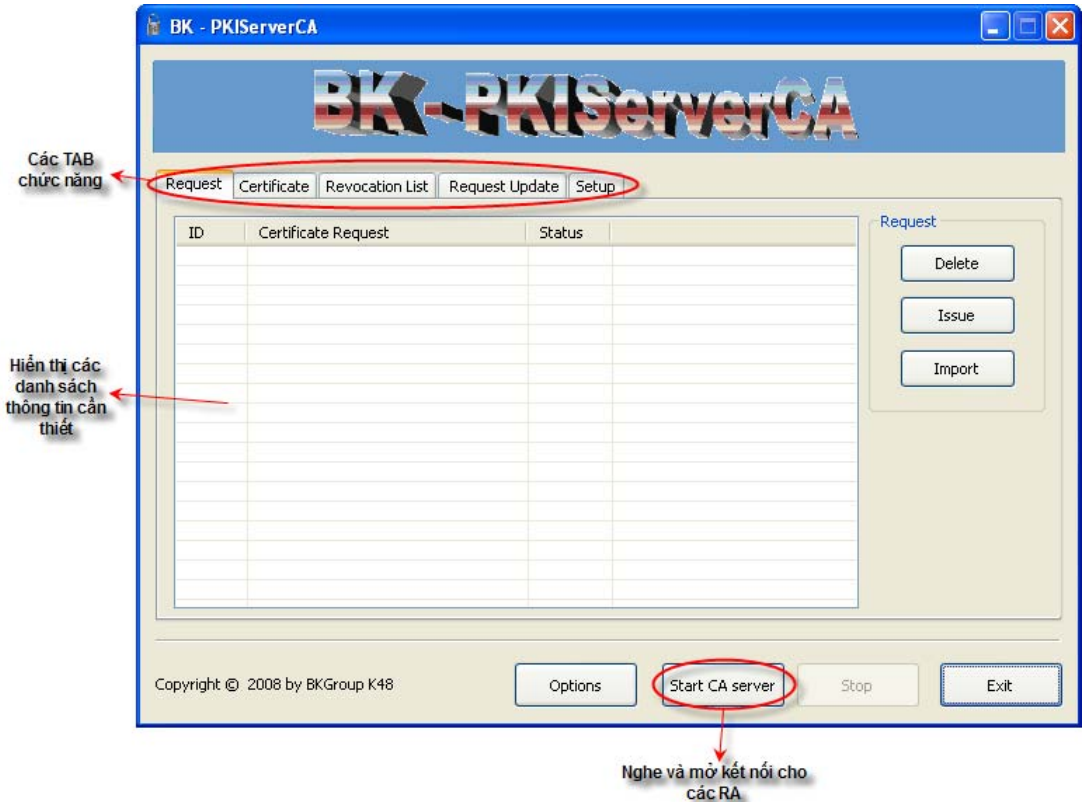
3.1.2. Làm việc với các chứng chỉ:



Các chức năng ứng với TAB Certificate người dùng có thể chọn là:

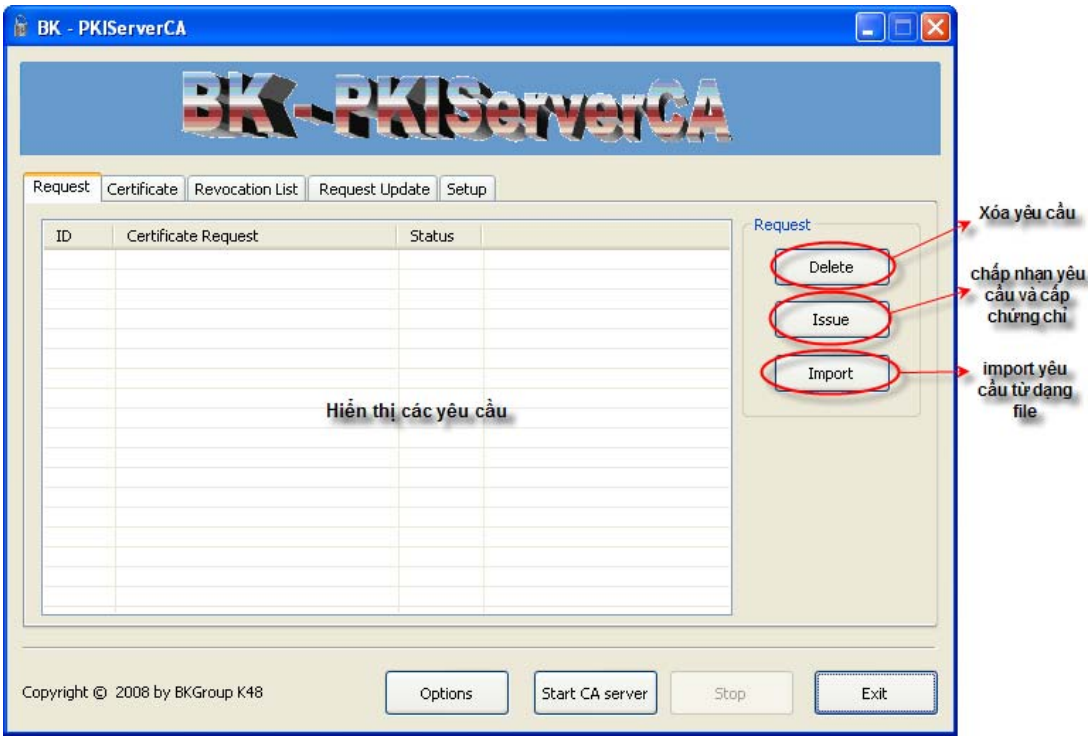
- Xin gia hạn: Sau khi thấy chứng chỉ của mình sử dụng sắp hết hạn, người dùng có thể gửi yêu cầu xin gia hạn lên cho CA.
- Kiểm tra yêu cầu gia hạn: Sau khi xin gia hạn, người dùng phải dùng chức năng này để kiểm tra xem đã được CA đồng ý chưa. Nếu đã được đồng ý thì chứng chỉ đó đã được gia hạn thêm 1 thời gian (mặc định của phiên bản hiện thời là 1 năm).
- Xin hủy: Nếu muốn hủy chứng chỉ, người dùng chọn chức năng này để gửi yêu cầu xin hủy lên cho CA.
- Kiểm tra yêu cầu hủy: Tương tự, sau khi xin hủy, người dùng phải dùng chức năng này để kiểm tra xem đã được CA đồng ý chưa.

3.2. Chương trình CA:



Tương tự giao diện của chương trình RA, chương trình CA cũng làm việc với các TAB chức năng. Ban đầu, phải ấn nút Start CA Server để nghe và cho phép các RA kết nối đến. Chúng ta sẽ lần lượt tìm hiểu các chức năng cụ thể của chương trình:

3.2.1. Làm việc với các Request.



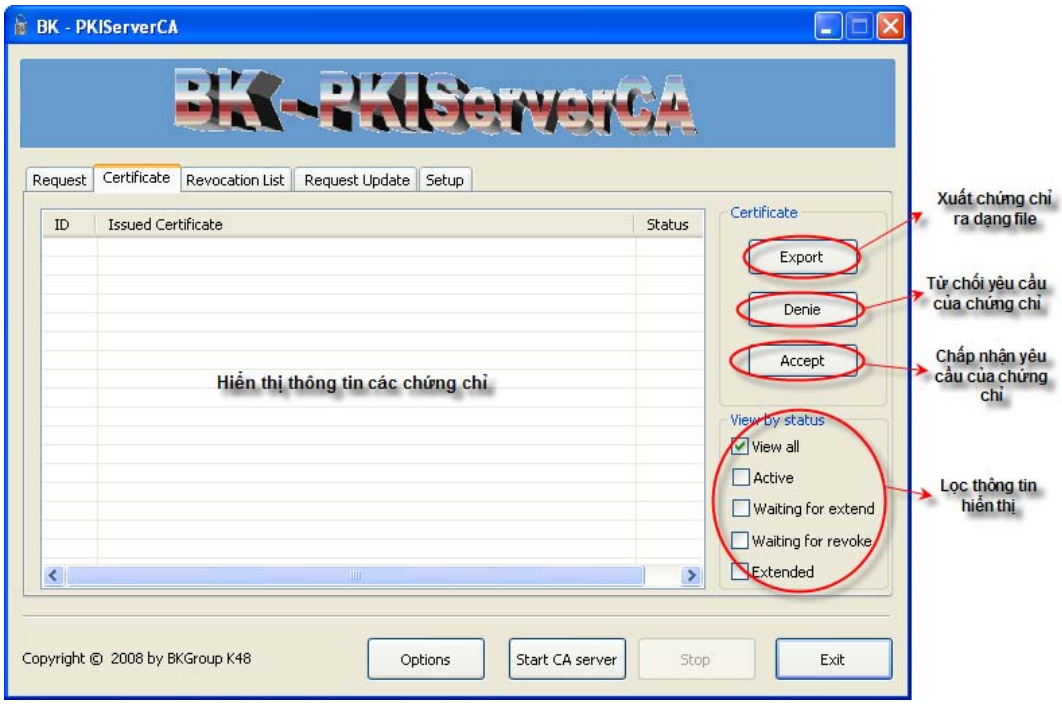
Các chức năng ứng với TAB Request:

- Xóa yêu cầu: Khi không chấp nhận yêu cầu đó, CA sẽ dùng chức năng này để xóa yêu cầu đó đi.
- Chấp nhận yêu cầu và cấp chứng chỉ: CA sử dụng chức năng này khi chấp nhận yêu cầu xin cấp chứng chỉ đó.
- Import yêu cầu từ dạng file: Sẽ đưa yêu cầu vào bằng dạng file.

3.2.2. Làm việc với TAB Certificate:

Các chức năng mà người dùng có thể thực hiện ứng với TAB Certificate :

- Xuất chứng chỉ ra dạng file.
- Từ chối yêu cầu của chứng chỉ: Các yêu cầu có dạng như xin gia hạn hoặc xin hủy, nếu từ chối các yêu cầu đó, CA sẽ chọn chức năng này.
- Chấp nhận yêu cầu của chứng chỉ: Tương tự, chấp nhận các yêu cầu đó, CA chọn chức năng này.
- Lọc thông tin hiển thị: Khi có quá nhiều thông tin được hiển thị ra, để tránh rối mắt, người dùng có thể dùng bộ lọc và chỉ cho hiển thị ra các kiểu chứng chỉ mà mình muốn làm việc với.


BK - PKIServerCA
BK - PKIServerCA
Request
Certificate
Revocation List
Request Update
Setup
ID
Issued Certificate
Status
Hiển thị thông tin các chứng chỉ
Certificate
Export
Denie
Accept
View by status
View all
Active
Waiting for extend
Waiting for revoke
Extended
Copyright © 2008 by BKGroup K48
Options
Start CA server
Stop
Exit
Xuất chứng chỉ ra dạng file
Từ chối yêu cầu của chứng chỉ
Chấp nhận yêu cầu của chứng chỉ
Lọc thông tin hiển thị

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ, BIỂU ĐỒ

1. GIỚI THIỆU

1.1 Mục đích

Đây là tài liệu thiết kế của hệ thống BK-BioPKI. Tài liệu dùng chủ yếu cho các thành viên tham gia phát triển hệ thống

1.2 Phạm vi

Tài liệu này nói tới hệ thống BK-BioPKI. Đây là hệ thống được phát triển để thử nghiệm sử dụng đặc điểm sinh trắc vào bảo mật, xác thực trong hệ PKI. Nó là một hệ PKI xây dựng theo kiến trúc CA đơn, đồng thời đã được tích hợp sinh trắc học vân tay vào. Hệ thống cho phép người dùng đăng kí vào hệ thống, xin cấp chứng chỉ có xác nhận của CA và sử dụng chứng chỉ trong các giao dịch nhất định

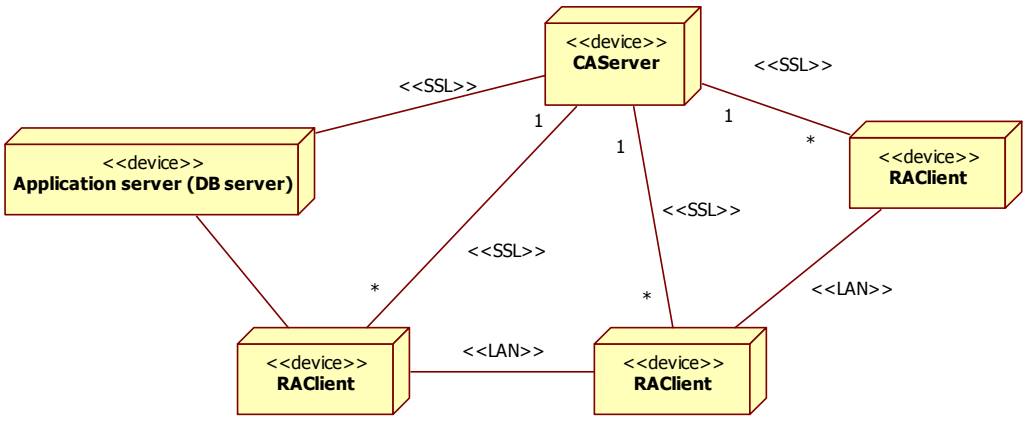
1.3 Từ viết tắt

PTN: phòng thí nghiệm.
PKI: Public Key Infrastructure.
RA: Registration Authority.
CA: Certification Authority.
CRL: Certificate Revocation List.

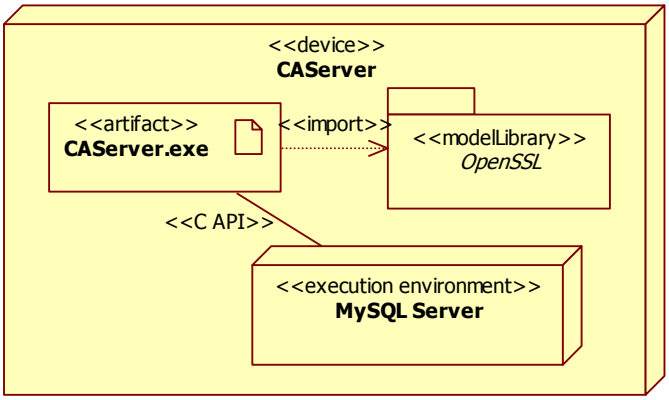
1.4 Tham khảo

[1].**http://www.staruml.com**
[2]. **www.openssl.org**.
[3]. Grady Booch, James Rumbaugh, Ivar Jacobson. "*The Unified Modeling Language User Guide SECOND EDITION*". Prentice Hall, November 16, 2005.

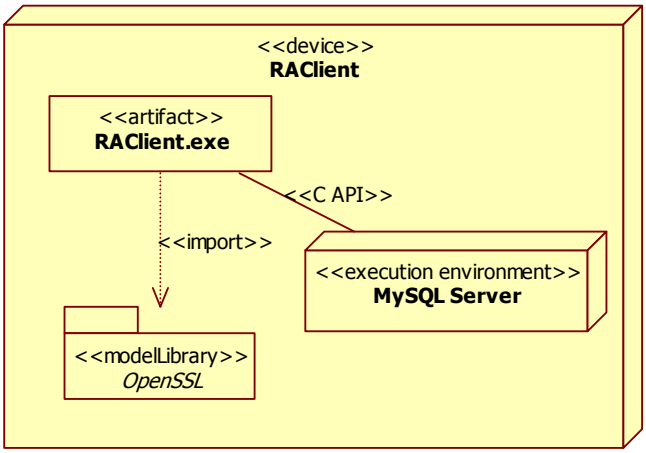
2. BIỂU ĐỒ TRIỂN KHAI



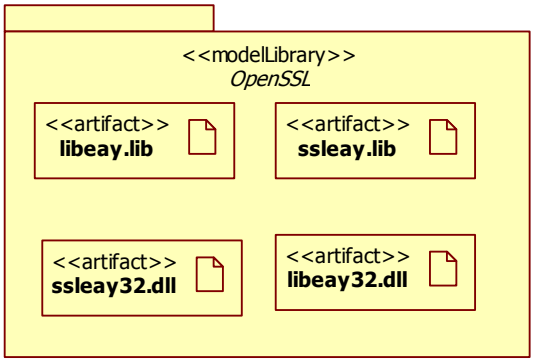
Hình 2-1 Biểu đồ triển khai của hệ thống BK-BioPKI



Hình 2-2 CAServer



Hình 2-3 RAClient



Hình 2-4 Các file lib, dll cần dùng của OpenSSL

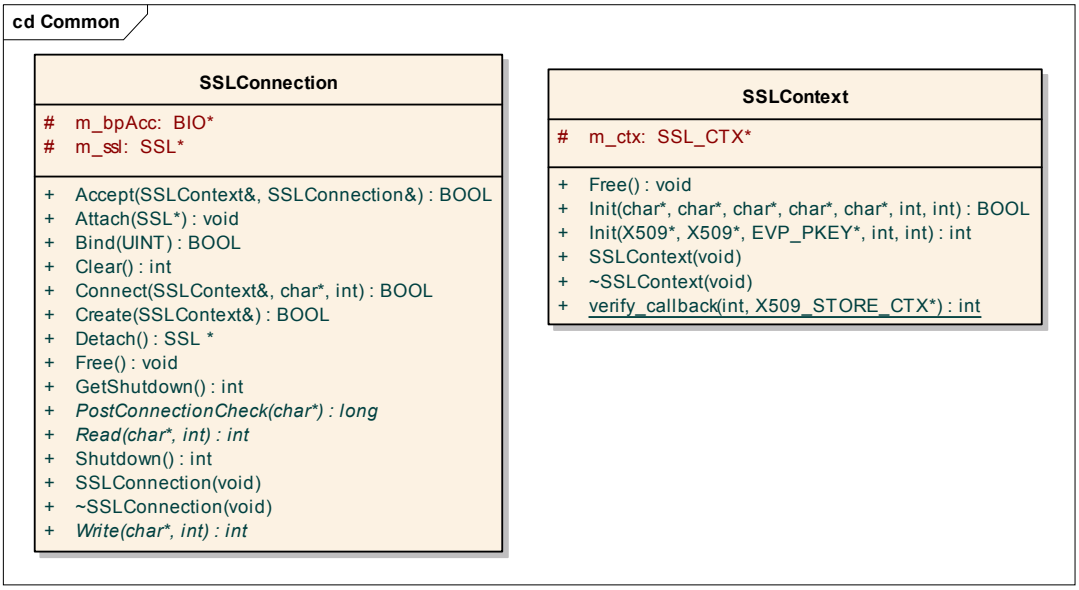
3. BIỀU ĐỒ LỚP

3.1. Các lớp xây dựng từ thư viện OpenSSL

Đây là một số lớp được xây dựng từ thư viện OpenSSL sử dụng các hàm API theo ngôn ngữ C dùng cho mã hóa, giao thức SSL và X.509. Các lớp được xây dựng bao gồm:

- *SSLConnection:* dùng cho kết nối SSL.
- *SSLContext:* dùng cho cấu hình kết nối SSL.
- *X509NameEntry:* biểu diễn một thành phần trong đinh danh.
- *X509Name:* biểu diễn định danh của thực thể trong PKI.
- *X509Request:* biểu diễn một yêu cầu chứng nhận số.
- *X509Extension:* biểu diễn một thành phần mở rộng của chứng nhận số theo chuẩn X.509.
- *X509ExtensionList:* biểu diễn danh sách các thành phần mở rộng.
- *X509Revoked:* biểu diễn một chứng nhận số bị hủy trong CRL
- *X509RevokedList:* biểu diễn tập các chứng nhận số bị hủy.
- *X509CRL:* biểu diễn CRL
- *X509Time:* biểu diễn đối tượng thời gian theo chuẩn ASN.1 dùng trong chứng nhận số X.509.
- *X509Certificate:* biểu diễn chứng nhận số X.509.
- *EVPHash:* dùng cho tạo chuỗi băm.
- *EVP_PKey:* dùng để quản lý cặp khóa cá nhân/công khai.
- *CnameProfile*
- *SimplePKICert*
- *X509CRLInfo*

3.1.1. Các lớp liên quan đến giao thức bảo mật SSL



Hình 3-1 Các lớp liên quan đến giao thức bảo mật SSL

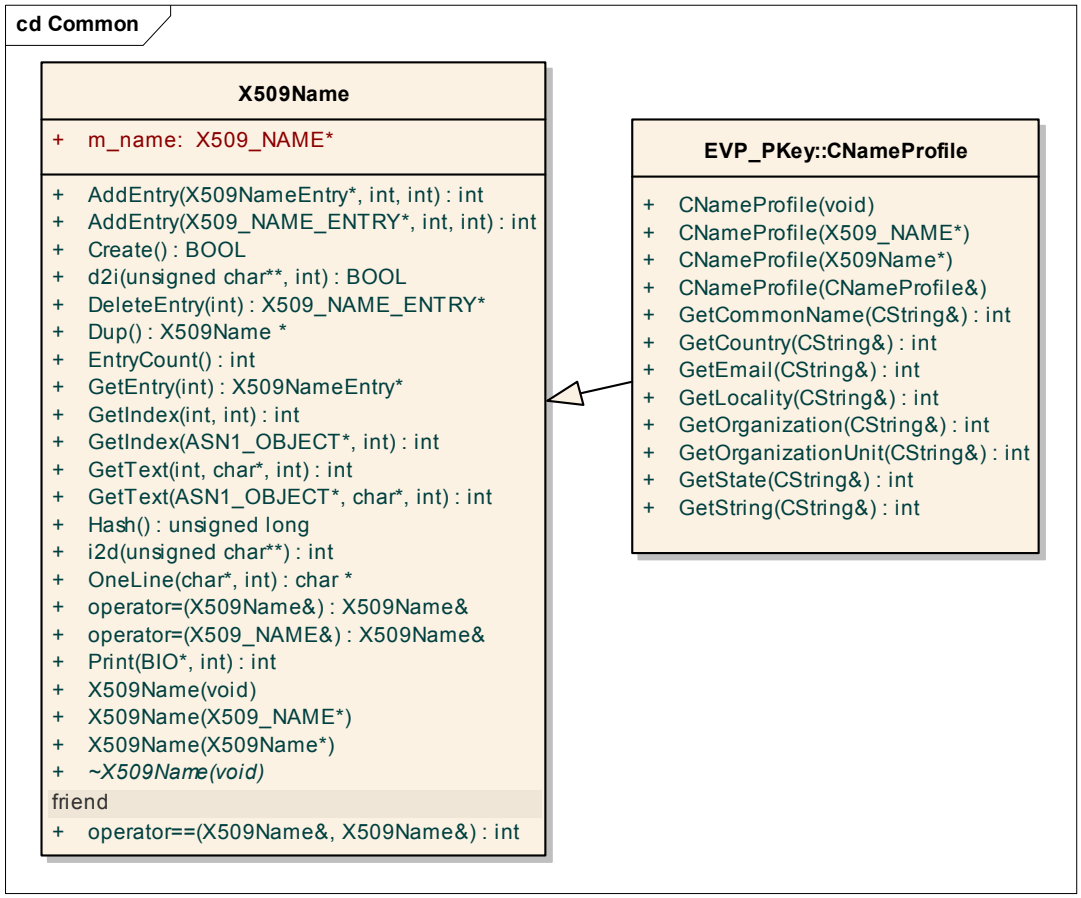
3.1.2. Lớp về chứng chỉ số X509

Hình 3-2 Lớp chứng chỉ của CA

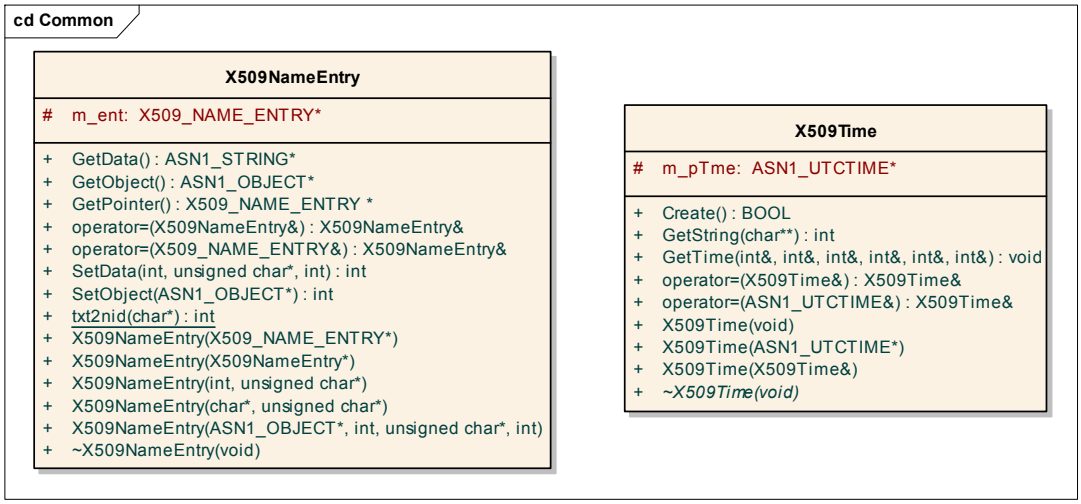
3.1.3. Các lớp quản lý mã hóa và băm

Hình 3-3. Quản lý mã hóa và băm

3.1.4. Các lớp biểu diễn các thành phần trong chứng chỉ số X509

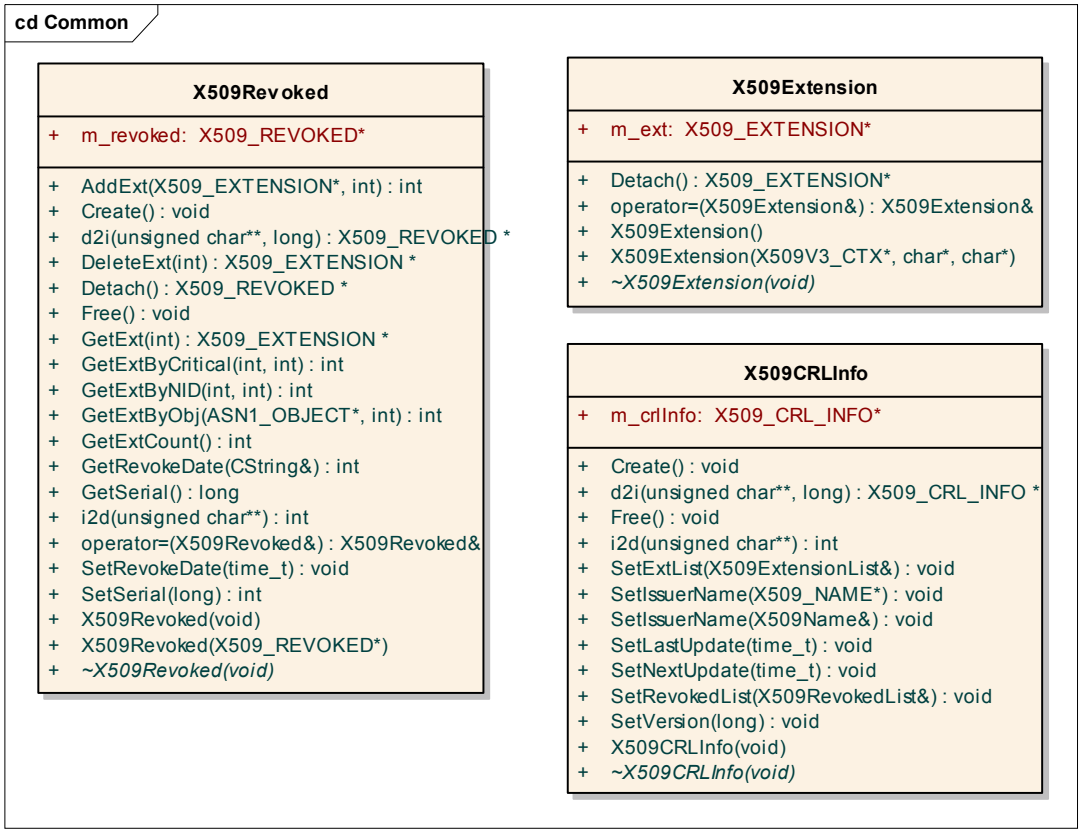


Hình 3-4 X509Name và CNameProfile



Hình 3-5 X509NameEntry và X509Time

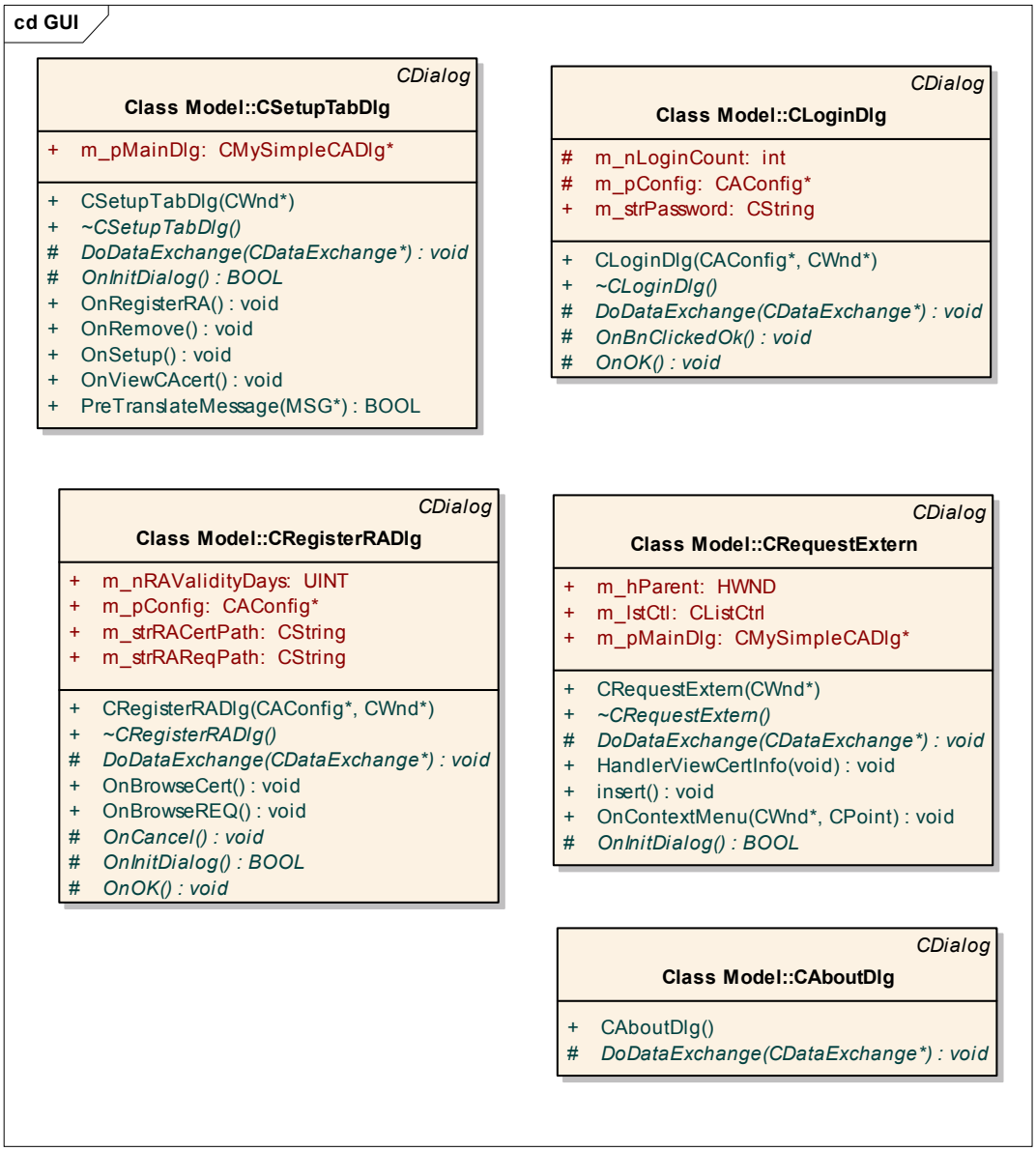
3.1.5. Các lớp quản lý việc hủy bỏ hay gia hạn chứng chỉ số X509



Hình 3-6 Quản lý hủy bỏ hay gia hạn

3.2. Thiết kế các lớp liên quan tới CAServer

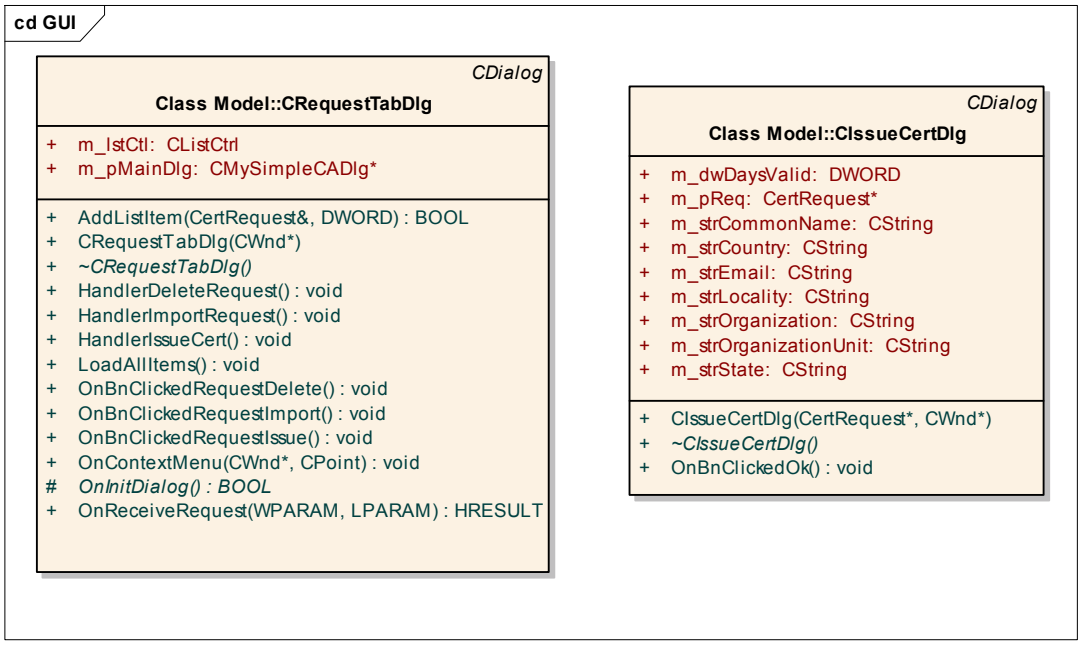
3.2.1. Các lớp giao diện của chức năng setup hệ thống và đăng ký, đăng nhập sử dụng hệ thống



Hình 3-7. Các lớp giao diện chức năng setup hệ thống

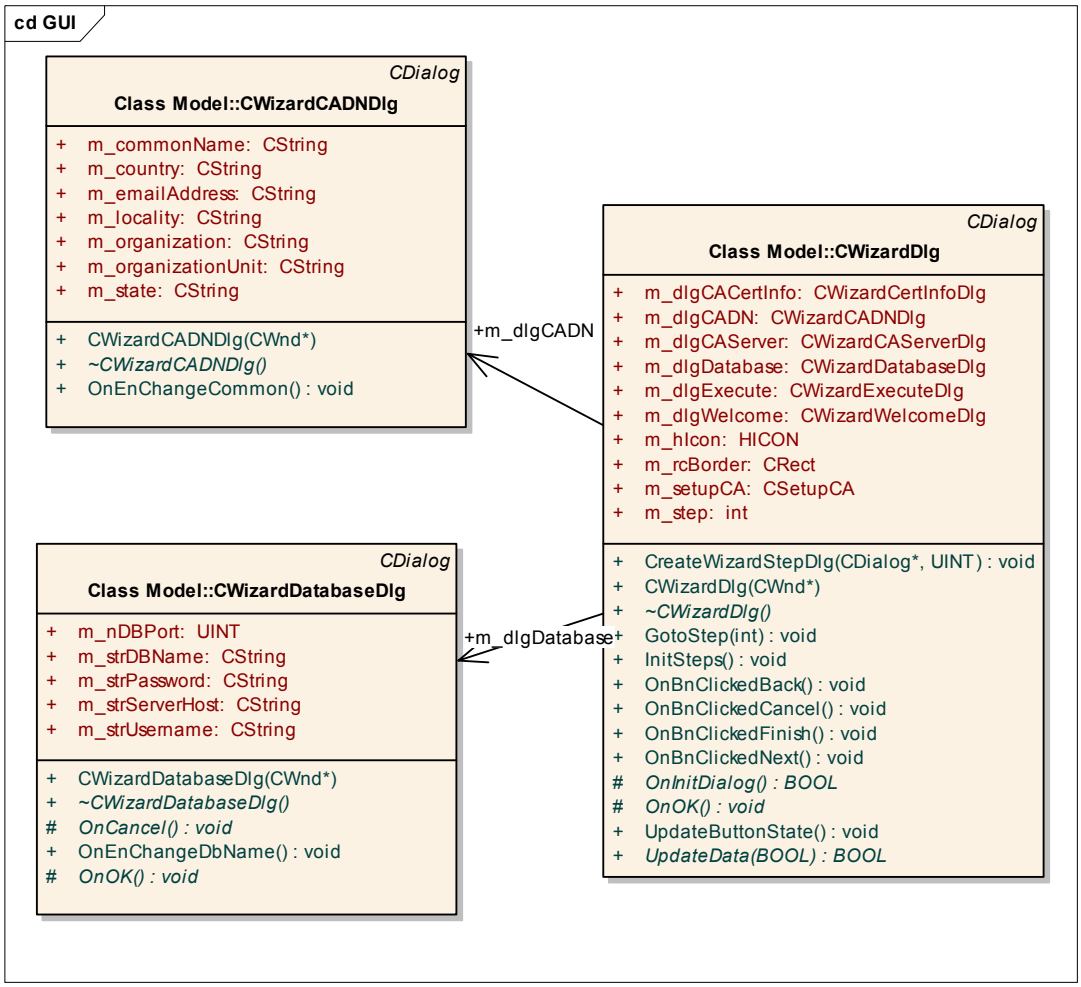
3.2.2. Các lớp giao diện của các tab chức năng liên quan đến quản lý chứng chỉ

Hình 3-8 Lớp CcertTabDlg và CCRLTabDlg

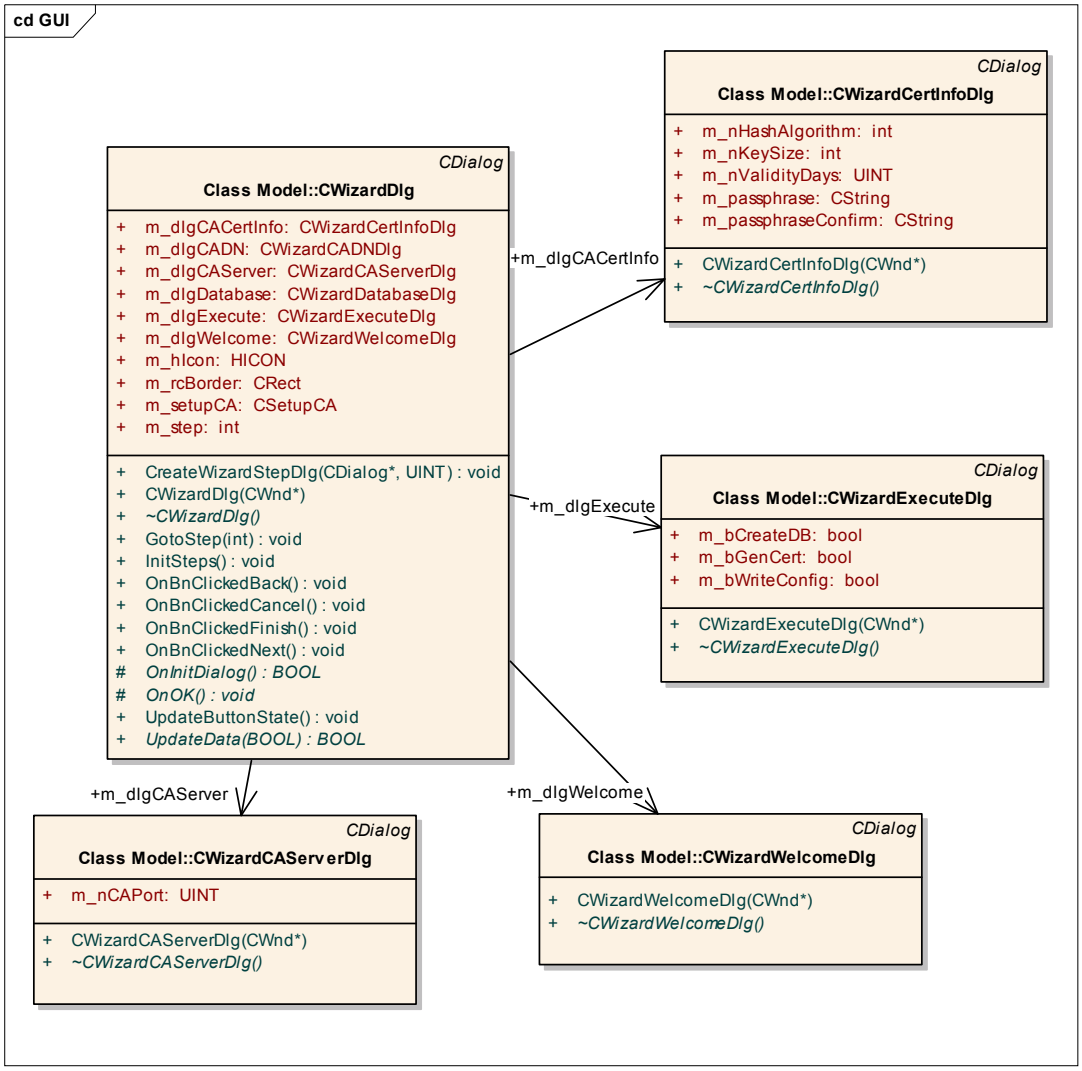


Hình 3-9 Lớp CrequestTabDlg và CIssueCertDlg

3.2.3. Giao diện cửa sổ các chức năng để thiết lập cấu hình hệ thống khi tiến hành cài đặt ban đầu cho hệ thống

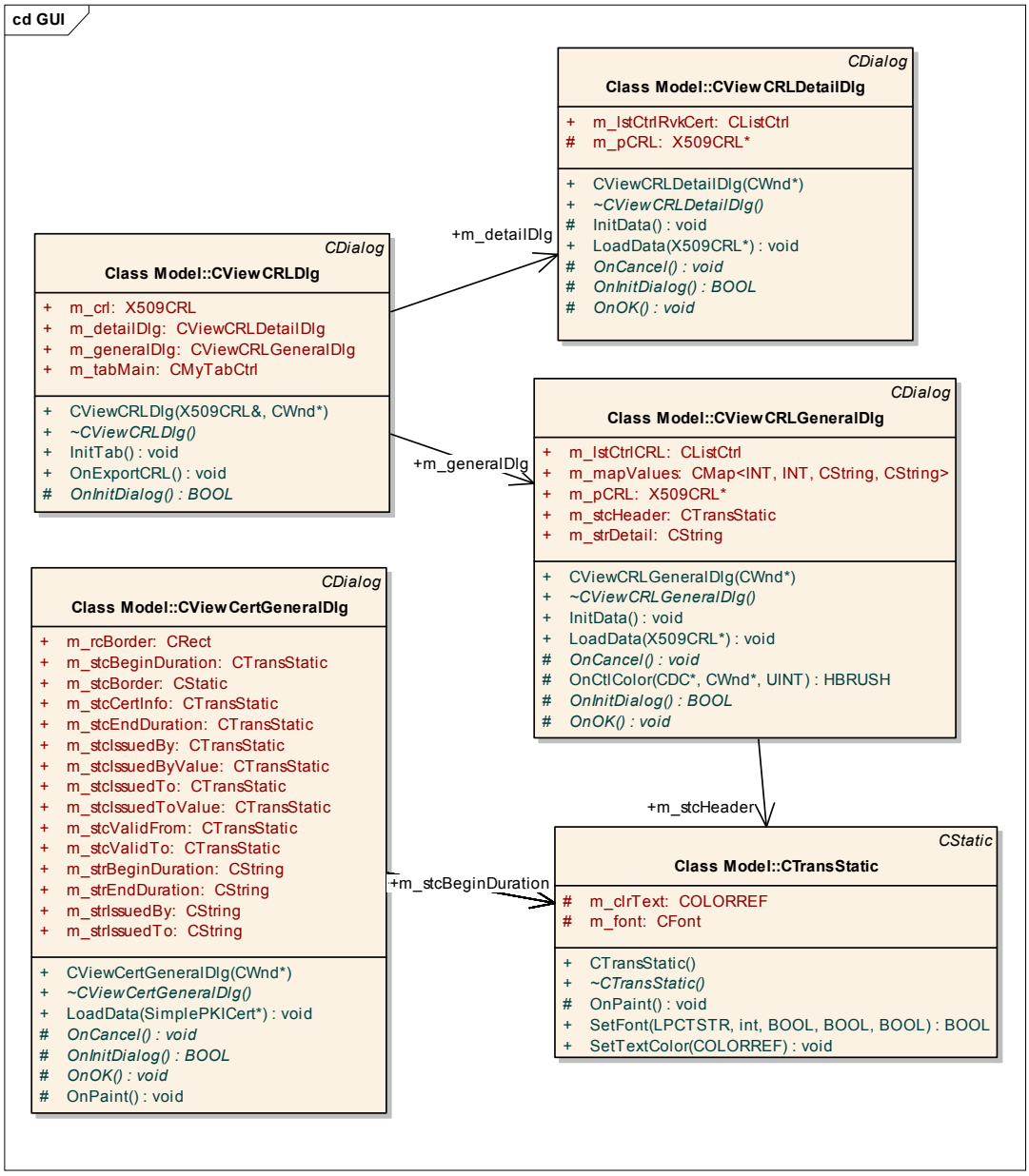


Hình 3-10 Các lớp giao diện cửa sổ các chức năng thiết lập cấu hình hệ thống (1)

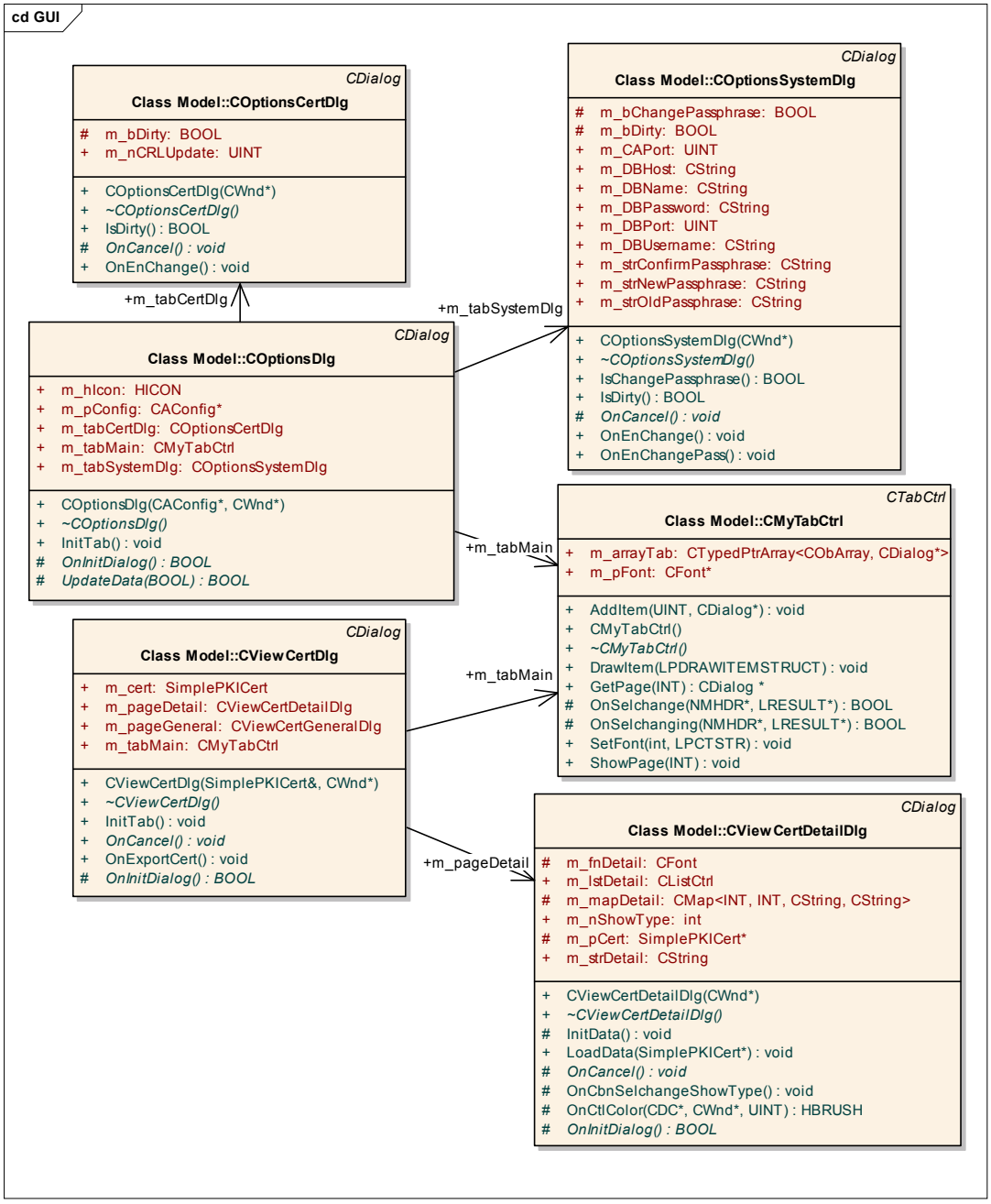


Hình 3-11 Các lớp giao diện cửa sổ các chức năng thiết lập cấu hình hệ thống (2)

3.2.4. Giao diện màn hình hiển thị thông tin chi tiết về chứng chỉ, thông tin chung về danh sách chứng chỉ bị thu hồi



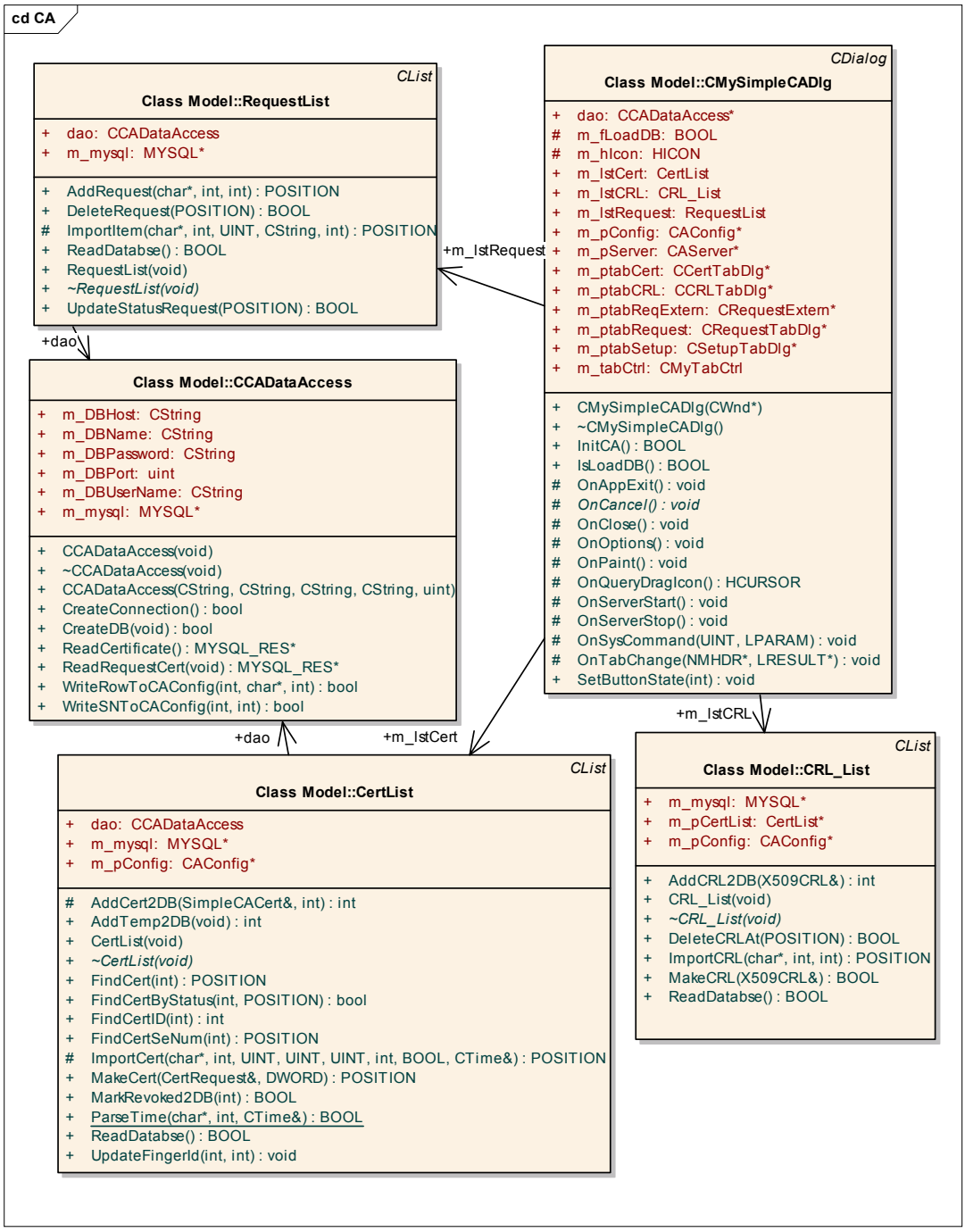
Hình 3-12 Các lớp giao diện hiển thị thông tin chi tiết chứng chỉ (1)



Hình 3-13 Các lớp giao diện hiển thị thông tin chi tiết chứng chỉ (2)

3.2.5. Các lớp kế thừa từ lớp CList

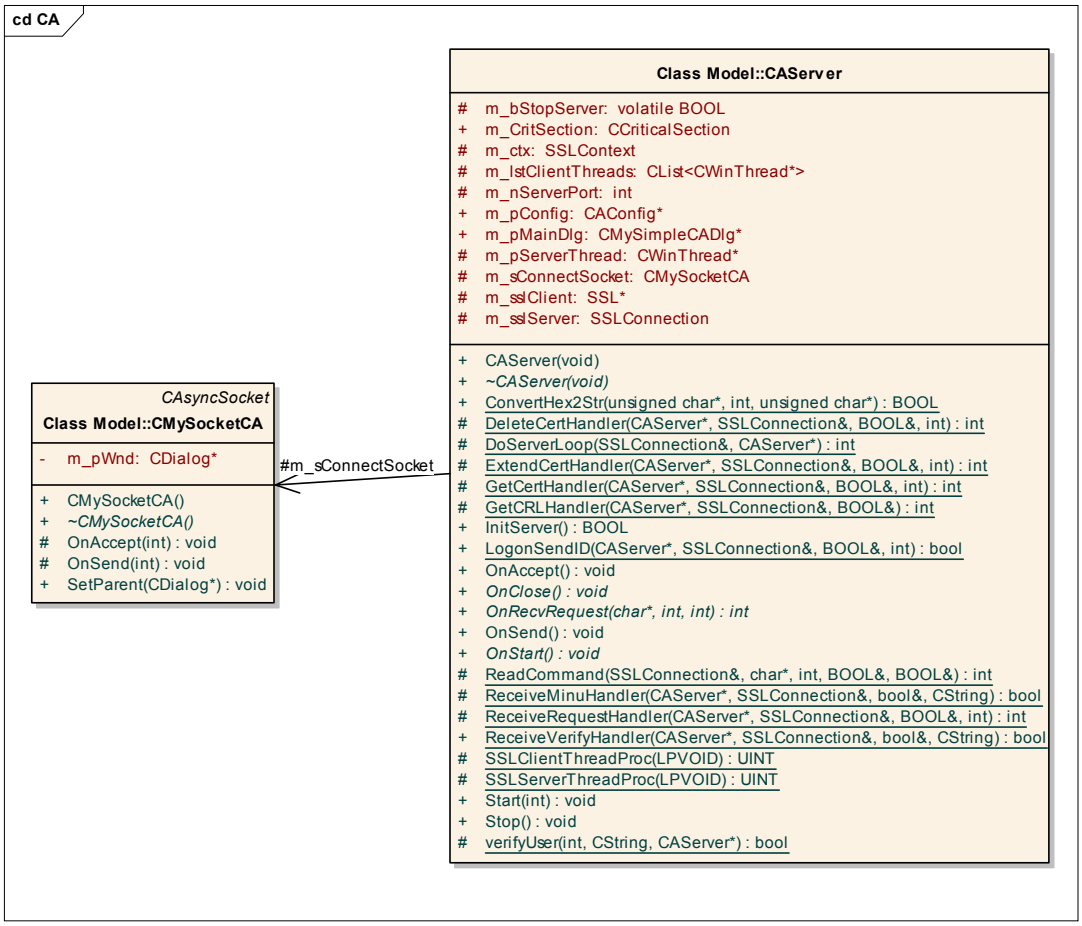
Các lớp này để hiển thị danh sách các yêu cầu,danh sách các chứng chỉ có trong cơ sở dữ liệu, danh sách các chứng chỉ đã bị hủy.Việc truy cập vào cơ sở dữ liệu được thực hiện thông qua lớp CADataAccess



Hình 3-14 Các lớp kế thừa để hiện thị danh sách yêu cầu, chứng chỉ

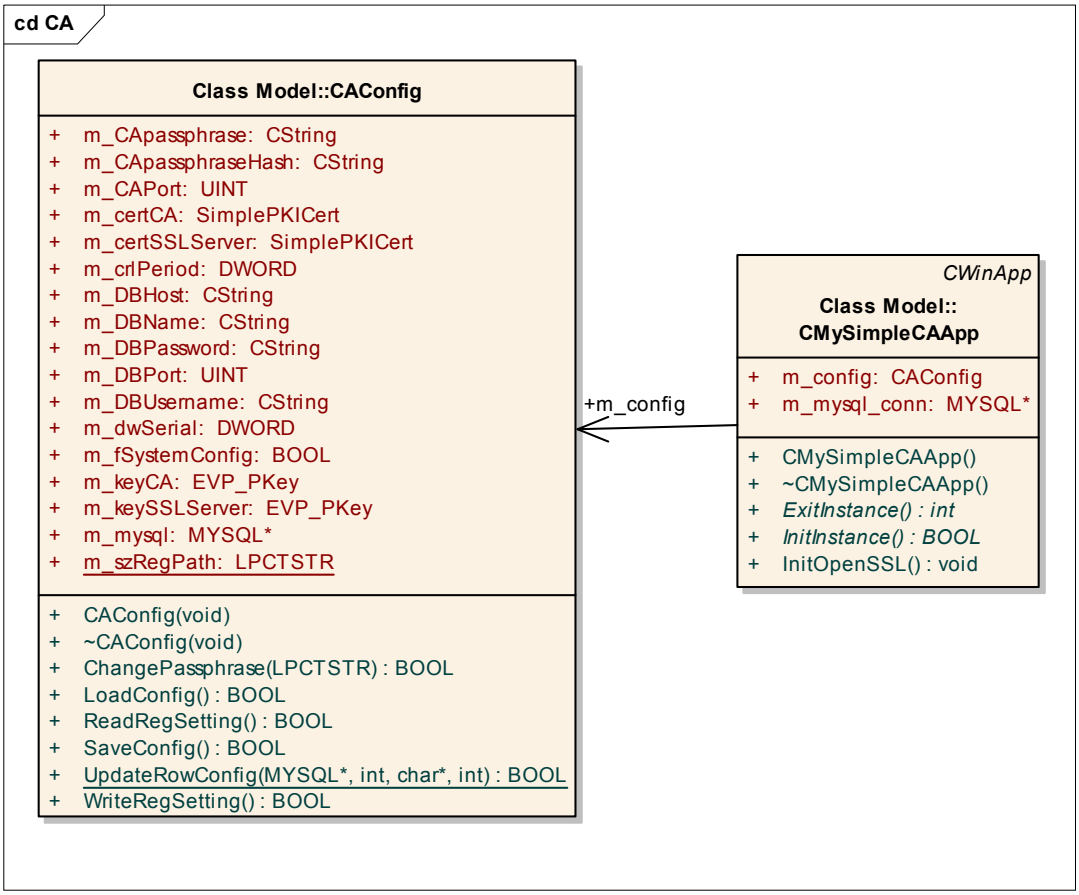
3.2.6. Lớp chính của CAServer

Các lớp này có nhiệm vụ duy trì hoạt động của CA, khởi tạo kết nối, lắng nghe yêu cầu từ client và trả lời các yêu cầu đó. CAServer giao tiếp với RAClient thông qua kênh truyền thông bảo mật SSL.



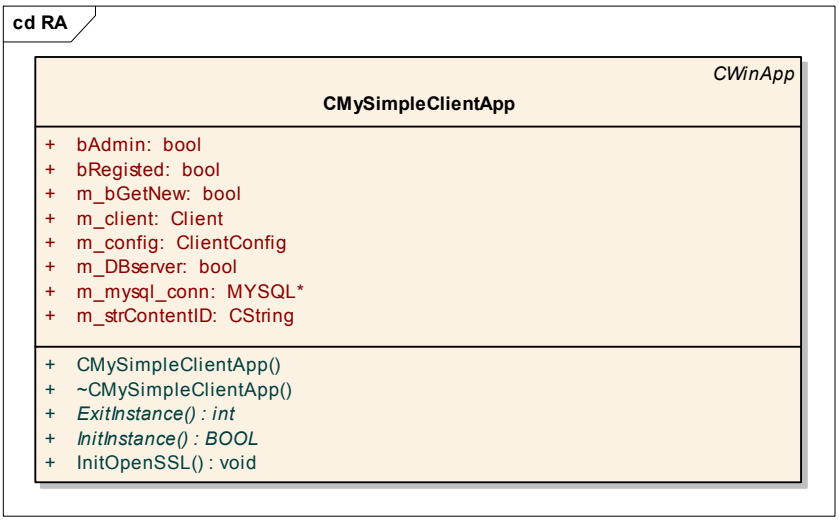
Hình 3-15 Lớp chính của CAServer : khởi tạo kết nối, lắng nghe yêu cầu và trả lời yêu cầu từ client

3.2.7. Lớp quản lý cấu hình của CAServer



Hình 3-16 Lớp quản lý cấu hình của CAServer

3.3. Thiết kế lớp của RAClient

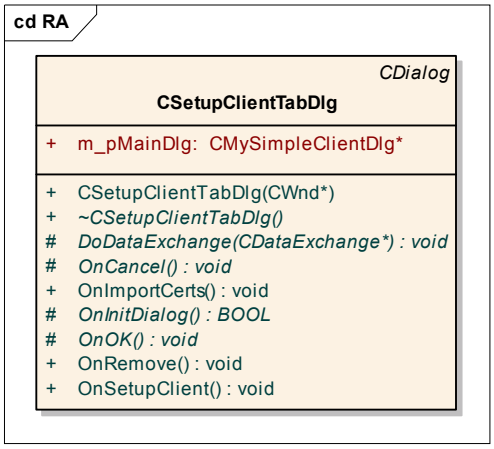


Hình 3-17 Lớp CMySimpleClientApp

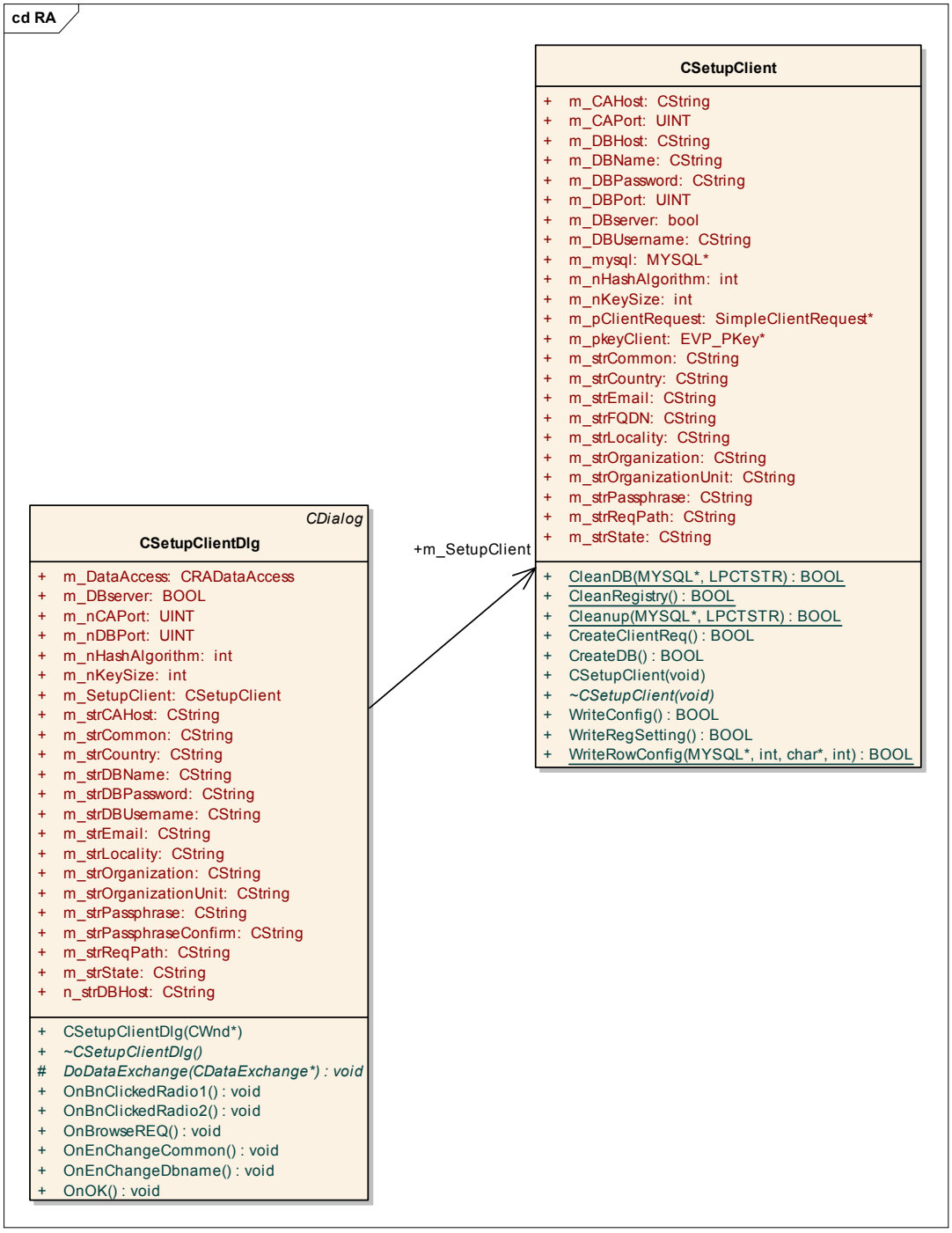
Kiểu	Tên	Ý nghĩa
MYSQL	m_mysql_conn	biến dùng để kết nối vào DB
BOOL	bRegisted	
BOOL	bAdmin	=1:Admin =0:User
ClientConfig	m_config	lưu trữ các thiết lập
Cstring	m_strContentID	
BOOL	m_bGetNew	=FALSE liên tục,ko thấy gì khả quan
Client	m_client	dùng để cho kết nối SSL

Bảng 3-1 Các thông số của lớp CmySimpleClientApp

3.3.1. Các lớp thuộc phần thiết lập cài đặt RA



Hình 3-18 CSetupClienTabDlg



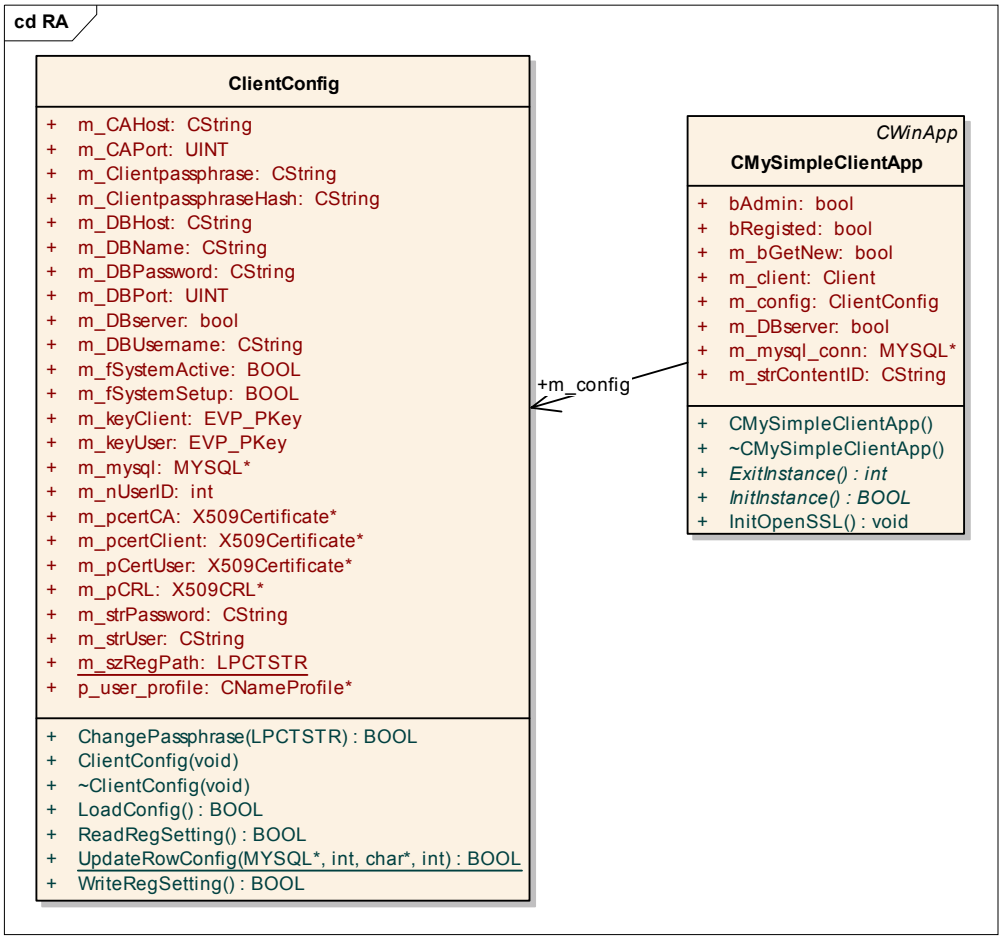
Hình 3-19 CsetupClient

Kiểu	tên	ý nghĩa
	m_DBHost, m_DBUsername, m_DBPassword, m_DBName, m_CAPort, m_mysql m_CAHost….	Thông số

CString	m_strCommon; m_strEmail; m_strCountry;m_strState; m_strLocality;m_strOrganization; m_strOrganizationUnit;	các thông tin của client admin
CString	m_strPassphrase	
CString	m_strReqPath	đường dẫn của file request
SimpleClientRequest	*m_pClientRequest	
EVP_PKey	m_pkeyClient	

Bảng 3-2 Mô tả lớp CsetupClient

3.3.2. Lớp chứa thông số cấu hình



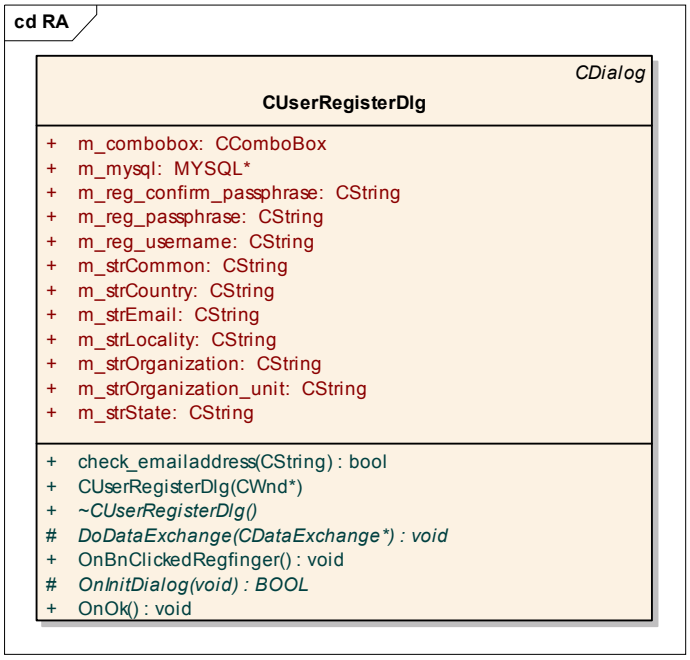
Hình 3-20 ClientConfig

3.3.3. Các lớp liên quan tới chức năng đăng nhập, đăng ký

Hình 3-21 CloginDlg

tên hàm hoặc biến	ý nghĩa
void CLoginDlg::VerifyUser()	kiểm tra xem m_username và m_strPassword có đúng ko,trả về biến bSuccess
CString m_username	username đăng nhập
MYSQL *m_mysql;	
int m_nLoginCount;	đếm số lần login, =3 thì out
ClientConfig m_pConfig	biến config được lấy từ cmysimpleclientapp.m_config
CString m_strPassword;	pass
BOOL bSuccess	=1:truy nhập ok =0:truy nhập thất bại
bool CLoginDlg::RegisterUser(CString passphrase, CString username)	đăng ký user và pass vào CSDL
bool CLoginDlg::IsUserRegisted(CString username)	kiểm tra trong CSDL xem đã đăng ký chưa

Bảng 3-3 Mô tả lớp CloginDlg

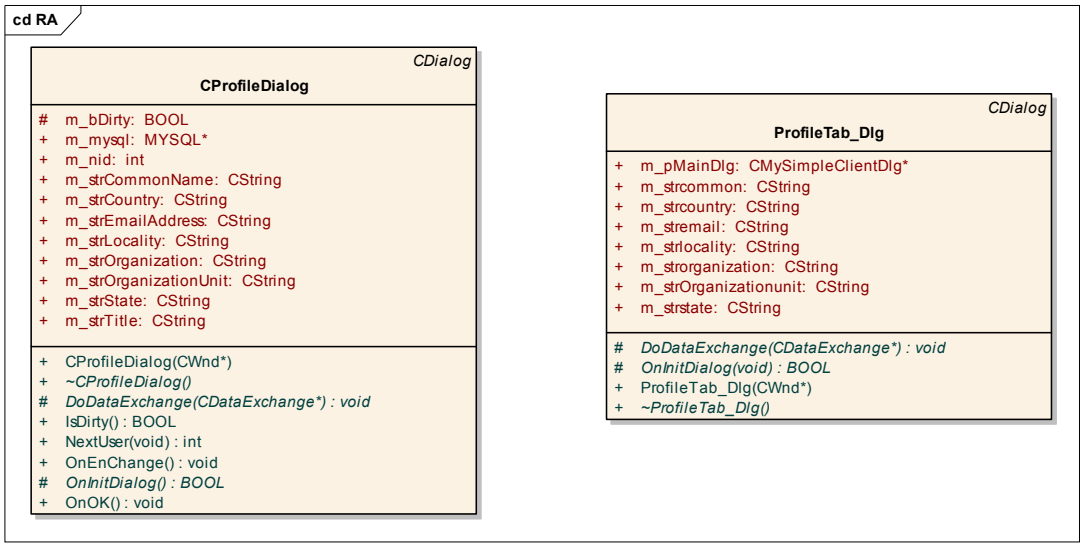


Hình 3-22 CUserRegisterDlg

3.3.4. Lớp làm việc với cơ sở dữ liệu

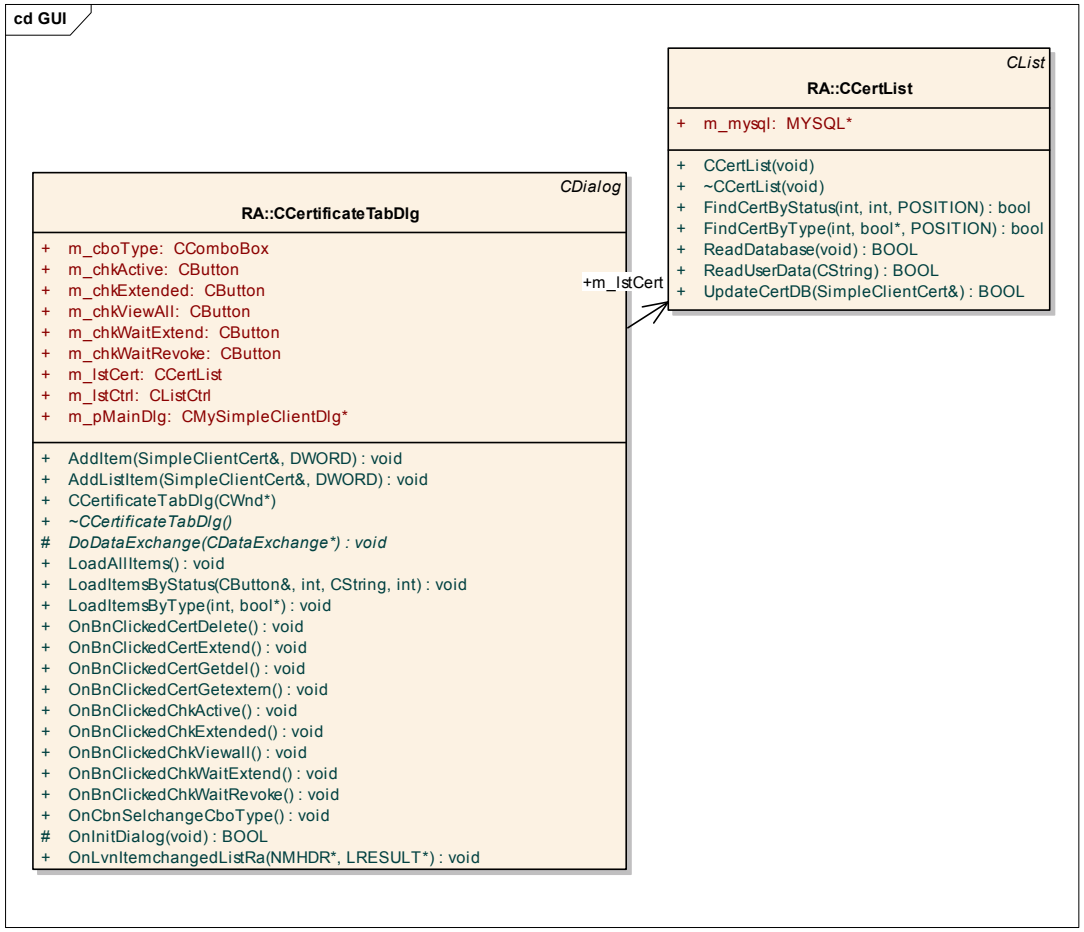
Hình 3-23 CRADataAccess

3.3.5. Lớp quản lý thông tin user



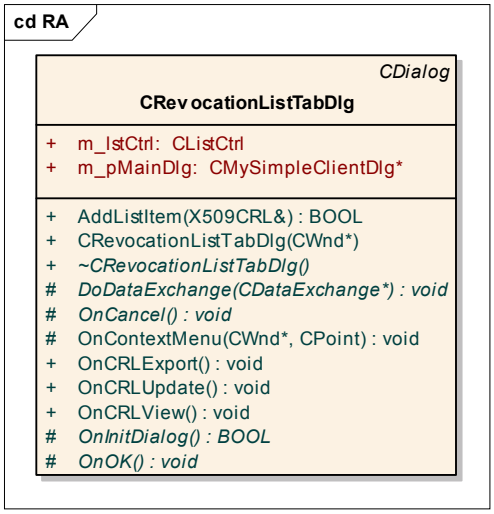
Hình 3-24 CProfileDialog

3.3.6. Lớp quản lý danh sách các chứng chỉ



Hình 3-25 CCertificateTabDlg

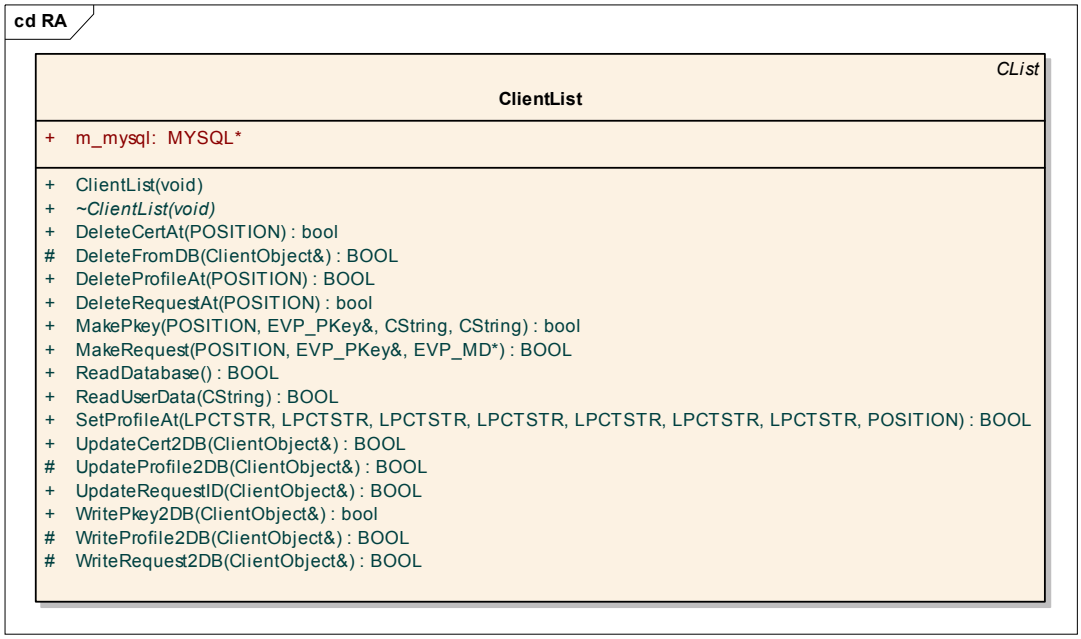
3.3.7. Lớp quản lý danh sách các chứng chỉ bị hủy



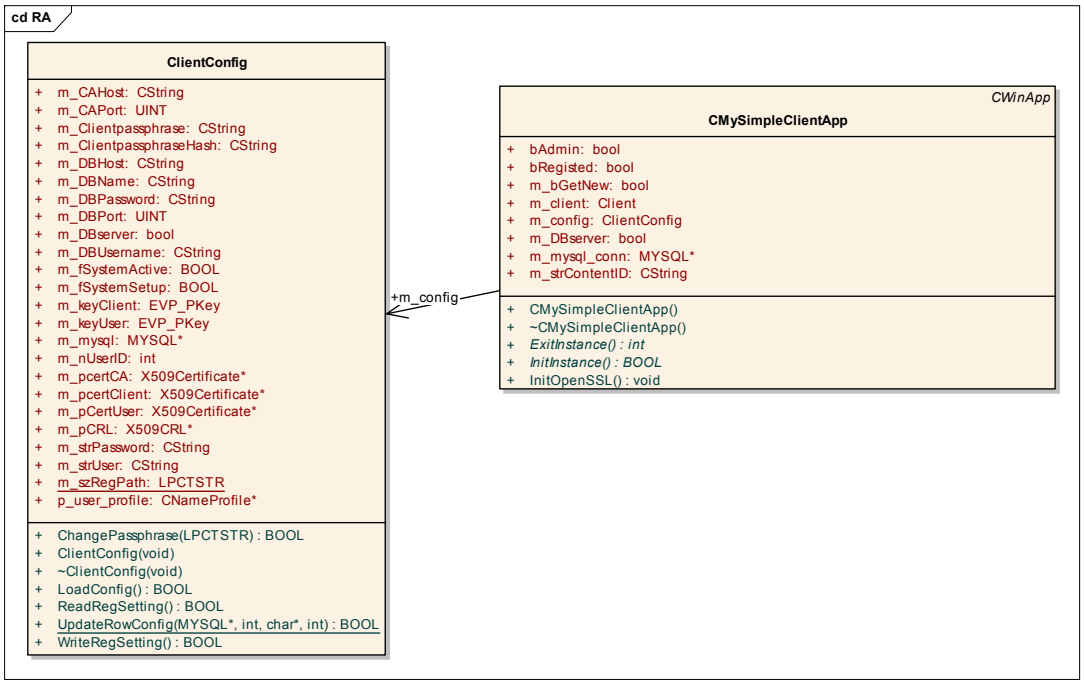
Hình 3-26 CRevocationListTabDlg

3.3.8. Lớp chính của RAClient

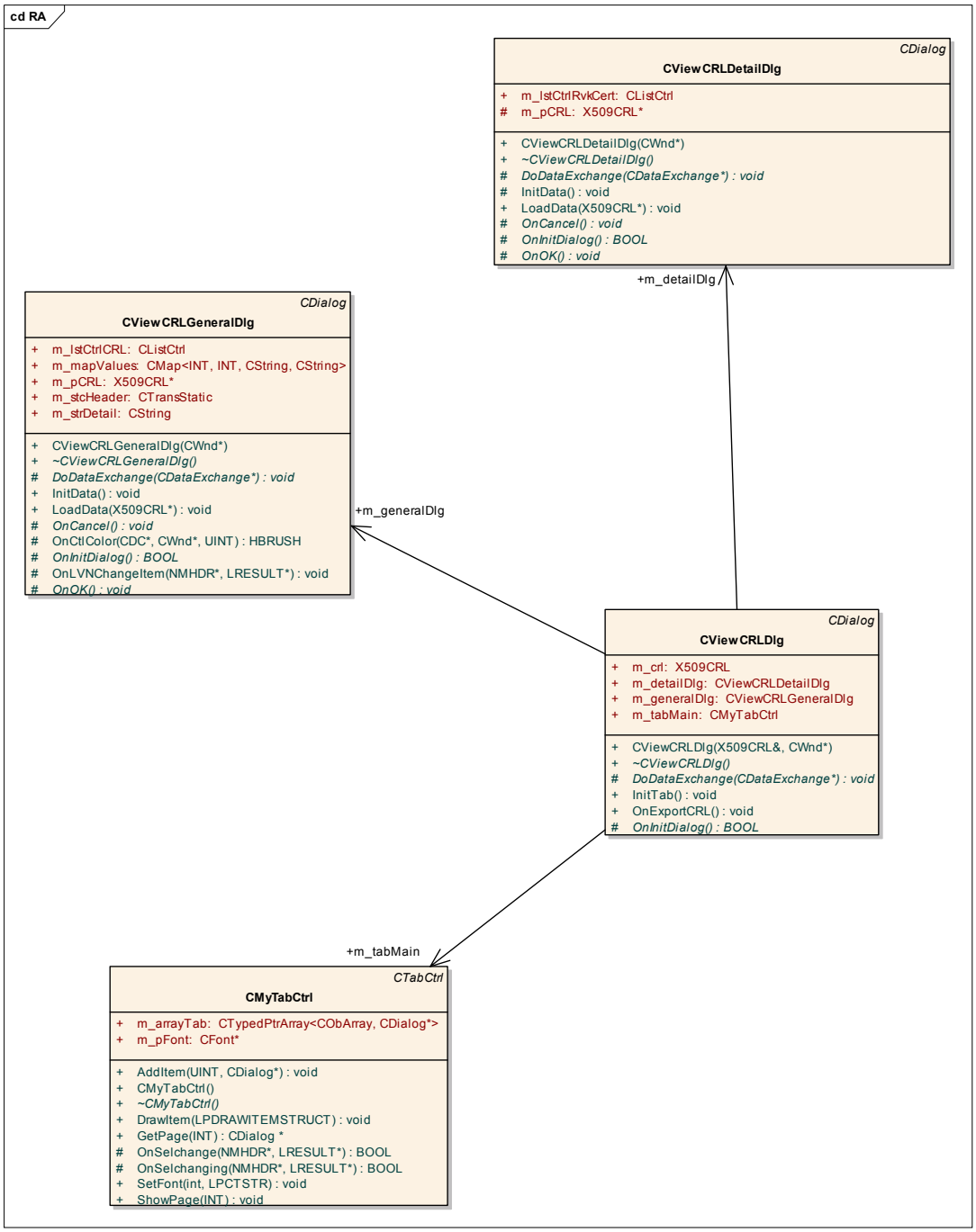
Hình 3-27 Client



Hình 3-28 ClienList

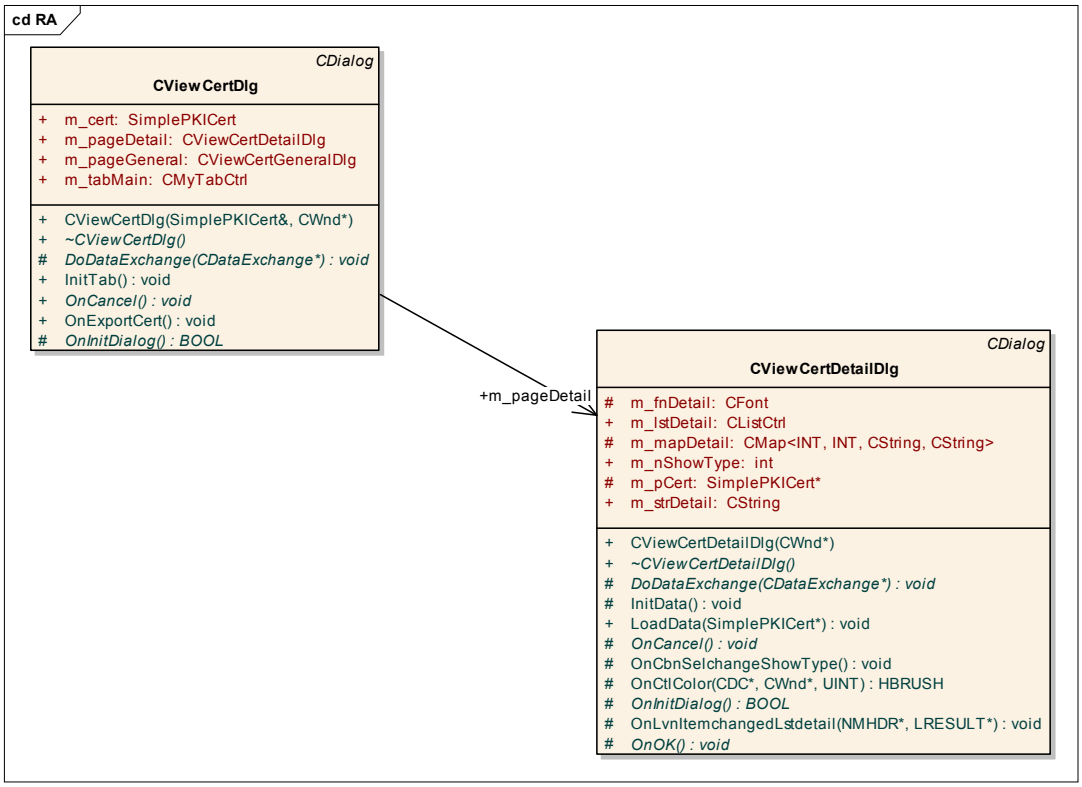


Hình 3-29 CMySimpleClientDlg, CmySimpleClientApp



Hình 3-30 Các lớp thuộc về các Tab chức năng của RAClient

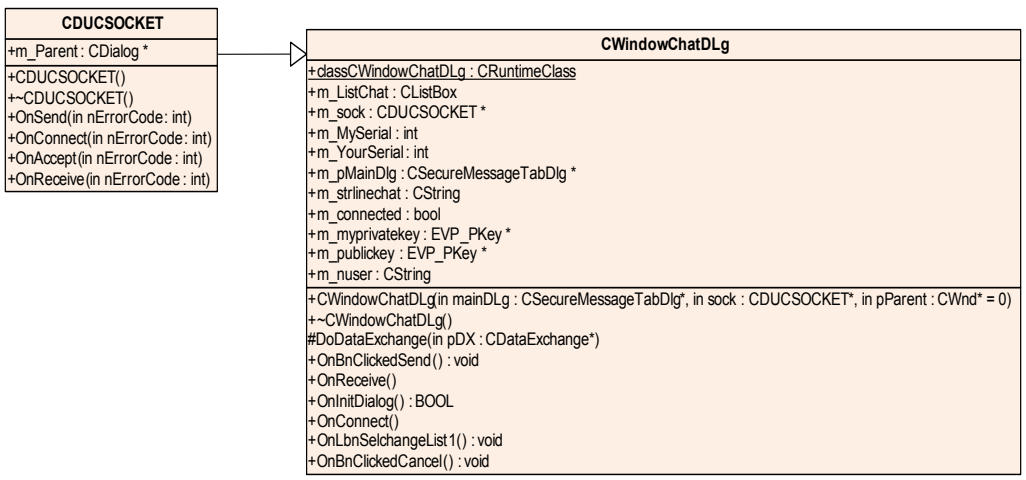
3.3.9. Lớp hiển thị nội dung chứng chỉ



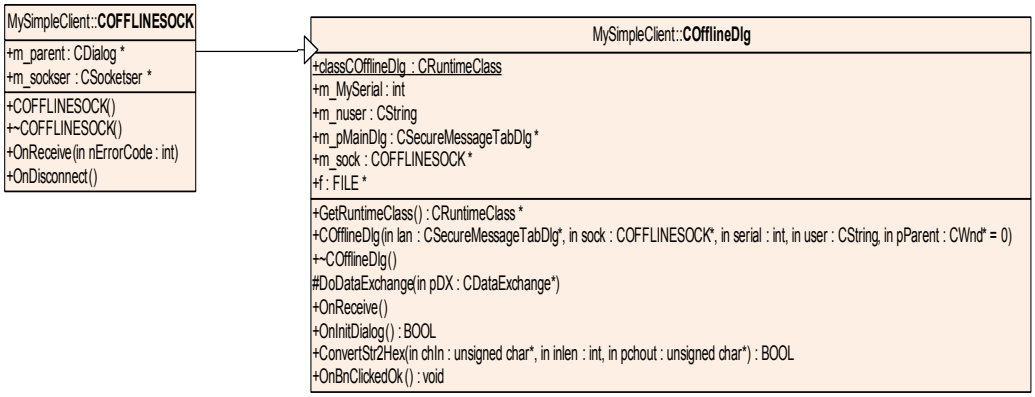
Hình 3-31 Các lớp hiển thị nội dung chứng chỉ số

3.4. Các lớp thuộc về các ứng dụng trong hệ thống

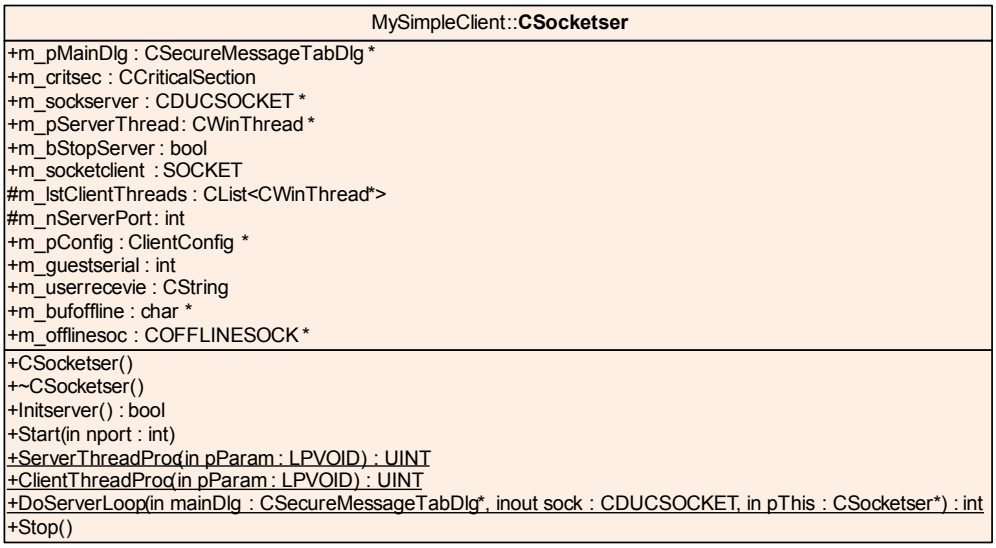
3.4.1. Ứng dụng bảo mật thông điệp



Hình 3-32

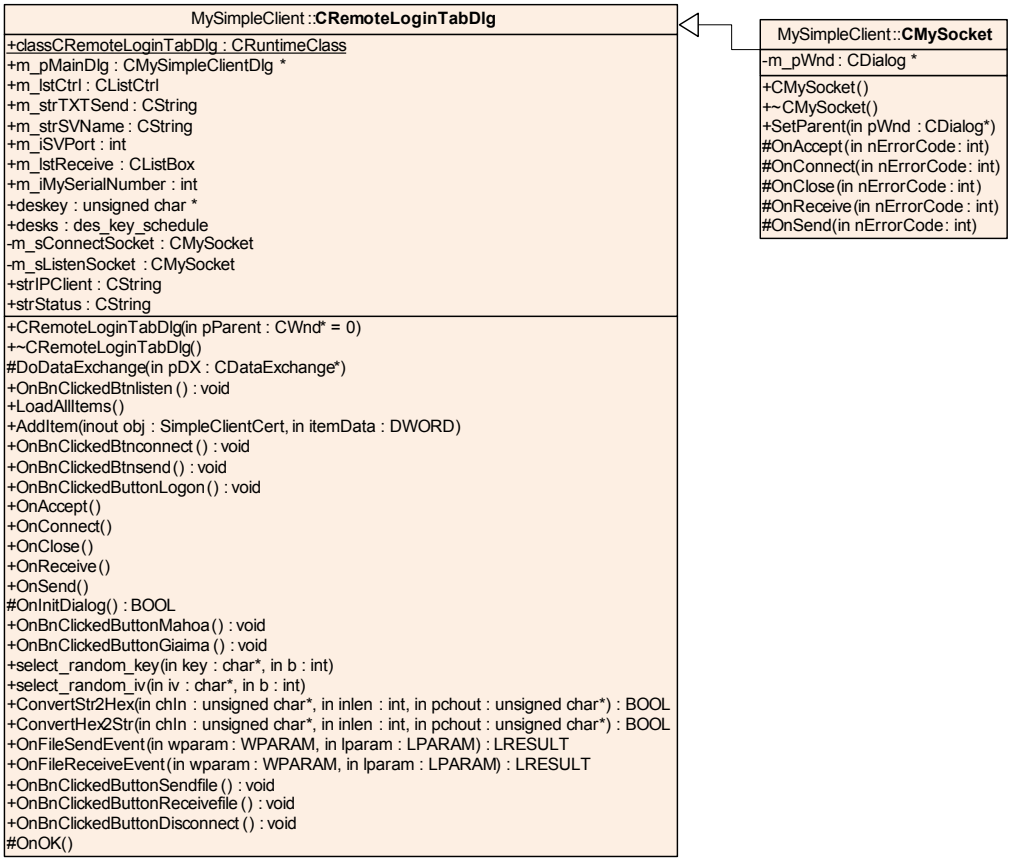


Hình 3-33



Hình 3-34

3.4.2. Ứng dụng bảo vệ truy nhập từ xa



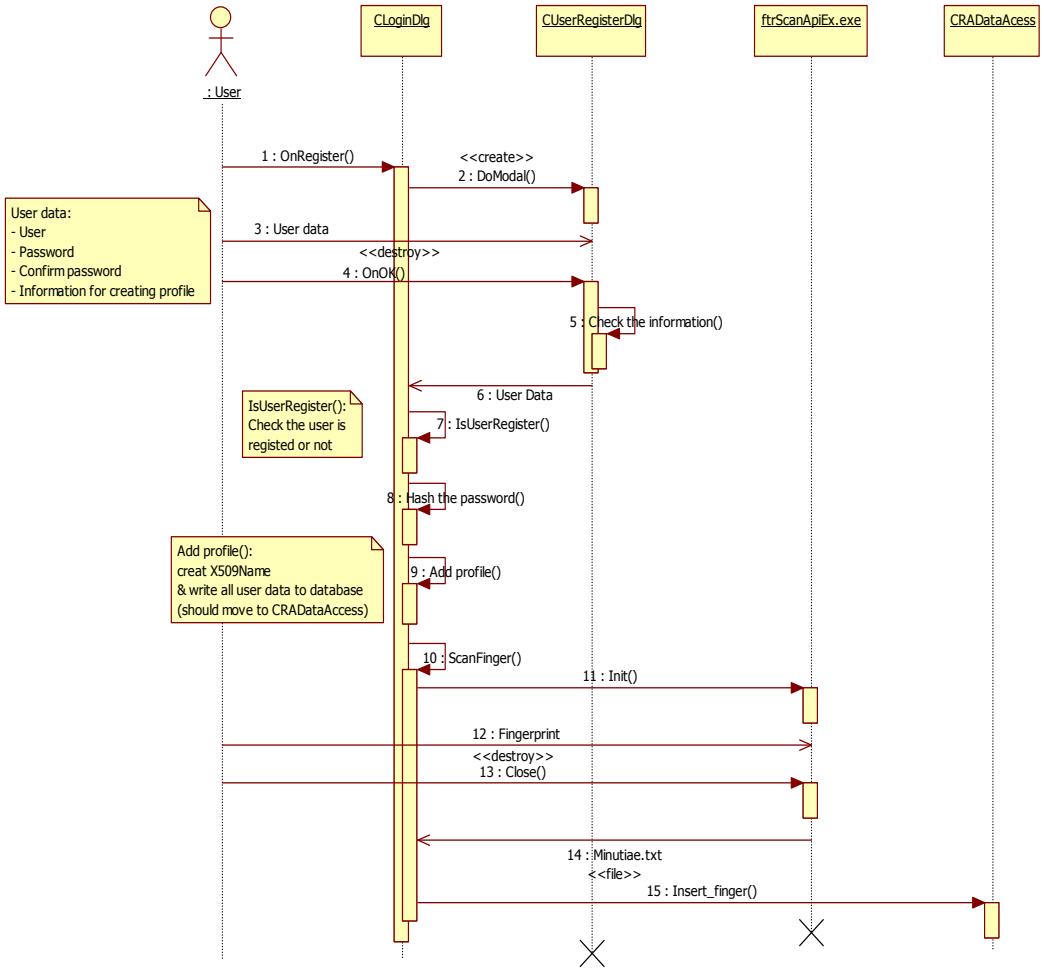
Hình 3-35

3.4.3. Ứng dụng chữ ký số và mã hóa thông điệp

Hình 3-36

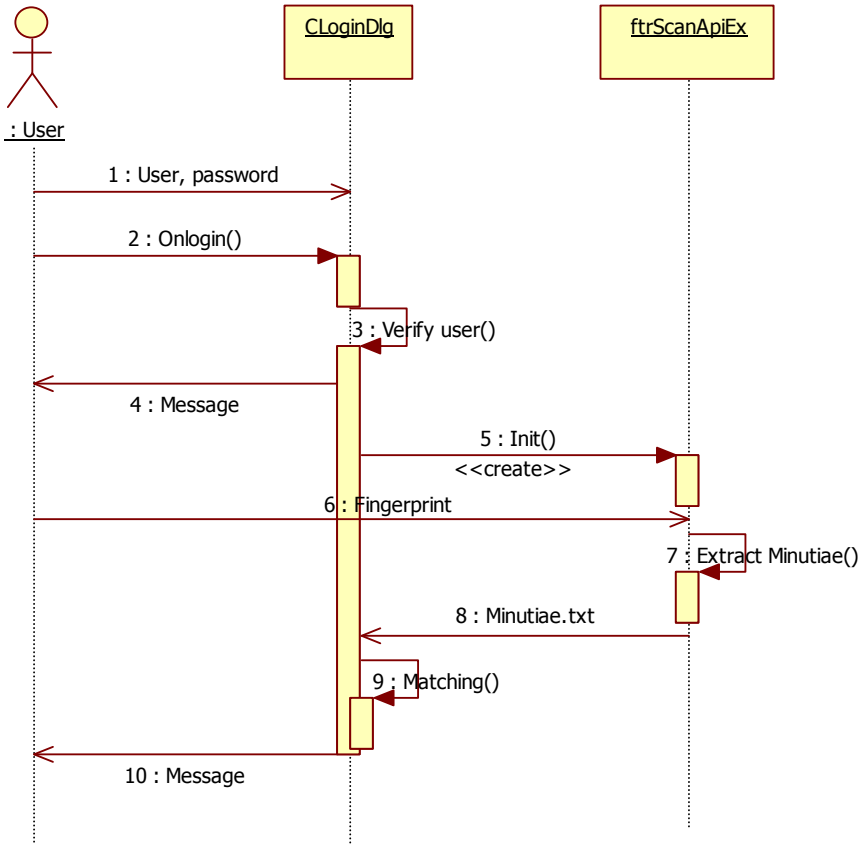
4. DIỄN BIẾN CÁC CA SỬ DỤNG

4.1. Đăng ký người dùng mới vào hệ thống



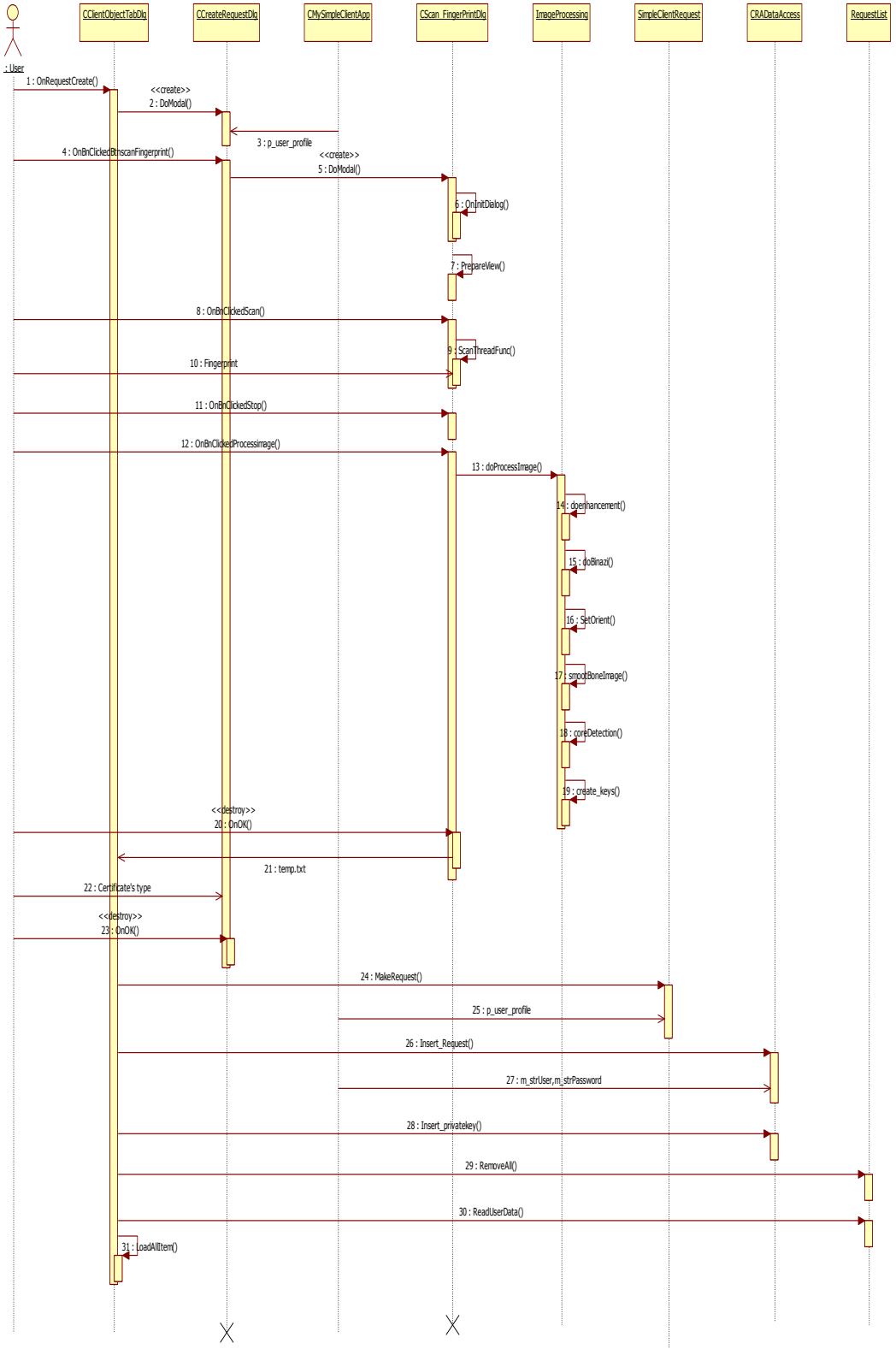
Hình 4-1 Biểu đồ diễn tiến hoạt động đăng ký người dùng mới vào hệ thống

4.2. Đăng nhập



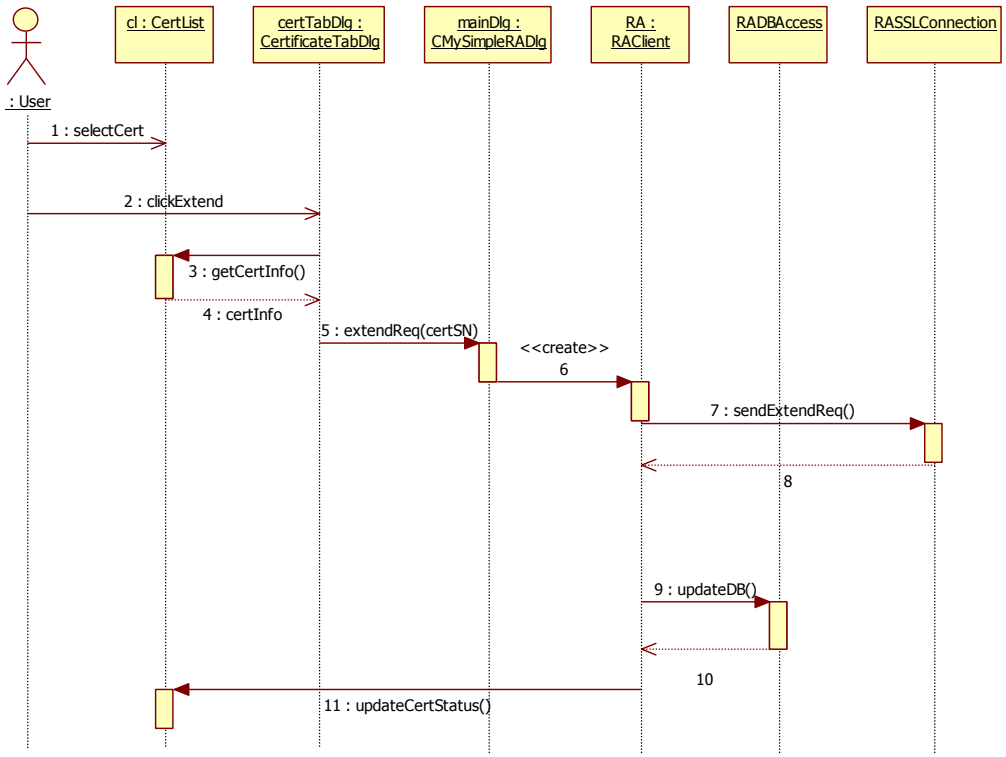
Hình 4-2 Biểu đồ diễn tiến hoạt động đăng nhập

4.3. Tạo yêu cầu chứng chỉ

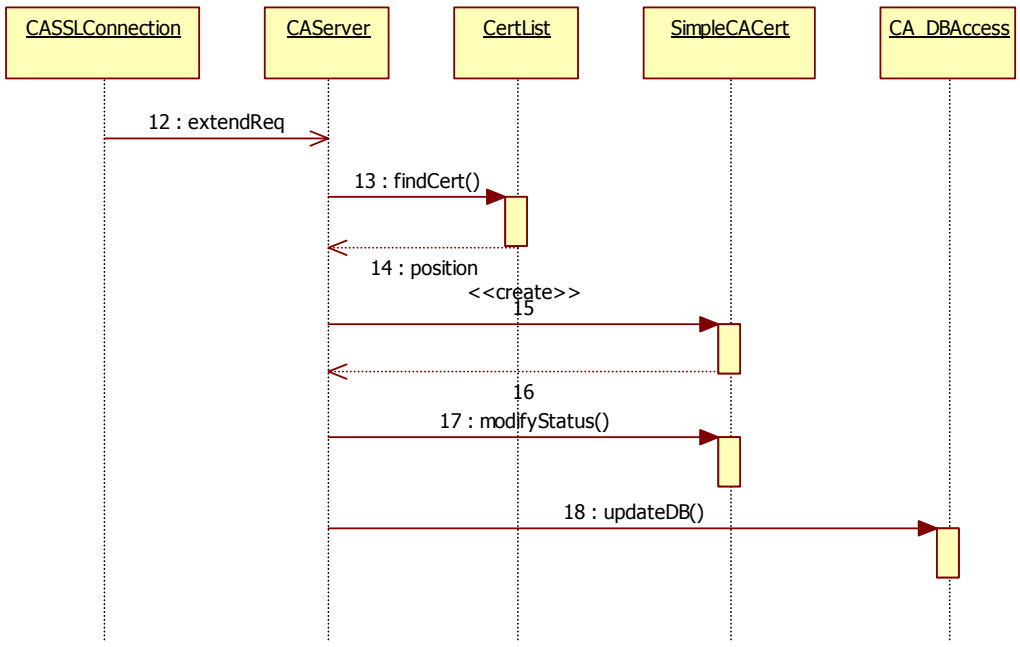


Hình 4-3 Tạo yêu cầu chứng chỉ

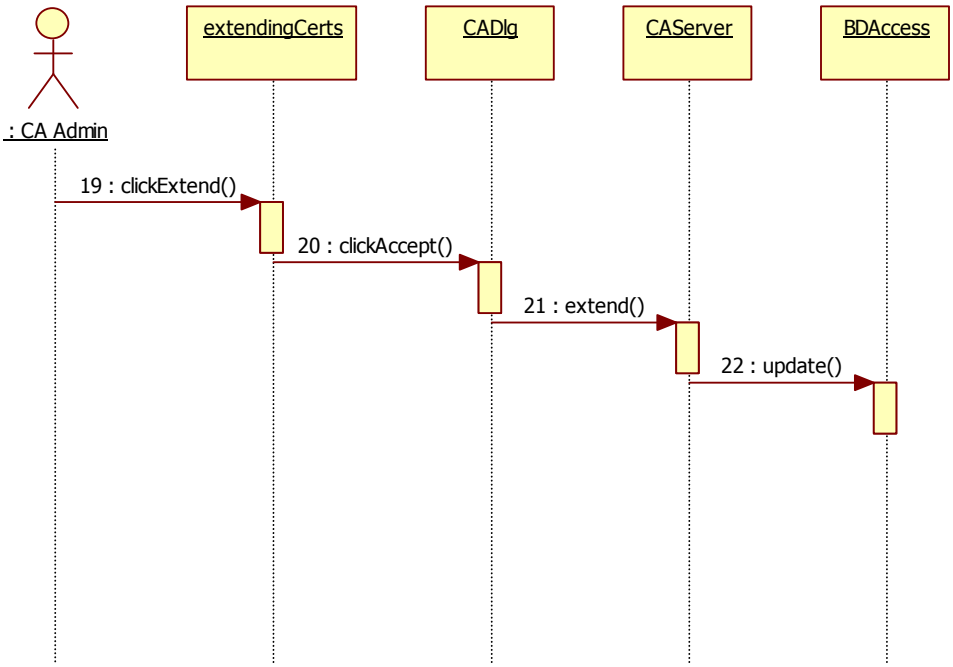
4.4. Gia hạn chứng chỉ



Hình 4-4 Gửi yêu cầu gia hạn

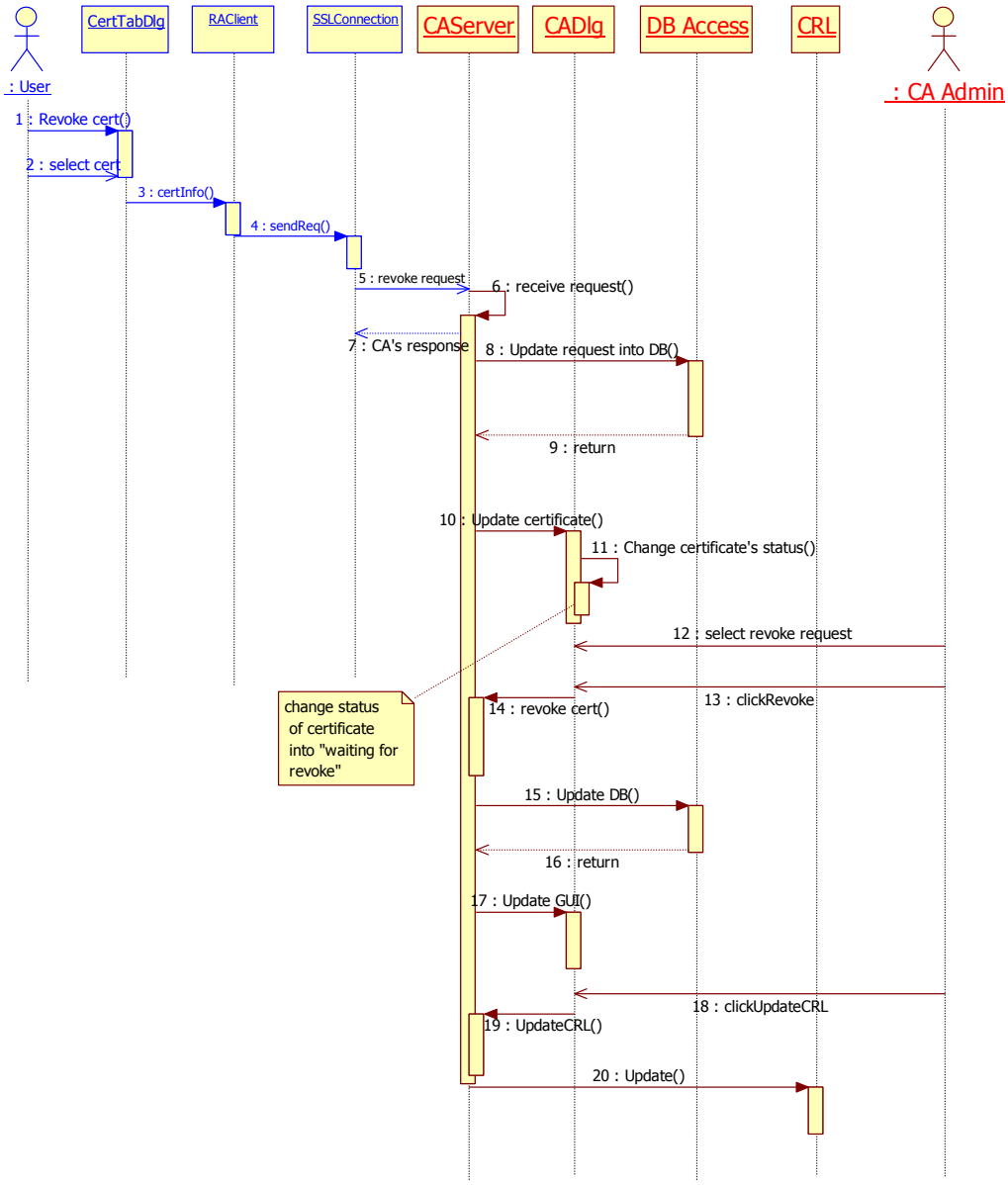


Hình 4-5 Nhận yêu cầu



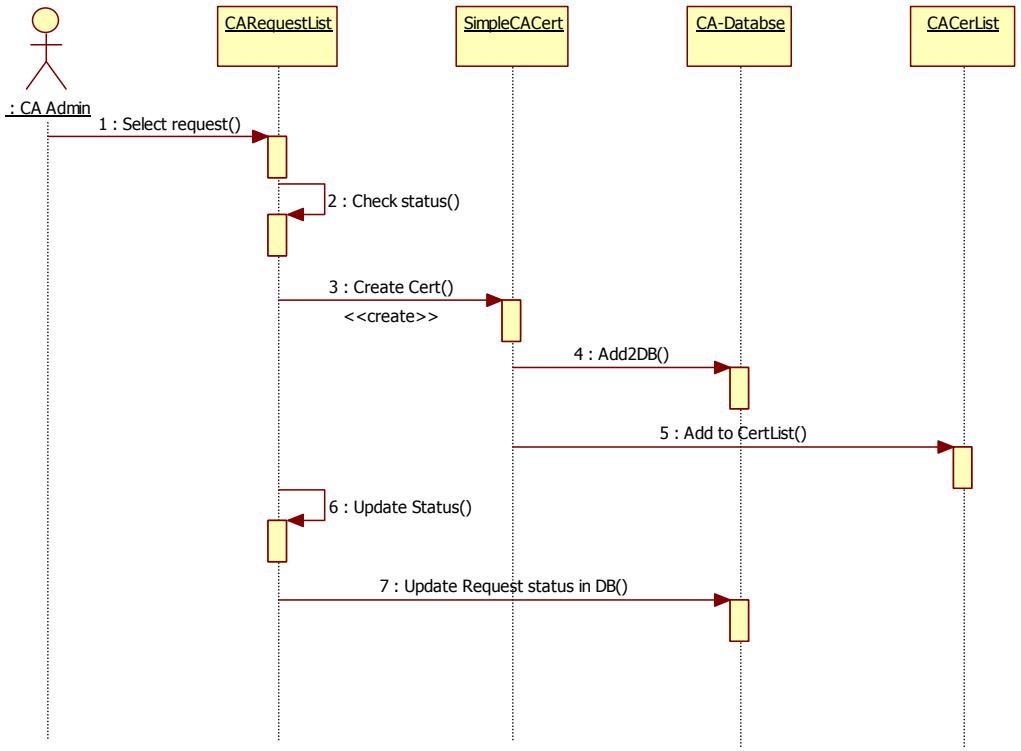
Hình 4-6 Gia hạn chứng chỉ

4.5. Thu hồi chứng chỉ



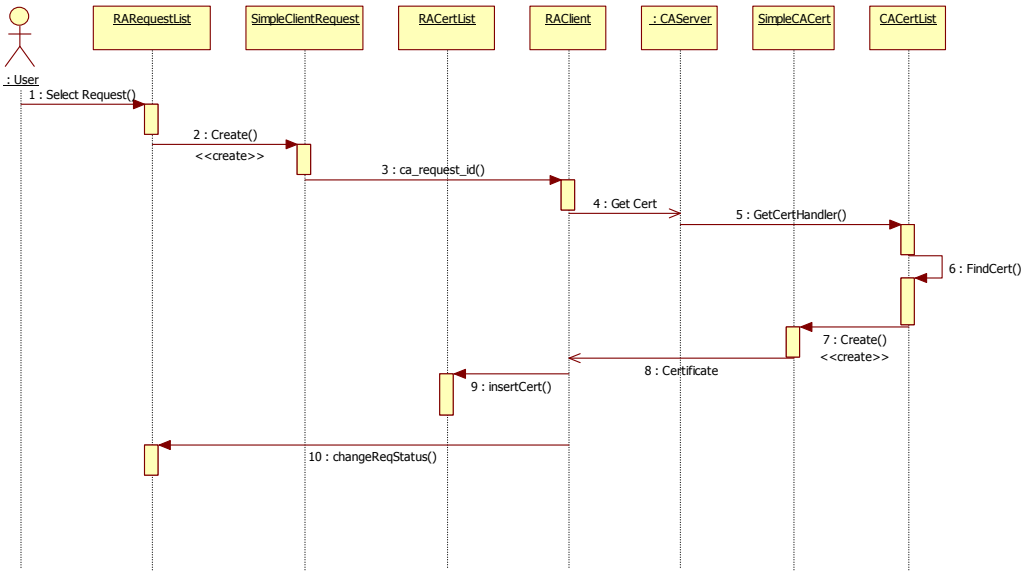
Hình 4-7 Thu hồi chứng chỉ

4.6. Phát hành chứng chỉ



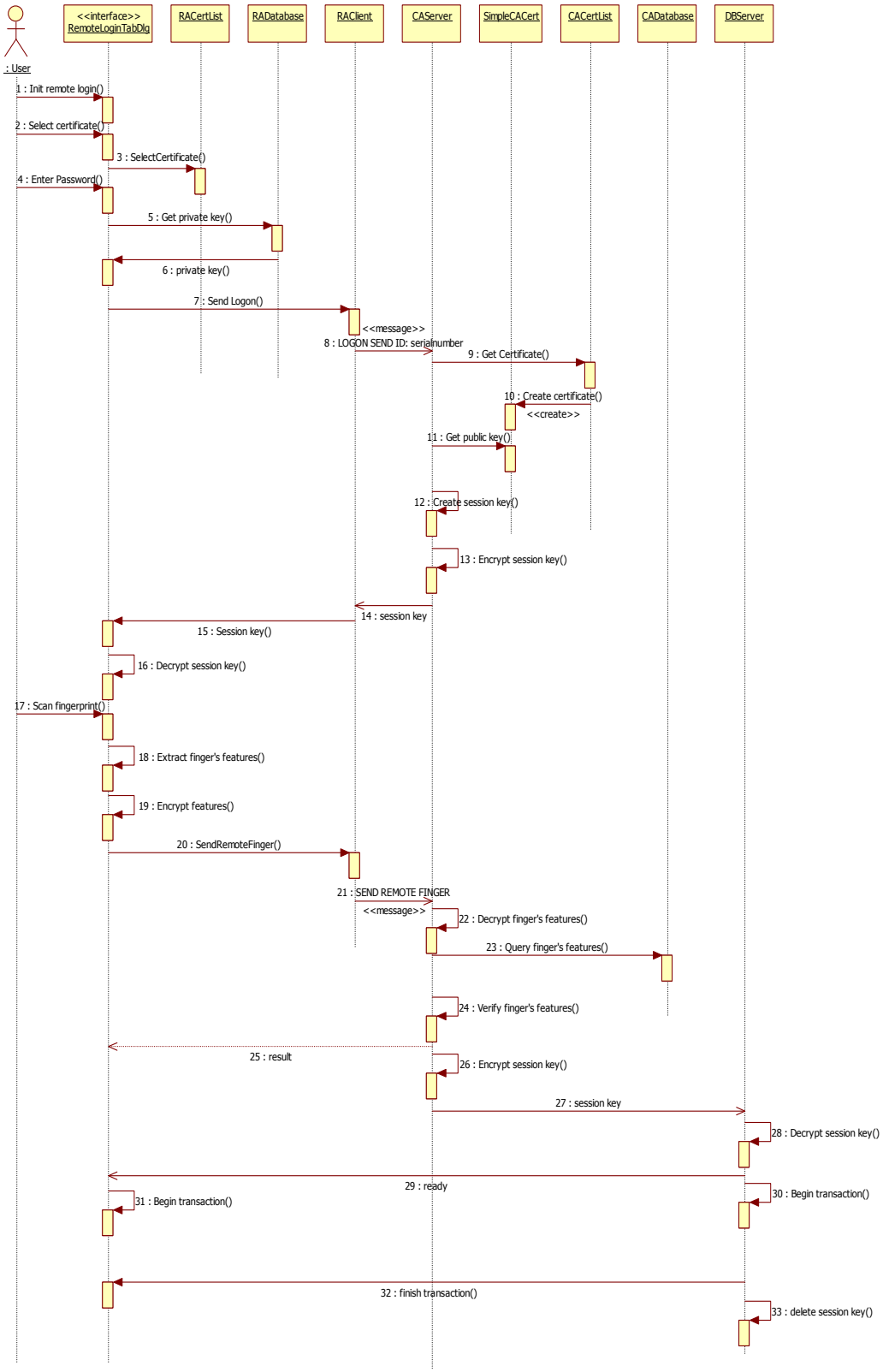
Hình 4-8 Phát hành chứng chỉ

4.7. Lấy chứng chỉ



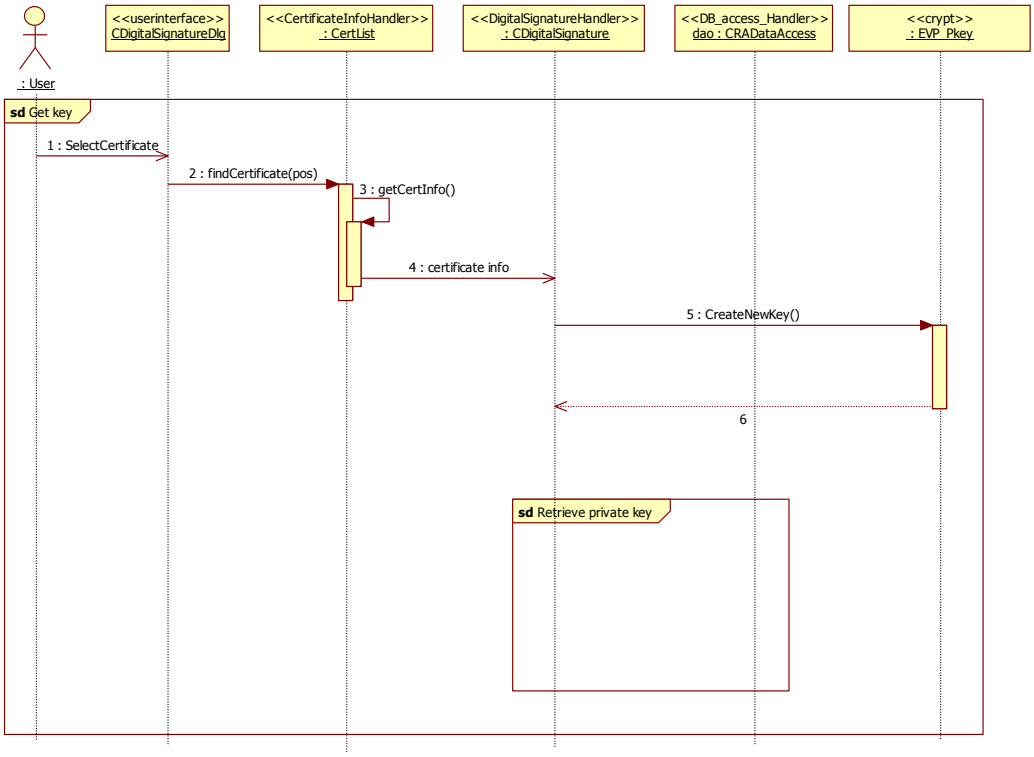
Hình 4-9 Lấy chứng chỉ

4.8. Truy cập từ xa

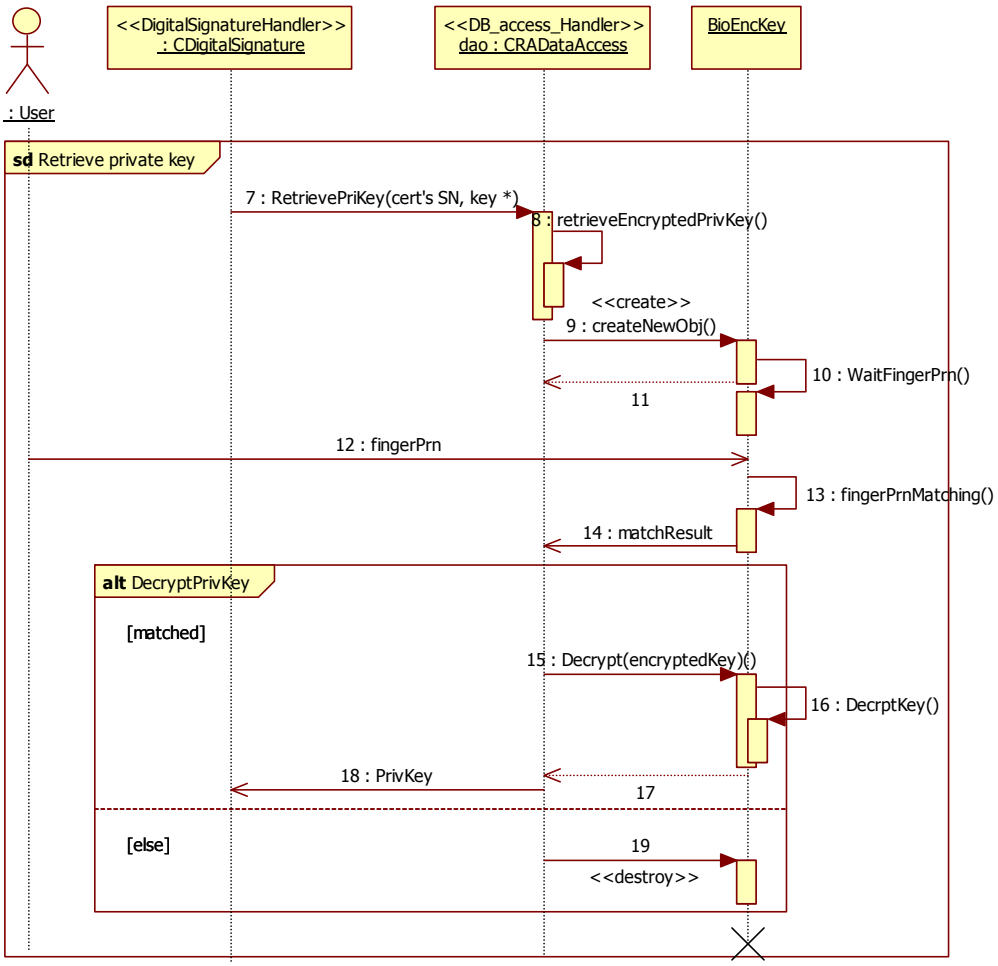


Hình 4-10 Truy cập từ xa

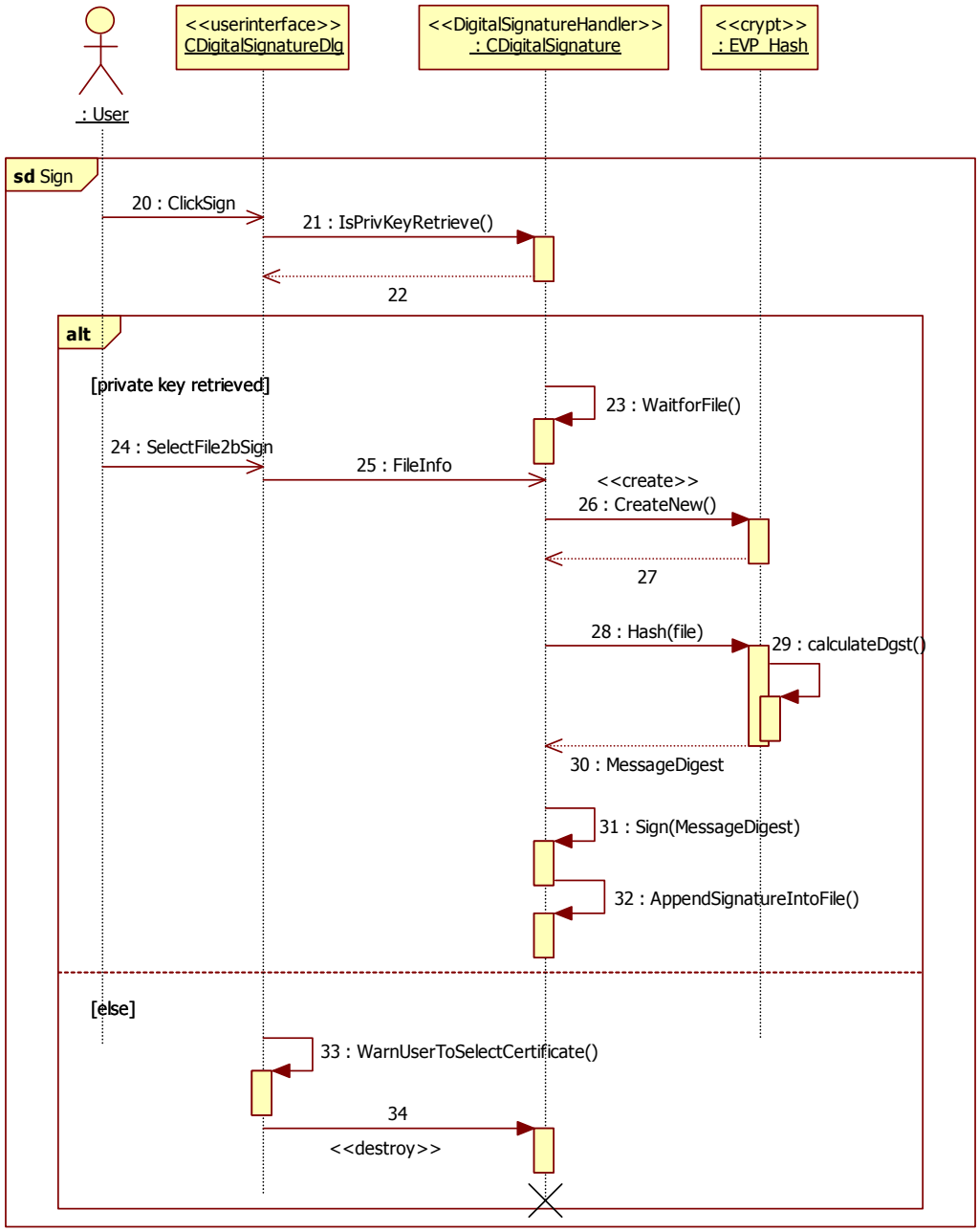
4.8. Chữ kí số



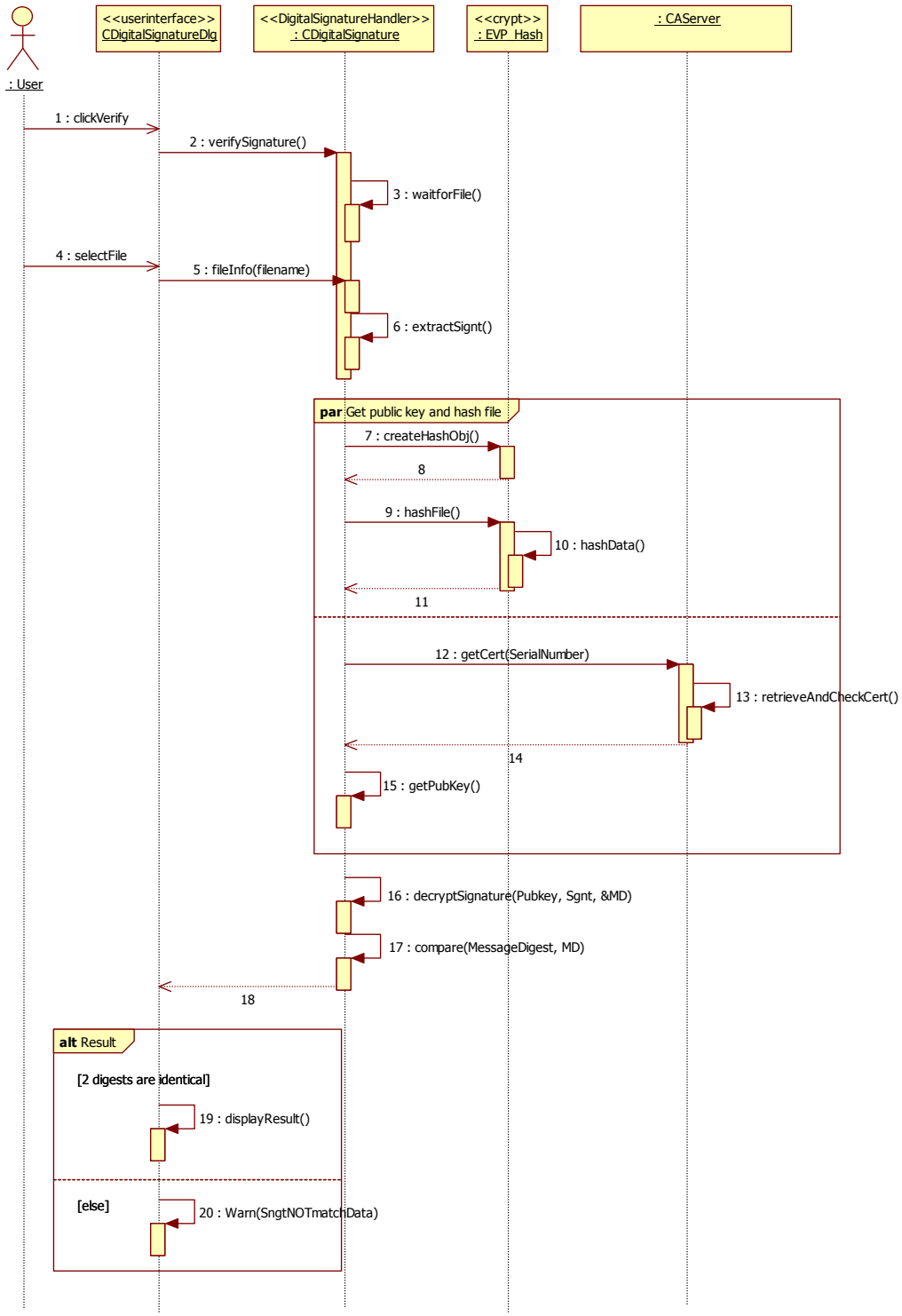
Hình 4-11 Ký



Hình 4-12 Lấy khóa cá nhân

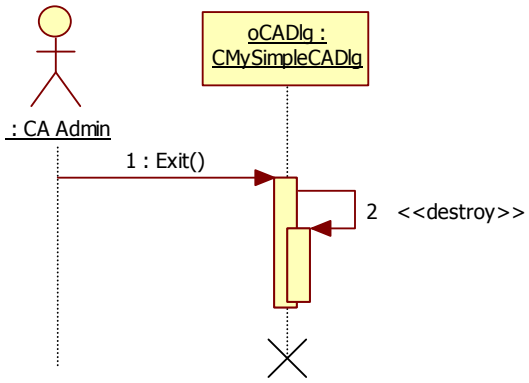

: User
<<userinterface>>
CDigitalSignatureDlg
<<DigitalSignatureHandler>>
: CDigitalSignature
<<crypt>>
: EVP_Hash
sd Sign
20 : ClickSign
21 : IsPrivKeyRetrieve()
22
alt
[private key retrieved]
23 : WaitforFile()
24 : SelectFile2bSign
25 : FileInfo
<<create>>
26 : CreateNew()
27
28 : Hash(file)
29 : calculateDgst()
30 : MessageDigest
31 : Sign(MessageDigest)
32 : AppendSignatureIntoFile()
[else]
33 : WarnUserToSelectCertificate()
34
<<destroy>>

Hình 4-13 Ký

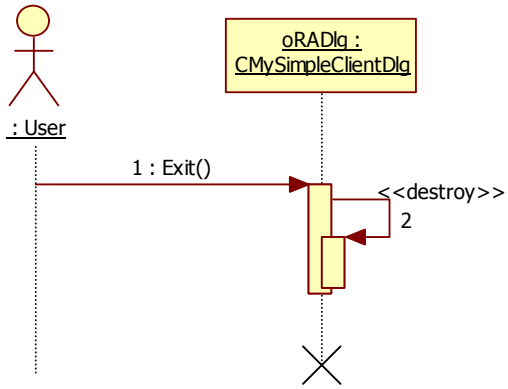


Hình 4-14 Kiểm tra chữ ký

4.10. Đăng xuất



Hình 4-15 Đăng xuất phía CA



Hình 4-16 Người dùng thoát khỏi hệ thống

5. THIẾT KẾ CƠ SỞ DỮ LIỆU

5.1. CAServer

5.1.1. Bảng tblCertificate

Tên trường	Khóa chính	Kiểu	Mô tả
SerialNumber	Yes	Int	Lưu trữ số sn của chứng chỉ.
RequestID	No	Int	Lưu trữ mã của yêu cầu tương ứng với yêu cầu trong bảng
X509Cert	No	BLOB	Nội dung của chứng chỉ.
Cert_Status	No	Int	Trạng thái của chứng chỉ: 0: Đang hoạt động. 1: Đang xin gia hạn 2: Đang xin hủy 3: Đã bị hủy
Revoke date	No	Datetime	Ngày chứng chỉ bị hủy

Bảng 5-1 tblCertificate

5.1.2. Bảng tblCRL:

Tên trường	Khóa chính	Kiểu	Mô tả
Date_signed	Yes	Datetime	Ngày CRL được CA ký rồi đưa vào kho chứa CRLs
CRL	No	BLOB	Nội dung của chứng chỉ.

Bảng 5-2 tblCRL

5.1.3. Bảng tblRequest

Tên trường	Khóa chính	Kiểu	Mô tả
RequestID	Yes	Int	Mã yêu cầu do chương trình tự sinh ra khi nhận được 1 yêu cầu từ RA.
Status	No	Int	Trạng thái của yêu cầu: 0: Đang chờ đợi. 1: Đã được chấp nhận. 2: Đã bị từ chối.
X509Request	No	BLOB	Dạng yêu cầu chuẩn X509.

Bảng 5-3 tblRequest

5.1.4. Mô tả tóm tắt các hoạt động liên quan tương tác đến CSDL:

+ Khi nhận được yêu cầu xin cấp chứng chỉ:

Chương trình sẽ sinh ra một mã gọi là requestID và lưu yêu cầu đó vào bảng tblRequest với trạng thái status=0.

Khi CA chấp nhận thì sẽ chuyển status đó thành 1 và tự sinh ra một chứng chỉ với 1 số Serial Number và ghi vào bảng tblCertificate, đồng thời có liên kết 1-1 với bảng tblRequest bằng thành phần requestID, và để biến trạng thái Cert_Status là 0.

+ Khi nhận được yêu cầu xin gia hạn chứng chỉ:

Chuyển giá trị trường Cert_Status thành 1 ⇔ Clien đang xin gia hạn

Nếu chấp nhận gia hạn thì chuyển Cert_Status thành 0 & set trường revoke_date⇔ Chứng chỉ được chấp nhận gia hạn và chứng chỉ bây giờ là có giá trị hoạt động

+ Khi nhận được yêu cầu xin chấm dứt sử dụng chứng chỉ:

Chuyển Cert_Status thành 2.

Nếu đồng ý thì chuyển Cert_Status thành 4

5.2. RAClient

5.2.1. Bảng user

Trường	Khóa chính	Kiểu dữ liệu	Mô tả
User	Yes	Varchar(20)	Tên người sử dụng
Profile	No	BLOB	Lưu trữ thông tin user theo chuẩn X509Name
Password	No	Varchar(20)	Lưu mã băm của password đăng nhập hệ thống của user
Fingerprint	No	BLOB	Lưu trữ vân tay của user ngay lúc đăng kí

Bảng 5-4 user

5.2.2. Bảng request

Trường	Khóa chính	Kiểu dữ liệu	Mô tả
RA RequestID	Yes	Interger	Tự động tăng, dùng làm mã yêu cầu mà RA cung cấp cho user.
X509Request	No	BLOB	Được tạo ra từ X509Name bằng hàm chuẩn của X509
CA RequestID	No	Interger	Đây là mã yêu cầu RA nhận được từ CA ngay khi CA nhận được request. Sử dụng để lấy chứng chỉ từ CA
Request Status	No	Interger	0: Requested 1: Submitted (Request đã được gửi lên CA và nhận được CA RequestID, chỉ khi nhận được cái này rồi mới chuyển) 2: Issued (Yêu cầu đã được chấp nhận) 3: Denied (Yêu cầu bị từ chối)
User	No	Varchar (20)	Khóa ngoài, liên kết nhiều -1 với bảng User.

Type	No	Interger	Loại chứng chỉ được yêu cầu cấp 0: chứng chỉ RA 1: chứng chỉ sử dụng chữ kí số 2: chứng chỉ sử dụng để mã hóa thông điệp 3: chứng chỉ sử dụng để truy cập từ xa

Bảng 5-5 Request

5.2.3. Bảng Certificate

Trường	Khóa chính	Kiểu dữ liệu	Mô tả
Serial Number	Yes	Interger	Serial number của chứng chỉ
X509Cert	No	BLOB	Lưu chứng chỉ dạng pem
User	No	Varchar(20)	Khóa ngoài, lk nhiều – 1 với bảng User
CA RequestID	No	Integer	Được đồng bộ từ bảng Request
Cert Status	No	Integer	1: đang hoạt động 2: bị hủy 3: hết hạn 4: đang gia hạn 5: đang xin hủy
Type	No	Interger	Loại chứng chỉ 0: chứng chỉ sử dụng chữ kí số 1: chứng chỉ sử dụng để mã hóa thông điệp 3: chứng chỉ sử dụng để truy cập từ xa

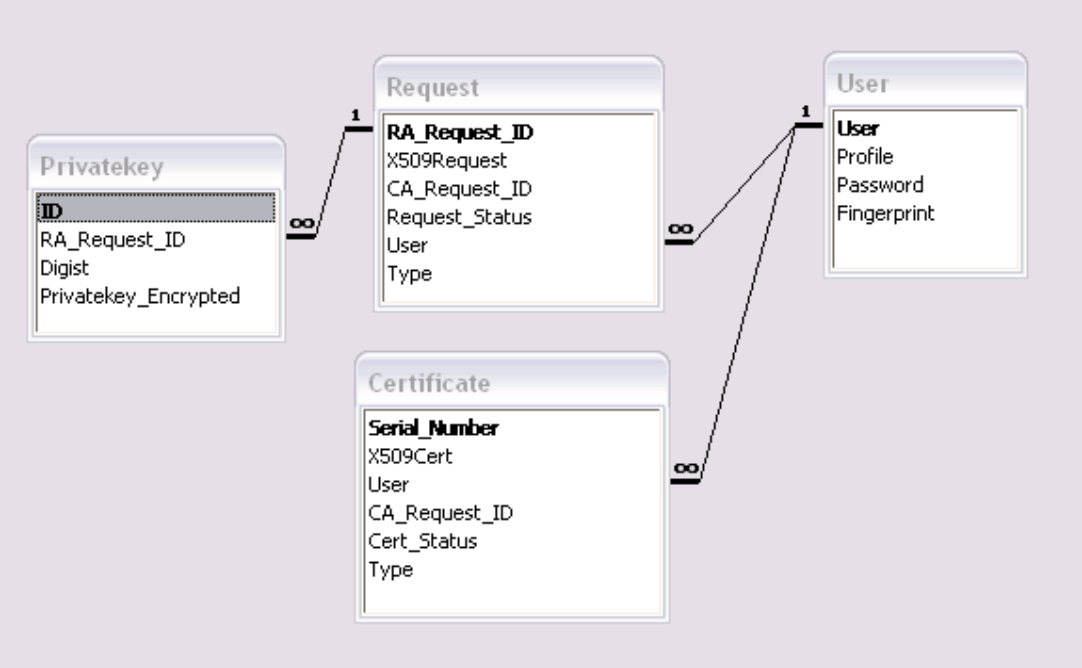
Bảng 5-6 Certificate

5.2.4. Bảng Khóa cá nhân

Trường	Khóa chính	Kiểu dữ liệu	Mô tả
ID	Yes	Interger	Tự động tăng
RARequestID	No	Interger	Mã yêu cầu ở RA
Digist	No	Varchar(30)	Mã băm của từng đặc trưng vân tay
Khóa cá nhân_Encryptedkey	No	BLOB	Chứa khóa cá nhân được mã hóa bởi từng đặc trưng vân tay tương ứng

Bảng 5-7 Khóa cá nhân

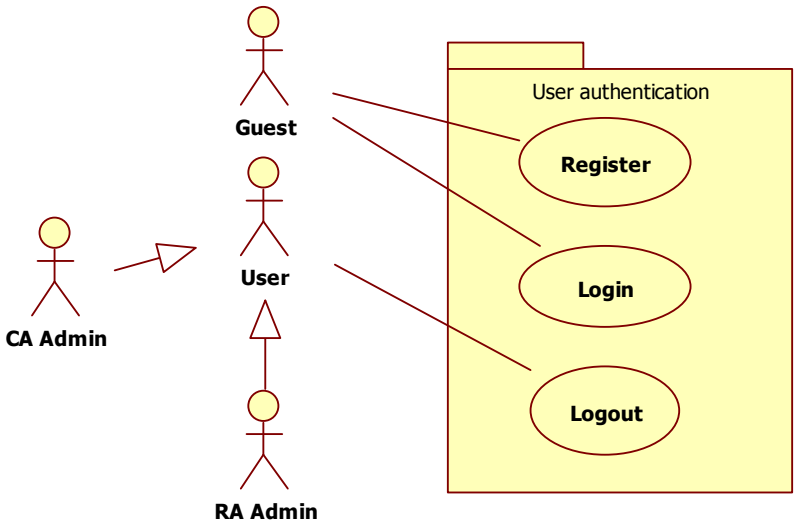
5.2.5. Quan hệ giữa các bảng



Hình 5-1 Quan hệ giữa các bảng

6. 6 ĐẶC TẢ CÁC CHỨC NĂNG

6.1. Các chức năng liên quan tới đăng nhập người dùng



6.1.1. Register

Tên ca sử dụng	Đăng kí (register)
Tác nhân	Khách
Mô tả	Khách chưa có tài khoản cần đăng ký để sử dụng các chức năng hệ thống cung cấp
Tiền đề	Khách chưa có tài khoản sử dụng hệ thống
Kết thúc thành công	Hệ thống tạo một tài khoản cho người khách
Kết thúc thất bại	Hệ thống không tạo tài khoản cho người khách.
Luồng sự kiện	1. Khách chọn "Đăng ký tài khoản" từ màn hình Login. 2. Hệ thống hiển thị form đăng kí trống để khách điền thông tin đăng kí. 3. Khách nhập các thông tin trên form đăng ký từ bàn phím, quét vân tay để lấy mẫu. 4. Hệ thống tạo tài khoản mới cho người khách nếu khách chọn đồng ý đăng kí ở bước 3. 4.1. Vân tay được hệ thống xử lý, trích đặc trưng để mã hóa khóa cá nhân 4.2. Các đặc trưng được băm và lưu vào cơ sở dữ liệu để đối sánh sau này. 5. Kết thúc ca sử dụng.
Ngoại lệ	3.1. Người khách có thể chọn thoát đăng kí bất kì lúc nào trong ca sử dụng để kết thúc ca sử dụng mà không đăng

	kí được tài khoản. 3.2. Người khách có thể xóa thông tin trong form để điền lại trước khi chọn đồng ý. 3.3. Nếu tên đăng nhập đã có, hoặc mật khẩu không khớp nhau: Hệ thống thông báo lỗi cho người sử dụng và trở lại bước 2.
Tần suất sử dụng	Thấp

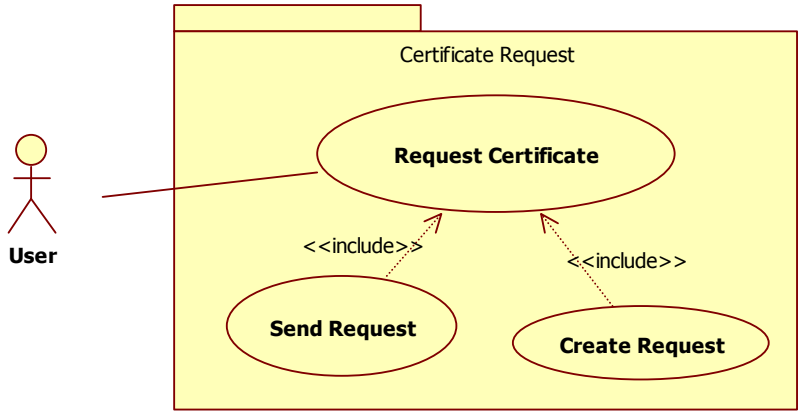
6.1.2. Login

Tên ca sử dụng	Đăng nhập
Tác nhân	Khách
Mô tả	Khách đăng nhập để sử dụng các chức năng của hệ thống
Tiền đề	Khách đã có tài khoản
Kết thúc thành công	Khách đăng nhập vào hệ thống và được sử dụng các quyền tương ứng của mình
Kết thúc thất bại	Khách không đăng nhập được vào hệ thống
Luồng sự kiện	1. Người khách chạy chương trình 2. Hệ thống hiển thị form đăng nhập 3. Người khách điền thông tin đăng nhập, quét vân tay để lấy mẫu vân tay, lựa chọn đồng ý đăng nhập. 4. Hệ thống kiểm tra thông tin đăng nhập, trích đặc trưng vân tay và đối sánh với các đặc trưng của người dùng đã lưu trong cơ sở dữ liệu để kiểm tra người dùng. 5. Nếu kiểm tra thấy đúng đúng thì người đó được đăng nhập vào hệ thống, trái lại sẽ báo lỗi.
Ngoại lệ	3.1. Nếu tên không tồn tại thì hệ thống báo lỗi và người khách quay lại bước 2. 3.2. Người khách có thể thoát khỏi quá trình Login bất kì lúc nào nếu chọn thoát từ form login. 3.3. Người khách có thể thay đổi thông tin đăng nhập bất kì lúc nào trước lúc chọn đồng ý đăng nhập.
Tần suất sử dụng	Cao

6.1.3. Logout

Tên ca sử dụng	Đăng xuất
Tác nhân	Người dùng
Mô tả	Người dùng thoát khỏi hệ thống khi kết thúc phiên làm việc
Tiền đề	Người dùng đã đăng nhập vào hệ thống
Kết quả	Người dùng ra khỏi hệ thống
Luồng sự kiện	Người dùng chọn "Thoát"
Ngoại lệ	Không có
Tần suất sử dụng	Cao

6.2 Các chức năng liên quan tới yêu cầu chứng chỉ



6.2.1. Tạo yêu cầu chứng chỉ

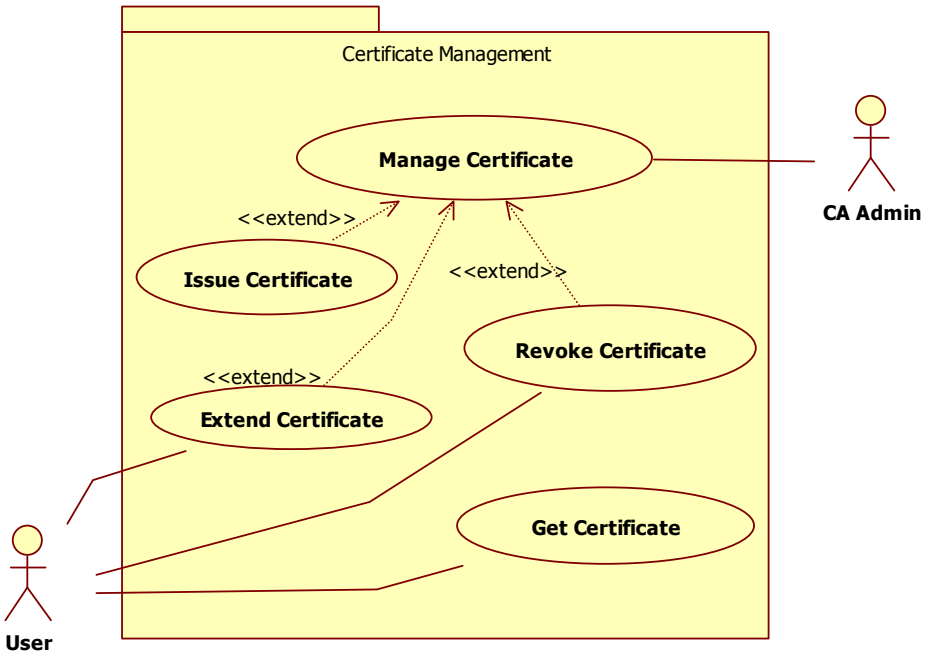
Tên ca sử dụng	Tạo yêu cầu chứng chỉ
Tác nhân	Người dùng của hệ thống
Mô tả	Người dùng tạo một yêu cầu xin cấp chứng chỉ cho bản thân theo định dạng X509.
Tiền đề	Người dùng đã Login vào hệ thống
Kết thúc thành công	Một yêu cầu chứng chỉ số theo chuẩn X509 được tạo ra
Kết thúc thất bại	Không tạo yêu cầu chứng chỉ số
Luồng sự kiện	1. Người dùng chọn tạo yêu cầu chứng chỉ từ giao diện của chương trình. 2. Hệ thống lấy thông tin chung về người dùng từ cơ sở dữ liệu.

	3. Hệ thống hiển thị form để người dùng nhập thông tin bổ sung ngoài thông tin về người dùng ở trên cho chứng chỉ. 4. Người dùng chọn kiểu chứng chỉ, có 3 kiểu: Chữ ký số, truy cập từ xa, mã hóa thông điệp. 5. Hệ thống sinh cặp khóa cá nhân và công khai cho người dùng 6. Hệ thống dùng đặc trưng vân tay mã hóa khóa cá nhân và lưu vào cơ sở dữ liệu. 7. Khóa cá nhân được dùng để kí lên yêu cầu 8. Yêu cầu được lưu vào cơ sở dữ liệu. Kết thúc thành công.
Ngoại lệ	
Tần suất sử dụng	Cao

6.2.2. Gửi yêu cầu chứng chỉ cho CA

Tên ca sử dụng	Gửi yêu cầu chứng chỉ cho CA
Tác nhân	Người dùng
Mô tả	Người dùng gửi yêu cầu cấp chứng chỉ lên cho CA duyệt cấp.
Tiền đề	RA đã kết nối với CA và đã có yêu cầu chứng chỉ của người dùng.
Kết thúc thành công	Yêu cầu chứng chỉ được gửi tới CA.
Kết thúc thất bại	Yêu cầu chứng chỉ không gửi tới được CA
Luồng sự kiện	1. Người dùng chọn gửi yêu cầu xin cấp chứng chỉ cho CA từ giao diện chương trình, nếu là chứng chỉ thuộc kiểu truy cập từ xa thì sẽ yêu cầu quét vân tay để lấy đặc trưng vân tay. 2. Hệ thống lấy yêu cầu cấp chứng chỉ số từ cơ sở dữ liệu và gửi lệnh yêu cầu cấp chứng chỉ cho CA 3. Hệ thống gửi yêu cầu cấp chứng chỉ cho CA qua kênh kết nối với CA. 4. RA nhận lại **mã yêu cầu** từ kênh kết nối với CA và lưu vào cơ sở dữ liệu. Kêt thúc thành công.
Ngoại lệ	Kết nối giữa CA và RA bị lỗi, kết thúc thất bại. Người dùng sẽ phải kích hoạt lại ca sử dụng.
Tần suất sử dụng	Cao

6.3 Các chức năng liên quan tới quản lý chứng chỉ



6.3.1 Phát hành chứng chỉ

Tên ca sử dụng	Phát hành chứng chỉ
Tác nhân	CA Admin
Mô tả	CA Admin chấp nhận một yêu cầu cấp chứng chỉ.
Tiền đề	Trong cơ sở dữ liệu đã chứa các yêu cầu cấp chứng chỉ
Kết thúc thành công	Một chứng chỉ số được CA kí xác nhận.
Kết thúc thất bại	Yêu cầu chứng chỉ không được kí xác nhận của CA.
Luồng sự kiện	1. CA Admin chọn một yêu cầu trong danh sách chờ cấp chứng chỉ trên form hiển thị danh sách của CA để cấp chứng chỉ.. 2. Hệ thống lấy yêu cầu cấp chứng chỉ từ trong cơ sở dữ liệu tương ứng với sự lựa chọn của CA Admin 3. Hệ thống hiển thị form chứa thông tin về yêu cầu chứng chỉ để CA Admin duyệt cấp. 4. CA Admin kiểm tra nội dung thông tin trên yêu cầu cấp chứng chỉ. 5. CA Admin chọn đồng ý cấp chứng chỉ. Nếu CA Admin chọn dừng thì kết thúc thất bại. 6. Hệ thống tạo chứng chỉ mới từ yêu cầu cấp này.

	7. Chứng chỉ mới được lưu vào cơ sở dữ liệu**.** 8. Yêu cầu được xóa khỏi danh sách chờ cấp. Giao diện được cập nhật. Kết thúc thành công..
Ngoại lệ	6.1. Nếu cặp khóa của chứng chỉ không hợp lệ thì kết thúc thất bại. 7.1. Nếu chứng chỉ không lưu được vào cơ sở dữ liệu thì kết thúc thất bại.
Tần suất sử dụng	Cao

6.3.2 Thu hồi chứng chỉ

Tên ca sử dụng	Thu hồi chứng chỉ
Tác nhân	Người dùng, CA.Admin
Mô tả	Khi người dùng yêu cầu hoặc khi CA Admin thấy cần thiết hủy bỏ hiệu lực của một chứng chỉ số đang lưu hành, CA Admin có thể hủy bỏ hiệu lực của chứng chỉ, đưa nó vào danh sách các chứng chỉ bị thu hồi.
Tiền đề	Chứng chỉ được yêu cầu thu hồi đã tồn tại. Có kết nối giữa RA và CA.
Kết thúc thành công	Chứng chỉ bị thu hồi, đưa vào danh sách CRL.
Kết thúc thất bại	Chứng chỉ không được đưa vào CRL.
Luồng sự kiện	1. Người dùng yêu cầu thu hồi chứng chỉ, hoặc CA Admin tự quyết định thu hồi chứng chỉ. 2. Nếu người dùng yêu cầu, RA sẽ gửi yêu cầu thu hồi chứng chỉ và số serial của chứng chỉ cần thu hồi lên CA. 3. Nếu CA Admin tự quyết định thu hồi, CA Admin sẽ chọn chứng chỉ thu hồi từ danh sách chứng chỉ trên giao diện của hệ thống. Hệ thống sẽ biết số serial chứng chỉ cần thu hồi. 4. Hệ thống đọc từ cơ sở dữ liệu ra chứng chỉ với số serial tương ứng, đánh dấu thu hồi chứng chỉ, chuyển chứng chỉ sang CRL. 5. CA gửi thông báo kết quả đã thu hồi chứng chỉ cho người dùng. Kết thúc thành công.
Ngoại lệ	4.1. Số serial không hợp lệ: số serial của chứng chỉ đã ở trong CRL, kết thúc thất bại. 4.2. CA Admin không đồng ý thu hồi chứng chỉ khi nhận được yêu cầu từ RA. CA sẽ gửi thông báo từ chối yêu cầu cho người dùng. Kết thúc thất bại.
Tần suất sử dụng	Trung bình

6.3.3 Gia hạn chứng chỉ

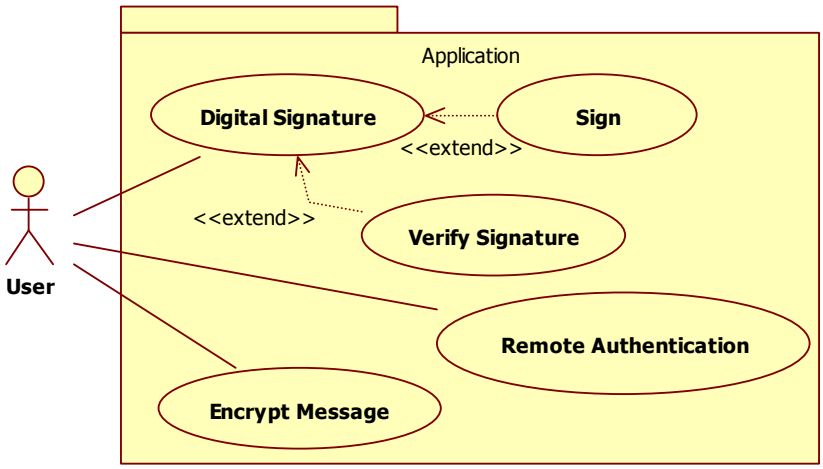
Tên ca sử dụng	Gia hạn chứng chỉ
Tác nhân	Người dùng, CA Admin.
Mô tả	Khi chứng chỉ hết hạn hoặc sắp hết hạn, người dùng yêu cầu CA gia hạn thời gian sử dụng chứng chỉ
Tiền đề	Có kết nối giữa RA và CA. Chứng chỉ đã tồn tại.
Kết thúc thành công	Chứng chỉ được gia hạn
Kết thúc thất bại	Chứng chỉ không được gia hạn
Luồng sự kiện	1. Người dùng chọn chứng chỉ cần gia hạn từ danh sách` chứng chỉ trên giao diện của chương trình. 2. Người dùng yêu cầu gia hạn chứng chỉ từ giao diện chương trình. 3. RA gửi yêu cầu gia hạn chứng chỉ & số serial của chứng chỉ cần gia hạn lên CA 4. CA nhận được yêu cầu thì gửi thông báo nhận được cho RA, thay đổi trạng thái chứng chỉ trong cơ sở dữ liệu thành “chứng chỉ chờ gia hạn”. 5. CA Admin quyết định có gia hạn cho chứng chỉ hay không 6. Nếu CA Admin không đồng ý gia hạn thì gửi thông báo từ chối cho người dùng. Kết thúc thất bại. 7. Nếu CA Admin đồng ý gia hạn thì chứng chỉ được gia hạn một năm kể từ thời điểm được gia hạn.. 8. CA cập nhật vào cơ sở dữ liệu nội dung và trạng thái của chứng chỉ, cập nhật trạng thái của chứng chỉ trên giao diện. Kết thúc thành công.
Ngoại lệ	
Tần suất sử dụng	Thấp

6.3.4 Lấy chứng chỉ để sử dụng

Tên ca sử dụng	Lấy chứng chỉ
Tác nhân	Người dùng
Mô tả	Người dùng yêu cầu lấy chứng chỉ từ CA.
Tiền đề	Có kết nối giữa CA và RA.
Kết thúc thành công	Người dùng nhận được chứng chỉ hoặc biết được chứng chỉ không được cấp hay không được gia hạn.
Kết thúc thất bại	Người dùng không nhận được chứng chỉ và cũng không biết được chứng chỉ có bị từ chối hay không.
Luồng sự kiện	1. Người dùng chọn yêu cầu chứng chỉ hoặc yêu cầu gia

	hạn từ giao diện của chương trình. 2. Người dùng chọn gửi lệnh yêu cầu lấy chứng chỉ lên CA từ giao diện của chương trình. 3. RA gửi lệnh lấy chứng chỉ cùng với mã yêu cầu nếu là chứng chỉ mới, hoặc cùng với số serial của chứng chỉ nếu là chứng chỉ gia hạn. 4. CA nhận yêu cầu. 5. Nếu cùng với lệnh lấy chứng chỉ là mã yêu cầu thì CA tìm trong cơ sở dữ liệu mã yêu cầu tương ứng xem chứng chỉ được cấp hay đang chờ cấp hoặc bị từ chối. 5.1. Nếu ứng với mã yêu cầu là chứng chỉ đang chờ cấp hoặc bị từ chối cấp thì CA trả lại thông báo về tình trạng của yêu cầu cho RA. Kết thúc thành công. 5.2. Nếu chứng chỉ đã được cấp thì CA gửi trả lời thông báo cho RA nhận chứng chỉ và gửi nội dung chứng chỉ về cho người dùng. Kết thúc thành công. 6. Nếu cùng với lệnh lấy chứng chỉ là số serial của chứng chỉ thì CA tìm trong cơ sở dữ liệu xem chứng chỉ ứng với số serial đó đang ở trạng thái nào. 6.1. Nếu chứng chỉ đã được gia hạn thì CA gửi lại cho RA. Kết thúc thành công. 6.2. Nếu chứng chỉ chưa được gia hạn thì CA gửi thông báo chưa được gia hạn cho RA. Kết thúc thành công.
Ngoại lệ	Mất kết nối giữa CA và RA trong quá trình gửi nhận thông điệp. Kết thúc thất bại.
Tần suất sử dụng	Cao

6.4. Các chức năng liên quan tới ứng dụng trên nền PKI



6.4.1. Tạo chữ kí số

Tên ca sử dụng	Tạo chữ kí số
Tác nhân	Người dùng của hệ thống
Mô tả	Người dùng dùng chứng chỉ để kí lên file, tạo ra chữ kí số.
Tiền đề	Người dùng đã Login vào hệ thống, đã có chứng chỉ được CA cấp.
Kết thúc thành công	Chữ kí số được tạo ra và đính kèm file được kí, có thể dùng để xác thực.
Kết thúc thất bại	Không tạo được chữ kí số.
Luồng sự kiện	1. Người dùng chọn một chứng chỉ dùng để kí từ danh sách các chứng chỉ dùng cho việc kí trên giao diện của hệ thống. 2. Người dùng kích hoạt chức năng kí của hệ thống bằng cách bấm nút kí trên giao diện. 3. Hệ thống lấy số serial number của chứng chỉ để chuẩn bị cho quá trình kí. 4. Hệ thống hiển thị hộp thoại cho người dùng chọn file để kí. 5. Người dùng chọn 1 file để kí. 6. Hệ thống băm nội dung của file đã được chọn. 7. Hệ thống lấy khóa cá nhân tương ứng với chứng chỉ dùng để kí từ cơ sở dữ liệu sau đó dùng khóa này mã hóa chuỗi băm từ file tạo thành chữ kí. 8. Chữ kí và các thông tin có liên quan được ghi kèm với file được kí vào một file mới. File này sau đó có thể dùng để xác thực với người dùng khác trong cùng hệ thống.

	9. Kết thúc thành công.
Ngoại lệ	Người dùng có thể dừng việc kí trong quá trình thực hiện ca sử dụng bất kì lúc nào trước lúc đồng ý chọn file được kí.
Tần suất sử dụng	

6.4.2. Xác thực chữ kí

Tên ca sử dụng	Kiểm tra chữ kí số
Tác nhân	Người dùng của hệ thống
Mô tả	Người dùng dùng kiểm tra một file cùng với chữ kí số đính kèm để xác thực người kí và sự toàn vẹn của file.
Tiền đề	Người dùng đã Login vào hệ thống, đã nhận được file có chữ kí số.
Kết thúc thành công	Xác thực được chữ kí số hoặc khẳng định được chữ kí số không khớp với nội dung của file và chứng chỉ dùng để kí.
Kết thúc thất bại	Không biết được chữ kí số có đúng hay không.
Luồng sự kiện	1. Người dùng kích hoạt chức năng kí của hệ thống bằng cách bấm nút kí trên giao diện. 2. Hệ thống hiển thị hộp thoại để người dùng chọn một file đã được kí. 3. Hệ thống tách file và chữ kí cùng với các thông tin liên quan ra. 4. Hệ thống dùng thông tin trong chữ kí và file để thực hiện quá trình kiểm tra chữ kí số. 5. Hệ thống kiểm tra tính hợp lệ của chứng chỉ dùng để kí. 6. Hệ thống băm file, dùng khóa công khai trong chứng chỉ kí để giải mã chữ kí và so sánh kết quả với mã băm của file. 7. Nếu chữ kí và file hợp lệ thì chữ kí được xác thực, trái lại thì không, kết thúc thành công.
Ngoại lệ	1.1. Người dùng có thể dừng việc kiểm tra trong quá trình thực hiện ca sử dụng bất kì lúc nào trước lúc đồng ý chọn file được kí. 2.1. Nếu file được chọn không fải là file đúng định dạng qui định trong hệ thống thì việc kiểm tra chữ kí thất bại. Ca sử dụng dừng lại.
Tần suất sử dụng	

6.4.3. Mã hóa thông điệp

a)**Tạo kênh gửi thông điệp**

Tên ca sử dụng	Tạo kênh gửi thông điệp
Tác nhân	Người dùng của hệ thống
Mô tả	Người dùng tạo kênh kết nối đến máy có user cần gửi,lấy public của chứng chỉ cần gửi
Tiền đề	Người dùng đã Login vào hệ thống, đã có chứng chỉ được CA cấp,đã biết cổng và địa chỉ IP của máy cần gửi
Kết thúc thành công	Tạo kênh chat thành công,lấy được public key chứng chỉ của người cần nhận.
Kết thúc thất bại	Không tạo được kênh chat hoặc không lấy được public key
Luồng sự kiện	1. Người dùng khởi tạo kênh kết nối 2. Nhập số Serial của chứng chỉ người được yêu cầu chat 3. Hệ thống lấy số serial number của chứng chỉ ,yêu cầu CA cấp cho chứng chỉ để sử dụng cho kênh chat 4. Hệ thống hiển thị hộp thoại chat
Ngoại lệ	
Tần suất sử dụng	

b) Bảo mật và lưu trữ thông điệp

Tên ca sử dụng	Bảo mật và lưu trữ
Tác nhân	Người dùng của hệ thống
Mô tả	Nhận được thông điệp,dùng private key của chứng chỉ tương ứng để giải mã,và dùng public key để mã hóa tin gửi đi
Tiền đề	Người dùng đã Login vào hệ thống, đã có chứng chỉ được CA cấp đồng kênh chat đã được lập thành công.
Kết thúc thành công	Mã hóa và giải mã thành công
Kết thúc thất bại	Giải mã lỗi hoặc không lưu được vào file
Luồng sự kiện	1. Hệ thống người gửi: nhận thông điệp, thêm time stamp vào đầu mỗi thông điệp+ tên user,rồi mã hóa cả cụm.Mỗi cụm mã hóa sẽ được thêm vào serial number ở đầu rồi gửi 2. Hệ thống người nhận : nhận được cả cụm gửi,tach lấy serial number,so sánh với serial number của chứng chỉ mình đang nắm,nếu trùng thì tách lấy phần tin mã hóa,dùng private key để giải mã,rồi đưa vào cửa sổ chát,nếu không trùng serial number thì lưu trữ vào file.
Ngoại lệ	Trong khi chat có thể hủy cửa sổ chat.
Tần suất sử dụng	

c)**Nhận tin nhắn offline**

Tên ca sử dụng	Nhận tin offline
Tác nhân	Người dùng của hệ thống
Mô tả	Người dùng đăng nhập hệ thống,tự hiện tin nhắn offline của người dùng
Tiền đề	Người dùng đã Login vào hệ thống, đã có chứng chỉ được CA cấp.
Kết thúc thành công	Giải mã và hiện tin thành công
Kết thúc thất bại	Không giải mã được
Luồng sự kiện	1. Người dùng đăng nhập hệ thống 2.Hệ thống kiểm tra trong số các chứng chỉ của người dùng,có chứng chỉ nào có tin nhắn được lưu ra file 3. Lấy privatekey tương ứng giải mã các tin nhắn 4. Hiển thị hộp thoại tin nhắn. 5. Xóa file lưu trữ.
Ngoại lệ	
Tần suất sử dụng	

6.4.4. Xác thực truy cập từ xa

Tên ca sử dụng	Nhận tin offline
Tác nhân	Người dùng của hệ thống
Mô tả	Người dùng muốn truy cập vào máy Database Server, và được CA xác thực, có sử dụng sinh trắc học vân tay.
Tiền đề	Người dùng đã Login vào hệ thống, đã có chứng chỉ thuộc kiểu truy cập từ xa được CA cấp. Có một DB Server đã đăng ký trước với CA.
Kết thúc thành công	Người dùng truy cập thành công vào DB Server và sở hữu 1 khóa phiên để thực hiện giao dịch trong phiên đó với DB Server.
Kết thúc thất bại	Không được phép truy nhập vào DB Server.
Luồng sự kiện	1. Đầu tiên User gửi yêu cầu muốn thực hiện truy cập từ xa lên CA bằng cách gửi kèm theo số Serial Number của chứng chỉ tương ứng và ID của DB Server mà User muốn thực hiện truy cập từ xa. 2. CA nhận được thông tin, dựa vào số SN đó, truy vấn vào CSDL của CA để lấy ra được chứng chỉ tương ứng. 3. CA sinh ra một khóa phiên ngẫu nhiên. 4. CA mã hóa khóa phiên bằng Public key (của User đó) và gửi đến cho User.

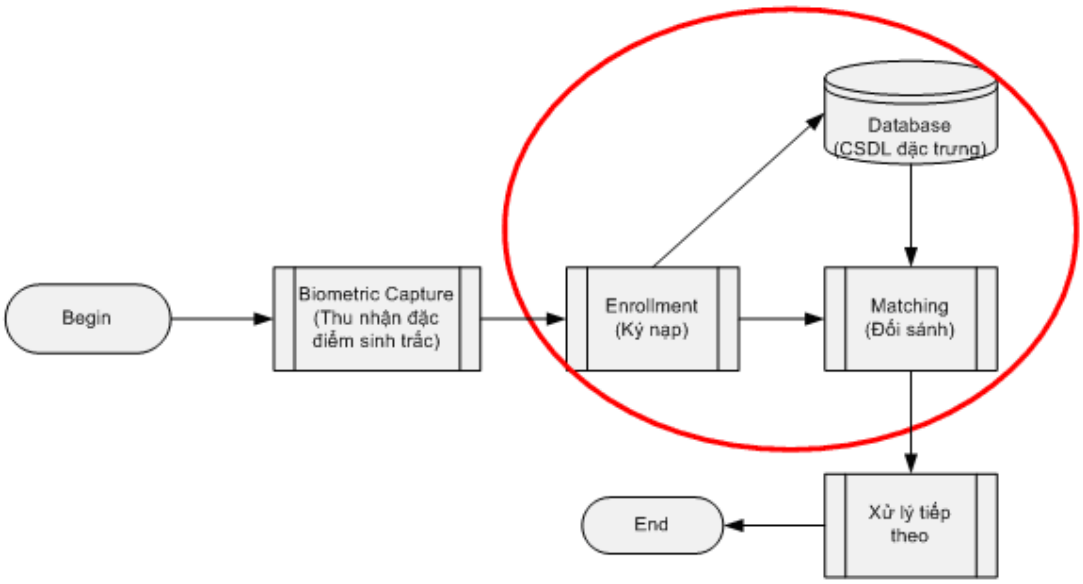
	5. User nhận được sẽ dùng Private key của mình để giải mã ra được khóa phiên. 6. User thực hiện quét vân tay để có được đặc trưng vân tay. 7. Mã hóa đặc trưng vân tay bằng khóa phiên và gửi đi cho CA. 8. CA dùng khóa phiên để giải mã và lấy ra được đặc trưng vân tay. 9. CA sẽ truy vấn vào CSDL và lấy ra được thông tin đặc trưng vân tay (mà User này đã gửi lên từ lúc đăng ký xin cấp chứng chỉ), CA sẽ thực hiện đối sánh vân tay và đưa ra kết quả chấp nhận hay không chấp nhận. 10. Nếu kết quả là không chấp nhận thì CA gửi thông báo cho User là không chấp nhận và dừng tiến trình. 11. Nếu kết quả là chấp nhận, CA sẽ gửi thông báo chấp nhận cho User. 12. CA lúc này cũng sẽ mã hóa khóa phiên bằng Public key của DB Server và gửi cho DB Server tương ứng. Từ lúc này trở đi, CA không còn tham gia vào kịch bản nữa. 13. User sau khi nhận được thông tin xác thực thành công của CA, sẽ mã hóa mật khẩu (mà có đăng ký với DB Server từ lúc đầu) bằng khóa phiên và gửi đến cho DB Server. 14. DB Server nhận từ CA khóa phiên được mã hóa bằng public key, sẽ dùng private key của mình để giải mã và lấy ra được khóa phiên. 15. Khi nhận được thông tin từ User, sẽ dùng khóa phiên để giải mã ra được mật khẩu, và truy vấn vào CSDL để xác thực mật khẩu (so sánh thông tin đã băm rồi được lưu trong CSDL). 16. Sau đó gửi thông tin xác thực về cho User. 17. Kể từ đây bắt đầu phiên giao dịch giữa DB Server và User, mọi thông tin gửi đi trên đường truyền đều được mã hóa bằng khóa phiên đó. 18. Sau khi kết thúc phiên giao dịch, DB Server sẽ xóa thông tin khóa phiên đó đi.
Ngoại lệ	
Tần suất sử dụng	Thấp

7. CHƯƠNG TRÌNH THỬ NGHIỆM THẨM ĐỊNH SINH TRẮC LÒNG BÀN TAY (PALMPRINT)

1. Giới thiệu về hệ thống

Một mô hình hệ thống an ninh sinh trắc có mô hình như hình 1.1. Trong đó có các quá trình:

- Thu nhận đặc điểm sinh trắc: như ảnh, ghi âm giọng nói, ….
- Ký nạp: là quá trình tách các đặc trưng sinh trắc, có thể thực hiện mã hóa rồi lưu vào cơ sở dữ liệu.
- Đối sánh: là quá trình "so sánh" mẫu đặc trưng trong CSDL với mẫu sinh trắc lấy vào sau này, để xác định có phải là người đó hay không?

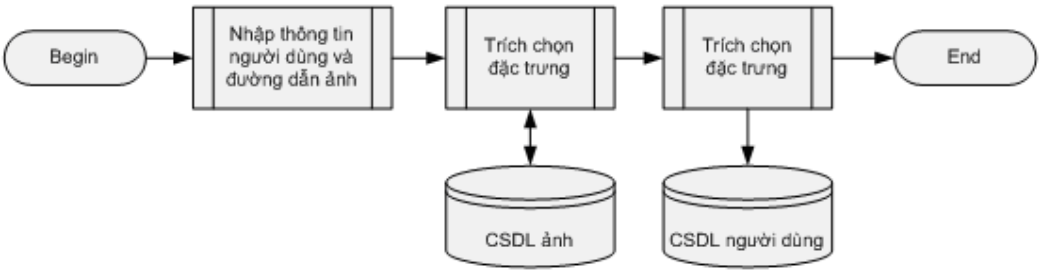


Hình 1.1. Quá trình của một hệ an ninh sinh trắc

Hệ thống thẩm định sinh trắc lòng bàn tay này sẽ được xây dựng dựa trên 2 pha chính: Đăng **Ký nạp (Enrollment)** và **Đối sánh (Matching).**

Đăng ký (Hình 1.2)

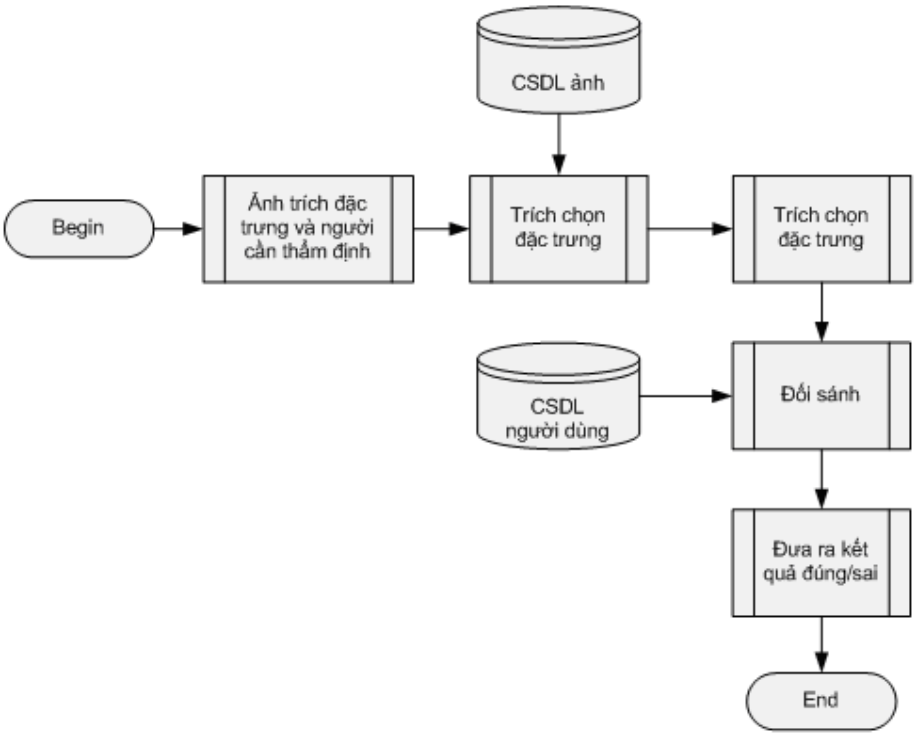
Quá trình ký nạp là quá trình nhập thông tin người sử dụng cũng như đưa ảnh lòng bàn tay vào. Hệ thống thực hiện trích các đặc trưng sinh trắc từ ảnh lòng bàn tay. Đối với thuật toán hệ thống thực hiện trích 4 loại đặc trưng khác nhau liên quan đến khoảng cách, cấu trúc và đường bàn tay. Cuối cùng hệ thống lưu những đặc trưng và thông tin người dùng vào CSDL.



Hình 1.2. Quá trình đăng ký người dùng

Đối sánh (Hình 1.3)

Ở pha này, các đặc trưng ở hình ảnh thu nhận sẽ được đem đối sánh với cơ sở dữ liệu có sẵn thông qua quá trình đăng ký. Quá trình đối sánh có thể thực hiện theo nhiều cách như so sánh độ sai khác về tọa độ, khoảng cách,…. Kết quả sẽ được trả lời ở đầu ra dưới dạng 'đúng' hoặc 'sai' (tương ứng với việc hệ thống xác định rằng thông tin sinh trắc có phải của người đó hay không)



Hình 1.3. Quá trình thẩm định người dùng

2. Chương trình palmprint

Ngôn ngữ

- Hiện tại chương trình được xây dựng dựa trên 2 ngôn ngữ là C# và Matlab 7.8

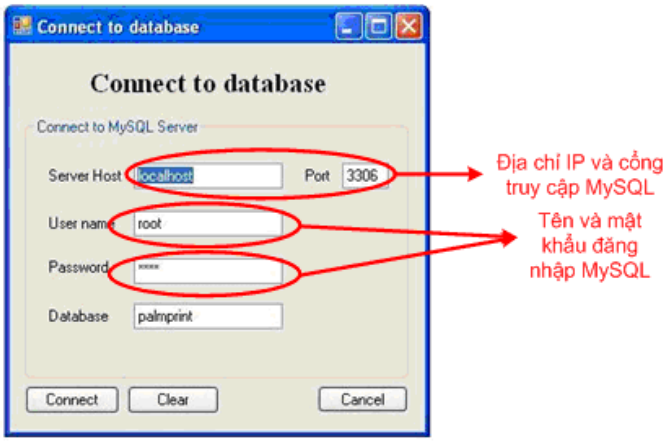
Cách cài đặt

- Cài đặt chương trình chính
- Cài đặt MCR (Matlab Compiler Runtime) 7.8
- Cài đặt .Net Framework 2.0

- Cài đặt MySQL Server 5.0 trở lên
- Cài đặt MySQL Connector 5.0 trở lên

Cách hoạt động của chương trình:

- **Kết nối CSDL:** là quá trình kết nối với cơ sở dữ liệu (ở đây chương trình dùng cơ sở dữ liệu MySQL) (hình 2.1). Các quá trình để kết nối với CSDL bao gồm các bước:
  - **Bước 1**: Nhập địa chỉ IP và cổng của MySQL. Thông thường địa chỉ Server là localhost (ngay tại máy cá nhân), cổng mặc định là 3306. Điều này cần chú ý khi cài MySQL Server.
  - **Bước 2**: Nhập user name và password để truy cập vào cơ sở dữ liệu MySQL.
  - **Bước 3:** Nhập tên CSDL chứa cơ sở dữ liệu về đặc trưng lòng bàn tay của người sử dụng. Chương trình có thể tạo mới một CSDL nếu chưa tồn tại hoặc truy cập vào một CSDL đã có

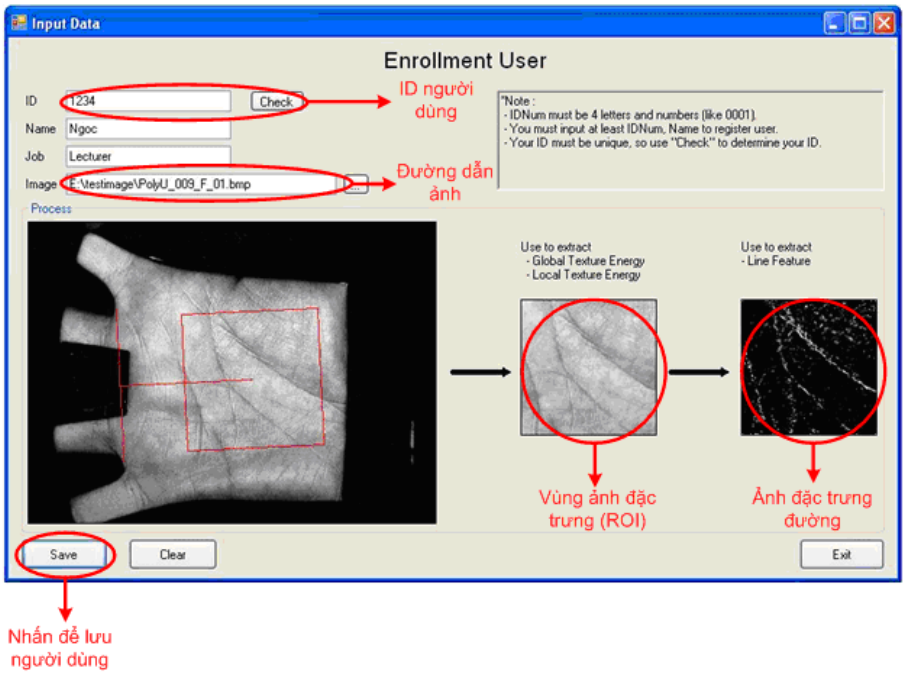


Hình 2.1. Màn hình kết nối CSDL

- Sau khi kết nối thành công với CSDL, chương trình sẽ chạy màn hình chính của chương trình bao gồm 3 chức năng là **Enrollment, Verify và Delete User** như hình dưới đây. Trong đó 2 chức năng chính của chương trình là **Enrollment (ký nạp người dùng)** và **Verify (thẩm định)**
  - **Enrollment (ký nạp người dùng):** là pha dùng để ghi nhận người dùng vào hệ thống cùng những thông tin sinh trắc thu nhận được
  - **Verify (thẩm định):** là pha dùng để thẩm định người dùng. Thực hiện lấy một ảnh đầu vào (chọn ảnh đã có), trích đặc trưng và so sánh với đặc trưng của người sử dụng đã có trong CSDL
  - **Delete User (xóa người dùng):** thực hiện xóa người sử dụng khỏi hệ thống hoặc xóa toàn bộ CSDL.
  - **Exit:** thoát chương trình.

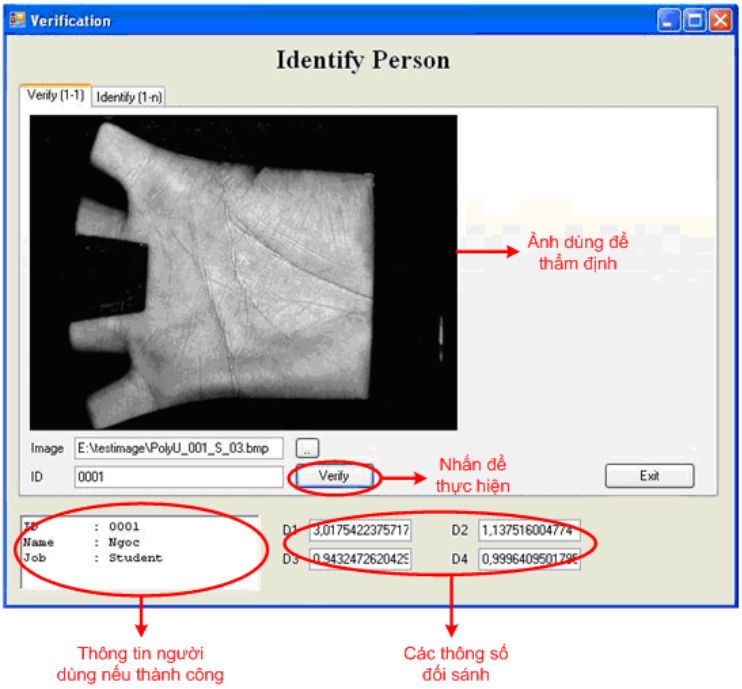
- **Enrollment (Ký nạp người dùng)**: thực hiện lưu người dùng và thông tin sinh trắc người đó vào hệ CSDL (Hình 2.2). Nó bao gồm các bước như sau:

- **Bước 1:** Nhập thông tin người dùng bao gồm các thông tin về ID, tên, nghề nghiệp. Trong đó thông tin về ID là phải duy nhất (có thực hiện kiểm soát tính duy nhất)
- **Bước 2:** Nhập đường dẫn ảnh lòng bàn tay người đó. Có thể chọn ảnh thông qua nút chọn file ở bên cạnh
- **Bước 3:** Nhấn nút Save để bắt đầu quá trình thực hiện. Chương trình sẽ thực hiện trích đặc trưng, lưu thông tin người đó và thông tin đặc trưng vào CSDL
    - Nếu thực hiện thành công, chương trình sẽ thông báo thành công (Successful).
    - Nếu ảnh bị lỗi, chương trình sẽ thông báo không trích được đặc trưng.



Hình 2.2. Màn hình đăng ký người dùng

- **Verify (thẩm định):** thẩm định xem ảnh lòng bàn tay đầu vào có phải là của một người nào đấy hay không (hình 2.3)
    - **Bước 1:** Nhập ID của người sử dụng cần thẩm định
    - **Bước 2:** Nhập đường dẫn ảnh lòng bàn tay cần trích đặc trưng (có thể chọn qua tính năng chọn bên cạnh)
    - **Bước 3:** Chương trình trích đặc trưng từ ảnh đầu vào
    - **Bước 4:** Chương trình thực hiện đối sánh đặc trưng trích được với đặc trưng của người có ID đã cho
        - Nếu kết quả đúng → đưa ra kết quả có đúng người đó hay không (nếu đúng đưa ra thông tin của người đó)
        - Nếu sai → chương trình báo không phải người đó



Hình 2.3. Màn hình thẩm định người dùng

- **Delete User (xóa người dùng):** thực hiện xóa người dùng khỏi CSDL
    - Chọn để hiện danh sách người sử dụng trong CSDL (viewList) bao gồm ID và tên mỗi người sử dụng (Xem hình dưới)
    - Nhập ID và/hoặc tên người sử dụng
        - Có thể chỉ cần nhập hoặc ID người sử dụng hoặc tên người sử dụng là đủ
        - Nếu nhập cả 2, chương trình thực hiện kiểm tra cả tên và ID, nếu cả 2 cùng trùng thì mới thực hiện xóa
        - Lưu ý: khi nhập tên, nếu có 2 người trùng tên, chương trình sẽ xóa cả 2 người sử dụng
    - Thực hiện xóa người sử dụng theo tên/ID đã có
        - Thực hiện xóa người sử dụng
        - Nếu người sử dụng không tồn tại, chương trình thông báo không tồn tại người dùng
        - Nếu quá trình xóa bị lỗi, chương trình thông báo lỗi

3. Hướng phát triển của hệ thống

- Hạn chế lớn nhất hiện tại của hệ thống chính là khả năng lấy ảnh trực tiếp từ thiết bị. Trong tương lai, hệ thống được phát triển để thực hiện lấy ảnh lòng bàn tay và xử lý trực tiếp từ thiết bị thu nhận.
- Mặc dù kết quả thuật toán khá tốt (các tỉ lệ sai sót nhỏ hơn 10%) nhưng để tăng tính khả thi cho hệ thống thì thuật toán trích đặc trưng và thẩm định cần được cải tiến để tăng độ chính xác cho hệ thống

- Đối với những đặc trưng từ ảnh lòng bàn tay, hiện tại hệ thống lưu trực tiếp những đặc trưng đó vào CSDL. Việc này tạo ra nguy cơ lớn khi truy cập CSDL từ xa hoặc máy tính bị xâm nhập. Do đó một vấn đề quan trọng là cần mã hóa những đặc trưng này trước khi lưu hay truyền đi nhằm hạn chế tối đa khả năng bị mất hoặc lộ thông tin đặc trưng sinh trắc.
- Ngôn ngữ hiện tại thực hiện là C# và Matlab. Trong thời gian tới, hệ thống chuyển sang dùng ngôn ngữ VC để thuận tiện cho quá trình nghiên cứu tích hợp vào hệ thống BioPKI cũng như kết hợp đa sinh trắc

4. Kết luận

Bản báo cáo đã mô tả khá đầy đủ hệ thống thẩm định sinh trắc lòng bàn tay ở thời điểm hiện tại, những gì đã đạt được cũng như những hạn chế. Ngoài ra báo cáo còn trình bày những mục đích phát triển tiếp theo của hệ thống giúp hệ thống hoạt động chính xác hơn và đưa vào hệ thống BioPKI

TÀI LIỆU THAM KHẢO

[1] David D.Zang “Palmprint Authentication”, Kluwer Academic Publishers, 2004 – Tài liệu chính cho thuật toán của hệ thống

[2] Palmprint Image Database PolyU II: http://www.comp.polyu.edu.hk – Nơi có CSDL ảnh về lòng bàn tay

[3] Detection Edge Algorithms: http://www.cim.mcgill.ca/~dparks/CornerDetector/index.htm

[4] Jain, A. K. (28-30 April 2004), "Biometric recognition: how do I know who you are?", Signal Processing and Communications Applications Conference, 2004

BỘ GIÁO DỤC VÀ ĐÀO TẠO
Trường Đại học Bách khoa Hà Nội

BÁO CÁO TÓM TẮT

Đề tài nhiệm vụ theo nghị định thư

Hệ thống an ninh thông tin dựa trên sinh trắc học Bio-PKI (Bio-PKI Based Information Security System)

Mã số: 12/2006/HĐ-NĐT

Chủ nhiệm đề tài

PGS. TS Nguyễn Thị Hoàng Lan
Khoa Công nghệ thông tin,
Đại học Bách khoa Hà Nội

Hà Nội 1 - 2009

Mục lục

DANH SÁCH CÁC CÁN BỘ VÀ SINH VIÊN THAM GIA THỰC HIỆN ĐỀ TÀI

A. DANH SÁCH CÁC CÁN BỘ THAM GIA TRỰC TIẾP

1. PGS.TS Nguyễn Thị Hoàng Lan	Khoa CNTT, ĐHBK HN, chủ nhiệm đề tài
2. TS Nguyễn Linh Giang	Khoa CNTT, ĐHBK HN
3. TS Hà Quốc Trung	Khoa CNTT, ĐHBK HN
4. ThS Bàng Quỳnh Mai	Khoa CNTT, ĐHBK HN
5. ThS Nguyễn Anh Hoàn	Khoa CNTT, ĐHBK HN
6. TS Ngô Hồng Sơn	Khoa CNTT, ĐHBK HN
7. KS Nguyễn Thị Hiền	Khoa CNTT, ĐHBK HN

B. DANH SÁCH CÁC CÁN BỘ THAM GIA TƯ VẤN

1. PGS. TS Đặng Văn Chuyết	Khoa CNTT, ĐHBK HN
2. ThS Đỗ Văn Uy	Khoa CNTT, ĐHBK HN
3. ThS Ngô Minh Dũng	Viện Khoa học hình sự, Bộ Công An

C. DANH SÁCH CÁC SINH VIÊN THAM GIA THỰC HIỆN ĐỀ TÀI

C1. Các sinh viên đại học

Tất cả các sinh viên đại học tham gia đề tài dưới đây đều đã hoàn đồ án tốt nghiệm theo hướng đề tài và đạt kết quả loại khá hoặcgiỏi.

Danh sách nhóm sinh viên K46 tham gia đề tài:

1.	Lê Anh Tuấn	TTM K46
2.	Ngô Trọng Cảnh	TTM
3.	Nguyễn Sinh Chung	Tin Pháp
4.	Nguyễn Văn Hạnh	KSCLC

Danh sách nhóm sinh viên K47 tham gia đề tài:

1.	Nguyễn Thạc Hiếu	TTM K47
2.	Nguyễn Quang Thụ	TTM
3.	Phạm Quang Thịnh	TTM
4.	Nguyễn Hoàng Anh	Tin Pháp
5.	Phạm Sỹ Lâm	KSCLC

Danh sách nhóm sinh viên K48 tham gia thiết kế phát triển hệ thống BioPKI và tham gia viết báo cáo tổng hợp đề tài:

1.	Lê Tiến Dũng (trưởng nhóm)	TTM K48
2.	Bùi Thành Đạt	TTM
3.	Nguyễn Thị Thu Hằng	KSTN
4.	Trần Hải Anh	Tin Pháp
5.	Dương Văn Đô	Tin Pháp
6.	Hoàng Trần Đức	TTM
7.	Ngô Tiến Dũng	TTM
8.	Trần Nguyên Ngọc	TTM

C2. Các sinh viên cao học

1. Trần Tuấn Vinh	Cao học CNTT - khóa 2003-2005 đã bảo vệ 2006
2. Nguyễn Anh Tài	Cao học CNTT - khóa 2004-2006 đã bảo vệ 2006
3. Vũ Thanh Thắng	Cao học CNTT - khóa 2005-2007 đã bảo vệ 12- 2007
4. Lê Quang Tùng	Cao học CNTT - khóa 2006-2008 đã bảo vệ 11- 2008
5. Lê Trần Vũ Anh	Cao học CNTT - khóa 2006-2008 đã bảo vệ 11- 2008
6. Hà Tiến Dũng	Cao học CNTT - khóa 2006-2008 đã bảo vệ 11- 2008

I. THÔNG TIN CHUNG VỀ ĐỀ TÀI

1. Tên đề tài

Hệ thống an ninh thông tin dựa trên sinh trắc học Bio-PKI
(Bio-PKI Based Information Security System)
Mã số: 12/ 2006/ HĐ-NĐT

2. Chủ nhiệm đề tài: PGS. TS Nguyễn Thị Hoàng Lan

Học hàm, học vị, chuyên môn: PGS.TS ngành Công nghệ Thông tin
Chức danh: Phó Trưởng khoa Công nghệ Thông tin, Đại học Bách Khoa Hà Nội
Điện thoại cơ quan: (84. 4) 38.68.25.96
Điện thoại nhà riêng: (84. 4) 38.32.89.25
Email: lannth@it-hut.edu.vn

3. Cơ quan chủ trì

Đại học Bách Khoa Hà Nội, Khoa Công nghệ Thông tin
Số 1 đường Đại Cồ Việt, Hà Nội

4. Họ và tên Chủ nhiệm phía đối tác nước ngoài:

TS. Ong Thian Song
Chức danh: Giám đốc điều hành Trung tâm nghiên cứu Sinh trắc học (CBB)
Trường Đại học Đa phương tiện Malaysia (MMU)
Tel: +606-252.33.43
Fax: +606-231.88.40
Emal: tsong@mmu.edu.vn

5. Cơ quan đối tác nước ngoài: Trường Đại học Đa phương tiện Malaysia
(Malaysia Multimedia University -MMU),
Trung tâm nghiên cứu Sinh trắc học và Sinh –Tin học (Center of Biometrics and Bioinformatics – CBB)
Khoa Khoa học và Công nghệ thông tin (Faculty of Information Science and Technology - FIST)
Malaysia Multimedia University (MMU),
Jalan Ayer Keroh Lama, 75450 Melaka Malaysia
http:///www.mmu.edu.my

6. Thời gian thực hiện đề tài: Từ 6/2006 đến 6/2008

7. Tổng kinh phí thực hiện đề tài: 800.000.000 VNĐ
Tổng kinh phí đã cấp 2006: 450.000.000 VNĐ
Tổng kinh phí đã cấp 2007: 350.000.000 VNĐ
Đề tài đã nhận được cấp đủ kinh phí đến 2008.

II. TÍNH CẤP THIẾT CỦA ĐỀ TÀI

Những năm cuối của thế kỷ XX và đầu thế kỷ XXI chứng kiến sự lớn mạnh vượt bậc của mạng Internet cả về quy mô và chất lượng. Internet được ứng dụng rộng rãi trên toàn thế giới ở mọi ngành nghề, lĩnh vực kinh tế, xã hội và an ninh. Tính phổ biến rộng rãi khiến Internet đã và đang là nền tảng cơ sở cho các giao dịch thương mại toàn cầu và các ứng dụng của giao dịch điện tử tạo thành một hình thức "xã hội ảo" với các đặc trưng riêng biệt. Đặc trưng của Internet là tính "ảo" và tính tự do tránh bị điều chỉnh bởi luật pháp, mọi người đều có thể tham gia và ít để lại dấu vết cá nhân của mình. Việc xác thực mỗi cá nhân qua mạng thông thường chỉ sử dụng password là khó khăn, nên nguy cơ xảy ra giả mạo định danh, bị lừa đảo trực tuyến là rất cao. Đây là vừa là điểm mạnh và cũng là điểm yếu của giao dịch điện tử qua mạng Internet. Trong điều kiện công nghệ thông tin và truyền thông phát triển vấn đề bảo mật an toàn thông tin và an ninh mạng là một trong những vấn đề thời sự cấp bách đang được nhiều quốc gia quan tâm về cả phương diện pháp lý ,về cả phương diện kỹ thuật và công nghệ.

Trong những năm gần đây các tội phạm công nghệ cao ngày càng gia tăng, vấn đề nghiên cứu các giải pháp nhằm đảm bảo an toàn thông tin, bảo mật dữ liệu trong các giao dịch điện tử qua môi trường mạng càng trở nên cấp thiết. Mặc dù đã có nhiều giải pháp đã được nghiên cứu và phát triển, nhiều sản phẩm công nghệ đã được nghiên cứu và ứng dụng, tuy nhiên vấn này vẫn luôn là vấn đề thời sự và thách thức. Giải pháp an ninh dựa trên các dấu hiệu sinh trắc học là một trong các hướng nghiên cứu mới đang được thế giới quan tâm phát triển và áp dụng.

III. MỤC TIÊU VÀ YÊU CẦU CỦA ĐỀ TÀI NHIỆM VỤ NGHỊ ĐỊNH THƯ

Nghiên cứu hệ thống an ninh thông tin (BioPKI Based Information Security System) dựa trên sự kết hợp các đặc trưng sinh trắc học con người với hạ tầng cơ sở bảo mật khóa công khai PKI là hướng nghiên cứu mới cho phép mang lại những ưu điểm hơn các hệ thống PKI hiện có về độ an toàn bảo mật, về tính xác thực thẩm định chủ thể con người trong các giao dịch điện tử qua mạng máy tính. Mục tiêu của đề tài nhiệm vụ theo nghị định thư hợp tác với Malaysia theo định hướng nghiên cứu vấn đề này.

III.1. Mục tiêu của nhiệm vụ đề tài

- Nghiên cứu đề xuất phương án kết hợp các đặc trưng của vân tay với mã bảo mật khóa công khai PKI tạo khóa mã sinh trắc, một giải pháp cho hệ BioPKI.
- Xây dựng thử nghiệm hạ tầng cơ sở hệ thống an ninh thông tin dựa BioPKI (protoptype). Thiết kế và xây dựng thử nghiệm phần mềm hệ thống BioPKI dựa trên mã sinh trắc học nhằm hướng tới các ứng dụng trong thẩm định xác thực sinh trắc học và kiểm soát truy cập dùng trong các lĩnh vực an ninh, thương mại điện tử, ngân hàng, giao dịch điện tử, chính phủ điện tử….
- Kết hợp nghiên cứu của 2 phía Việt Nam và Malaysia, thử nghiệm phát triển ứng dụng hệ thống BioPKI.

III.2. Tóm tắt các yêu cầu sản phẩm của đề tài đã đăng ký trong thuyết minh nhiệm vụ (kết quả dạng II và III)

Tên sản phẩm:

Hệ thống an ninh thông tin dựa trên mã sinh trắc học Bio-PKI (gọi tắt là Hệ thống an ninh thông tin Bio-PKI)

Các sản phẩm kết quả bao gồm:

- Kết quả giải pháp tích hợp đặc trưng vân tay với mã bảo mật trong hệ PKI thành hệ BioPKI.
- Kết quả thử nghiệm Prototype về hạ tầng hệ thống BioPKI để thẩm định xác thực vân tay trong hệ BioPKI.
- Kết quả phần mềm máy tính cho hệ thống BioPKI, hệ sinh trắc bao gồm: phần mềm đăng ký, mã hóa khóa sinh trắc vân tay BioPKI và phần mềm thẩm định xác thực vân tay.
- Các báo cáo: Báo cáo phân tích thiết kế hệ thống và hướng ứng dụng trong thẩm định xác thực vân tay trong các giao dịch điện tử, kiểm soát truy nhập; Các báo cáo định kỳ và báo cáo tổng hợp đề tài.

IV. NỘI DUNG NGHIÊN CỨU

IV.1. Nghiên cứu tổng quan

Nội dung phần này được trình bày trong 3 chương của báo cáo tổng hợp bao gồm các nghiên cứu tổng quan, tổng hợp các tài liệu nghiên cứu từ các bài báo và tài liệu trên thế giới những năm gần đây về các lĩnh vực liên quan đến mục tiêu nhiệm vụ đề tài.

- Khảo sát về giao dịch điện tử, các yêu cầu an ninh thông tin trong giao dịch điện tử qua mạng.
    - Khảo sát về thương mại điện tử, giao dịch điện tử trên thế giới
    - Tình hình phát triển các giao dịch điện tử ở Việt Nam và cơ sở pháp lý
    - Nhu cầu về an toàn bảo mật thông tin trong giao dịch điện tử
    - Khái quát về các giải pháp công nghệ bảo mật an toàn thông tin và an ninh mạng
- Sinh trắc học và hệ thống an ninh bảo mật thông tin dựa trên sinh trắc học
    - Tổng quan về sinh trắc học và hệ thống sinh trắc học (Biometric System)
    - Đánh giá hiệu năng và chất lượng hoạt động của hệ sinh trắc học
    - Hệ thống an ninh bảo mật dựa trên trắc học (Biometric based Security System)
- Cơ sở hạ tầng khóa công khai PKI và vấn đề an toàn trong hệ thống PKI
    - Hệ mật mã khóa công khai
    - Cơ sở hạ tầng khóa công khai (Public Key Infrastructure)
    - Các giao dịch điện tử trong hạ tầng khóa công khai và vấn đề an toàn thông tin

IV.2. Xây dựng mô hình giải pháp

Nghiên cứu phân tích các hướng tiếp cận BioPKI kết hợp xác thực sinh trắc với cơ sở hạ tầng khóa công khai PKI và xây dựng mô hình giải pháp hệ thống BioPKI, nội dung chi tiết phần này được trình bày trong chương 4 của báo cáo tổng hợp, bao gồm các phần sau:

- Nghiên cứu phân tích các hướng tiếp cận hệ thống BioPKI theo các tài liệu nghiên cứu
  - Giải pháp 1: đối sánh đặc trưng sinh trắc thay mật khẩu để xác thực chủ thể
  - Giải pháp 2: kết hợp kỹ thuật nhận dạng sinh trắc với kỹ thuật mật mã, mã hóa bảo mật khóa cá nhân
  - Giải pháp 3: dùng sinh trắc học để sinh khóa cá nhân.
- Đề xuất mô hình tích hợp hệ sinh trắc vân tay kết hợp giải pháp 1 và giải pháp 2 vào hạ tầng khóa công khai PKI thành hệ BK-BioPKI.
- Đề xuất giải pháp công nghệ xây dựng hệ thống BK-BioPKI của đề tài trên cơ sở xây dựng hệ lõi PKI dùng OpenSSL kết hợp với phần mềm hệ thống thẩm định xác thực sinh trắc vân tay sống trực tuyến dùng thiết bị quét thông dụng, giá thành thấp, dễ khả thi, dùng ngôn ngữ C++ kết hợp với Matlab.

IV.3. Phân tích thiết kế hệ thống BioPKI và xây dựng phần mềm cơ sở hệ thống BioPKI

Phần phân tích thiết kế xây dựng hệ thống BK-BioPKI được trình bày chi tiết trong các chương 5, 6, 7 của Báo cáo tổng hợp, gồm các nội dung chính dưới đây:

- Phân tích thiết kế và xây dựng phần mềm hệ xác thực sinh trắc vân tay trong hệ BK-BioPKI:
  - Phân tích thiết kế và xây dựng phần mềm phân hệ sinh trắc 1 (theo giải pháp 1): Hệ thẩm định đặc trưng vân tay sống trực tuyến trong hệ thống BK-BioPKI
  - Phân tích thiết kế và xây dựng phần mềm phân hệ sinh trắc 2 (theo giải pháp 2): Hệ sinh khóa sinh trắc, mã hóa bảo mật khóa cá nhân trong hệ BK-BioPKI.
- Phân tích thiết kế xây dựng hệ thống hạ tầng khóa công khai PKI trên môi trường OpenSSL và các giao dịch cơ sở trong hệ thống BK-BioPKI:
  - Phân tích thiết kế các thành phần chức năng của hệ thống BK-BioPKI
  - Thiết kế xây dựng và lập trình phần mềm cơ sở các chức năng hoạt động hệ thống BK-BioPKI. Thiết kế các tình huống giao dịch và xây dựng các giao thức trong các giao dịch
  - Thiết kế và lập trình cài đặt các thành phần chính phần mềm cơ sở và các giao thức, giao dịch cơ sở của hệ thống BK-BioPKI, bao gồm:
    - Thiết lập hệ thống CA, RA, khởi động hoạt động,
    - Quản lý chứng chỉ (CA): cấp mới, gia hạn, thu hồi chứng chỉ
    - Đăng ký người dùng (user)

- Thiết kế xây dựng và lập trình phần mềm tại máy người dùng trong hệ thống BK-BioPKI bao gồm các chức năng chủ yếu sau:
  - Thiết lập RA
  - Đăng nhập, đăng xuất chương trình
  - Xin cấp chứng chỉ
  - Xin gia hạn chứng chỉ
  - Xin thu hồi chứng chỉ
  - Sử dụng chứng chỉ trong các giao dịch (chữ ký số, bảo mật thông điệp)
  - Quản lý người dùng: đăng kí, sửa đổi, xóa bỏ người dùng.

- Thiết kế tích hợp toàn bộ hệ thống an ninh thông tin BK-BioPKI và thử nghiệm
  - Xây dựng hệ thống theo mô hình đã đề xuất gồm 2 phân hệ sinh trắc vân tay tích hợp vào cơ sở hạ tầng PKI thành hệ BK-BioPKI trong hoạt động sau:
    - Phân hệ sinh trắc 1, đối sánh đặc trưng sinh trắc thay mật khẩu để xác thực chủ thể được tích hợp vào hoạt động đăng nhập của hệ BK-BioPKI
    - Phân hệ sinh trắc 2, sinh khóa sinh trắc hợp mật mã bảo vệ khóa cá nhân được tích hợp vào trong các giao dịch xin cấp chứng chỉ và sử dụng chứng chỉ trong hệ BK-BioPKI
  - Thiết kế cài đặt tích hợp phần mềm phân hệ sinh trắc 1
  - Thiết kế cài đặt tích hợp phần mềm phân hệ sinh trắc 2 trong hệ thống BK-BioPKI.

IV.4. Xây dựng kịch bản và thử nghiệm ứng dụng hệ BK-BioPKI trong môi trường mạng PTN

Nội dung phần này được trình bày chi tiết trong chương 8 của Báo cáo tổng hợp

- Xây dựng thử nghiệm lập trình ứng dụng chữ ký số trong hệ thống BK-BioPKI
- Xây dựng kịch bản thử nghiệm và lập trình ứng dụng mã hóa thông điệp
- Xây dựng kịch bản thử nghiệm và lập trình ứng dụng kiểm soát bảo mật truy cập từ xa

V. CÁCH TIẾP CẬN VÀ TRIỂN KHAI THỰC HIỆN ĐỀ TÀI

V.1. Các tiếp cận và phương pháp nghiên cứu

Căn cứ vào yêu cầu nhiệm vụ để thực hiện quá trình nghiên cứu, chúng tôi thực hiện phương pháp tiếp cận từ vấn đề tổng thể đến phân tích cụ thể, tiếp cận từ ngoài vào trong hệ thống, thể hiện như sau:

- Từ nghiên cứu khảo sát và nghiên cứu tổng hợp lý thuyết đến xây dựng phương án
- Từ nghiên cứu xây dựng mô hình giải pháp về phương diện lý thuyết đến giải pháp công nghệ thực thi
- Từ phân tích thiết kế toàn bộ hệ thống đến thực hiện xây dựng và lập trình cài đặt hệ thống hệ thống lõi PKI trên cơ sở sử dụng bộ phần mềm thư viện OpenSSL.

- Từ nghiên cứu thử nghiệm các thuật toán sinh trắc, xây dựng phần mềm hệ thống sinh trắc vân tay đến nghiên cứu thiết kế tích hợp phần mềm sinh trắc vào PKI thành hệ thống BioPKI.
- Từ kịch bản đến xây dựng các ứng dụng thử nghiệm hệ BioPKI trong phòng thí nghiệm

Hệ thống BioPKI của đề tài được triển khai xây dựng hệ thống theo các phiên bản đơn giản đến phức tạp, theo tiến độ qua 4 giai đoạn từ phiên bản BioPKI Ver.1 đến BioPKI Ver.4 với các chức năng được phát triển tích hợp dần dần từ đơn giản đến phức tạp hơn.

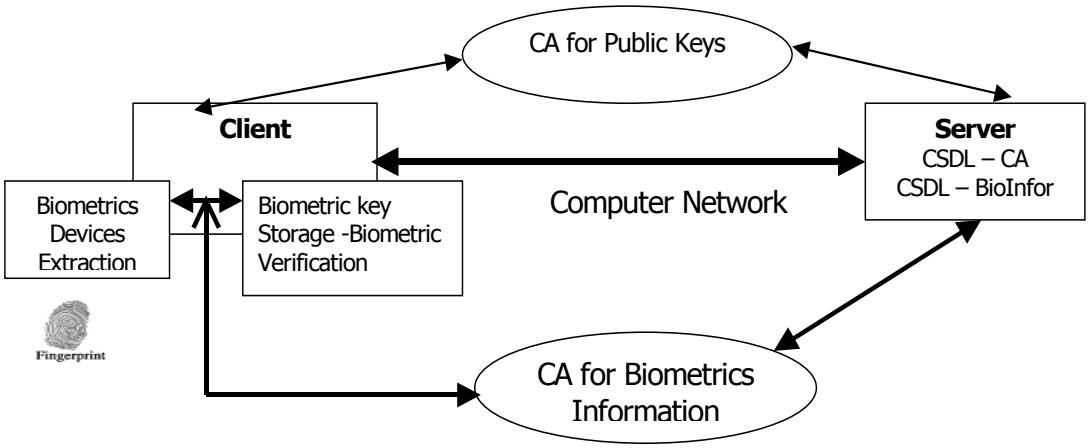
V.2. Tóm tắt quá trình thực hiện đề tài nhiệm vụ tiến độ đã đăng ký trong thuyết minh

- **Giai đoạn 1: từ tháng 6 đến tháng 12-2006: Phiên bản hệ thống BioPKI Ver.1**
  - Nghiên cứu và thử nghiệm các thuật toán: Thu nhận vân tay, trích chọn đặc trưng, sinh khóa sinh trắc và thẩm định xác thực vân tay
  - Nghiên cứu các hướng tiếp cận hệ thống BioPKI
  - Xây dựng phương án và môi trường phần mềm hệ thống BioPKI dựa trên bộ thư viện mở OpenSSL và ngôn ngữ C++
- **Giai đoạn 2: từ tháng 1-2007 đến 6-2007: Phiên bản hệ thống BK-BioPKI Ver.2**
  - Phân tích thiết kế các mô đun cơ sở hạ tầng hệ thống PKI: CA, RA User
  - Tiếp tục nghiên cứu và thử nghiệm các thuật toán sinh trắc học vân tay
  - Xây dựng và thiết kế phần mềm phần hệ sinh trắc học (Biometric) bao gồm: Ký mã sinh trắc và thẩm định vân tay trong hệ thống BK-BioPKI
- **Giai đoạn 3 và 4: từ 7/2007 đến 6/2008 Phiên bản hệ thống BK-BioPKI Ver. 3.1 và phiên bản Ver.4 kết hợp hệ thống và thử nghiệm ứng dụng**
  - Phân tích thiết kế phát triển và lập trình toàn bộ Protoptye cơ sở hạ tầng hệ thống BK-BioPKI trong môi trường mạng PTN
  - Phân tích thiết kế phát triển phân hệ sinh trắc Biometric với 2 môđun và thử nghiệm vào ứng dụng hệ thống Ver.4
  - Phân tích thiết kế tích hợp phân hệ sinh trắc vào toàn bộ hệ thống BK-BioPKI phiên bản Ver.4
  - Xây dựng mô hình kịch bản và thử nghiệm 3 ứng dụng trong hệ BK-BioPKI Ver.4

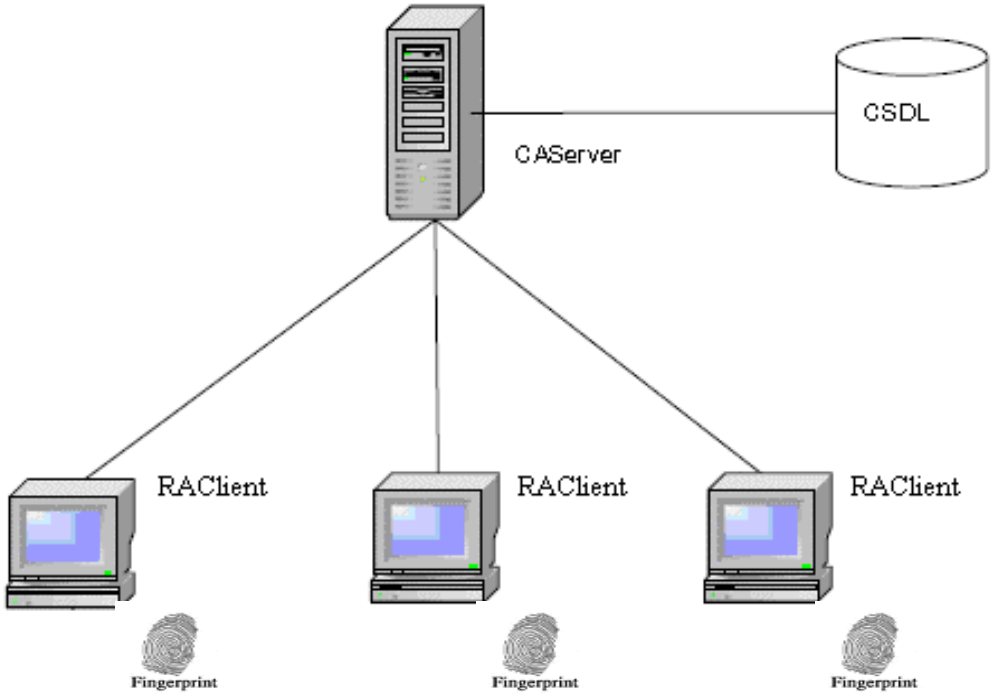
VI. TỔNG HỢP CÁC KẾT QUẢ ĐẠT ĐƯỢC

VI.1. Kết quả về giải pháp tích hợp đặc trưng vân tay với mã bảo mật trong hệ PKI thành hệ thống BioPKI.

Đề tài đã đề xuất mô hình giải pháp tích hợp đặc trưng vân tay với hạ tầng khóa công khai thành hệ thống BioPKI.



Hình 1. Khung làm việc của hệ thống BioPKI trong môi trường mạng



Hình 2. Mô hình mức khung cảnh hệ thống an ninh thông tin dựa trên sinh trắc học BioPKI

Mô hình hệ thống BioPKI bao gồm các thành phần hệ thống sau:

- Hệ thống lõi hạ tầng khóa công khai PKI: Hệ thống lõi PKI được xây dựng theo mô hình kiến trúc CA với đầy đủ các thành phần chức năng cơ bản của hệ PKI bao gồm:

  - CA (Certificate Authority): Bộ phận thẩm quyền phát hành các chứng chỉ và chứng thực các chứng chỉ

  - RA (Registration Authority): Bộ phận thẩm quyền đăng ký chứng chỉ,

  - Certificate Holder- User: người sử dụng trong hệ thống PKI, chủ thể chứng chỉ,

  - Digital Certificate Distribution System: Hệ thống phân phối chứng chỉ số, kho chứa

Hệ thống lõi PKI được thiết kế và lập trình trên môi trường bộ thư viện mã nguồn mở OpenSSL, theo chuẩn X509. Trong mô hình hệ BioPKI hiện nay RA có vai trò quản lý người dùng, lưu trữ khóa cá nhân được bảo mật bằng sinh trắc vân tay. Toàn bộ các giao thức và các giao dịch cơ sở giữa RA và CA được thiết kế và cài đặt làm cơ sở để tích hợp hệ sinh trắc tạo vào máy người sử dụng (users)

- Hệ thống thẩm định xác thực sinh trắc vân tay (Fingerprint Biometric System)

Dùng sinh trắc vân tay sống được lấy trực tuyến từ thiết bị scanner. Hoạt động của hệ thống sinh trắc gồm 2 pha chức năng:

+ Pha đăng ký sinh trắc (Enrollment):
  - Đăng ký người dùng
  - Lấy dấu vân tay sống trực tuyến từ thiết bị quét thông dụng
  - Xử lý ảnh trích chọn đặc trưng
  - Mã hóa đặc trưng
  - Lưu trữ mã đặc trưng
+ Pha thẩm định xác thực (Verification - Authentication):
  - Lấy dấu vân tay sống trực tuyến từ thiết bị quét
  - Xử lý ảnh trích chọn đặc trưng
  - Đối sánh thẩm định trực tuyến (online) xác thực vân tay của chủ thể người dùng

- Mô hình BioPKI: Đề xuất mô hình giải pháp tích hợp thẩm định sinh trắc vân tay sống trực tuyến vào hệ lõi hạ tầng khóa công khai (gọi tên là BK-BioPKI), bao gồm 2 phân hệ sinh trắc sau:

- Phân hệ thẩm định xác thực trực tuyến vân tay người dùng được tích hợp vào quá trình đăng nhập hệ thống BioPKI thay password, các dấu đặc trưng vân tay được mã hóa và lưu trữ tại máy user (được gọi là Phân hệ sinh trắc 1)

- Phân hệ sinh trắc vân tay kết hợp với quá trình mật mã và sử dụng chứng chỉ số trong hệ BioPKI, sinh khóa sinh trắc để mã hóa bảo mật khóa cá nhân của người dùng trong hệ thống (được gọi là Phân hệ sinh trắc 2). Phần mềm phân hệ sinh trắc 2 được tích hợp vào hệ BioPKI tại máy user, được quản lý bởi RA và xác thực bởi CA (chi tiết của mô hình tích hợp sẽ được trình bày trong chương 5 và chương 7 báo cáo tổng hợp)

VI.2. Kết quả thiết kế và xây dựng thử nghiệm hệ thống BioPKI (Prototype) kết hợp thẩm định xác thực vân tay sống, trực tuyến.

VI.2.1. Giải pháp công nghệ thiết kế và triển khai hệ thống BK-BioPKI

- Theo mô hình đã trình bày ở trên, giải pháp về công nghệ, môi trường phần mềm để thiết kế và triển khai hệ thống bao gồm:

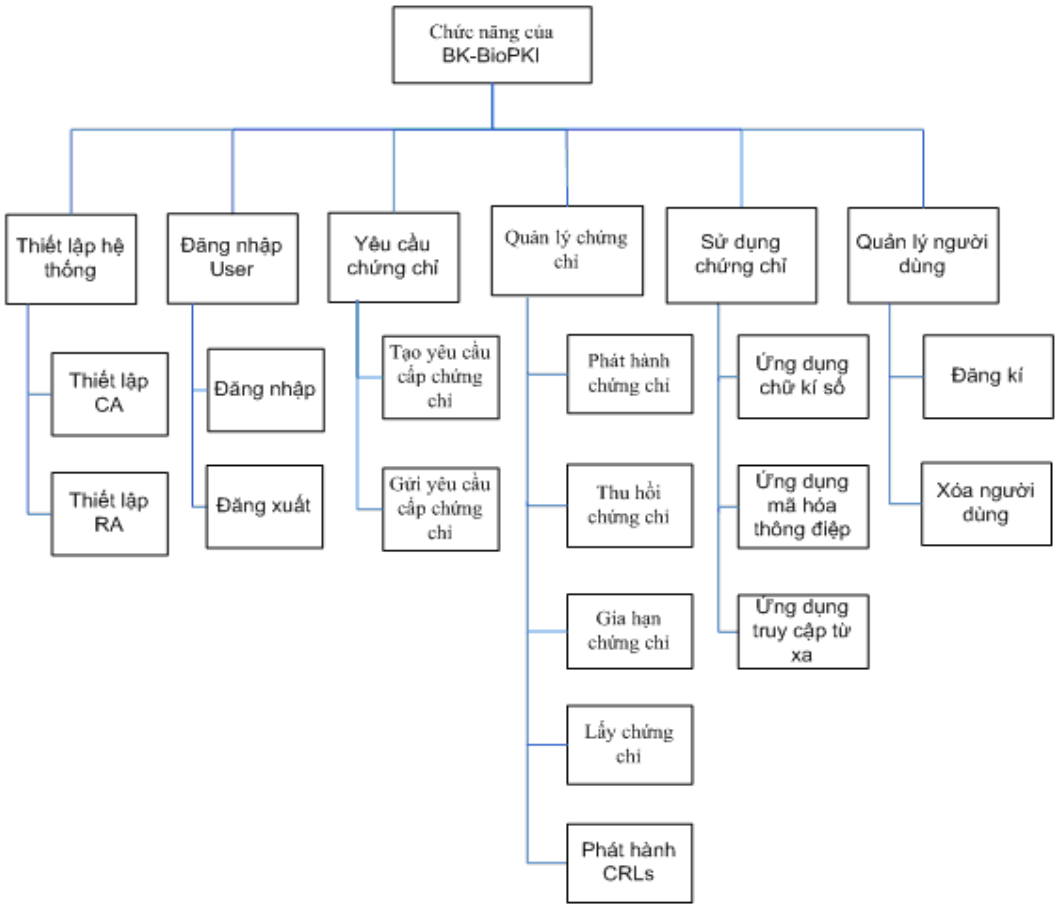
- Cấu hình mạng cục bộ cho hệ thống BK-BioPKI trong giai đoạn này bao gồm một máy Server và các máy Client (users) kết nối hoạt động trong môi trường mạng tác nghiệp tại phòng thí nghiệm khoa CNTT – ĐHBK HN. Tất cả các máy trong phòng thí nghiệm được cài đặt môi

trường lập trình Windows XP SP1, bộ công cụ lập trình Microsoft visual studio 2003, hệ quản trị cơ sở dữ liệu MySQL.

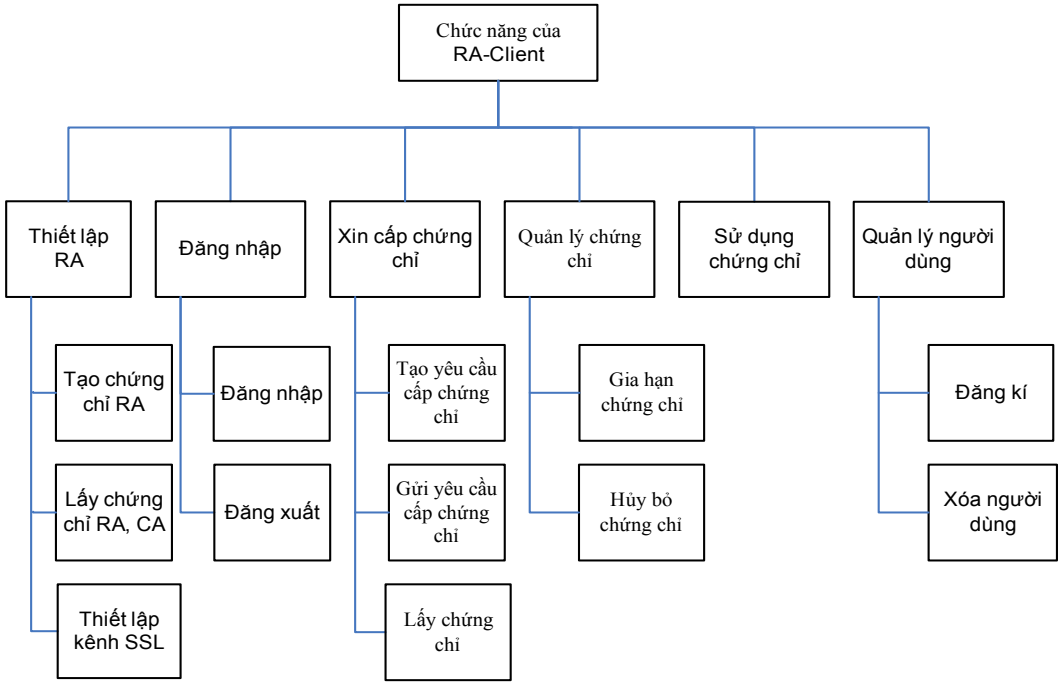
- Hệ thống lõi PKI với kiến trúc CA đơn được xây dựng trên cơ sở bộ thư viện mở OpenSSL
- Ảnh vân tay sống được lấy trực tuyến qua thiết bị quét vân tay với các thông số kỹ thuật sau: Scaner Futronic model 9880, Futronic's FS82 USB 2.0 Fingerprint scanner with scanning window size is 16x24mm; Image resolution is 480x320 pixel, 500 DPI; Raw fingerprint image file size is 150K byte; with Live Finger Detection (LFD). Đầu ra thiết bị quét Futronic's FS82 USB 2.0 chỉ cung cấp ảnh vân tay theo định dạng file *.bmp, không có phần mềm xử lý ảnh kèm theo bộ quét.
- Bộ phần mềm xử lý ảnh vân tay và phần mềm hệ thống sinh trắc gồm các thuật toán được thiết kế và cài đặt bằng ngôn ngữ C++ với Windows 2003 và Matlab.

VI.2.2. Phân tích thiết kế toàn bộ hệ thống BK-BioPKI (prototype)

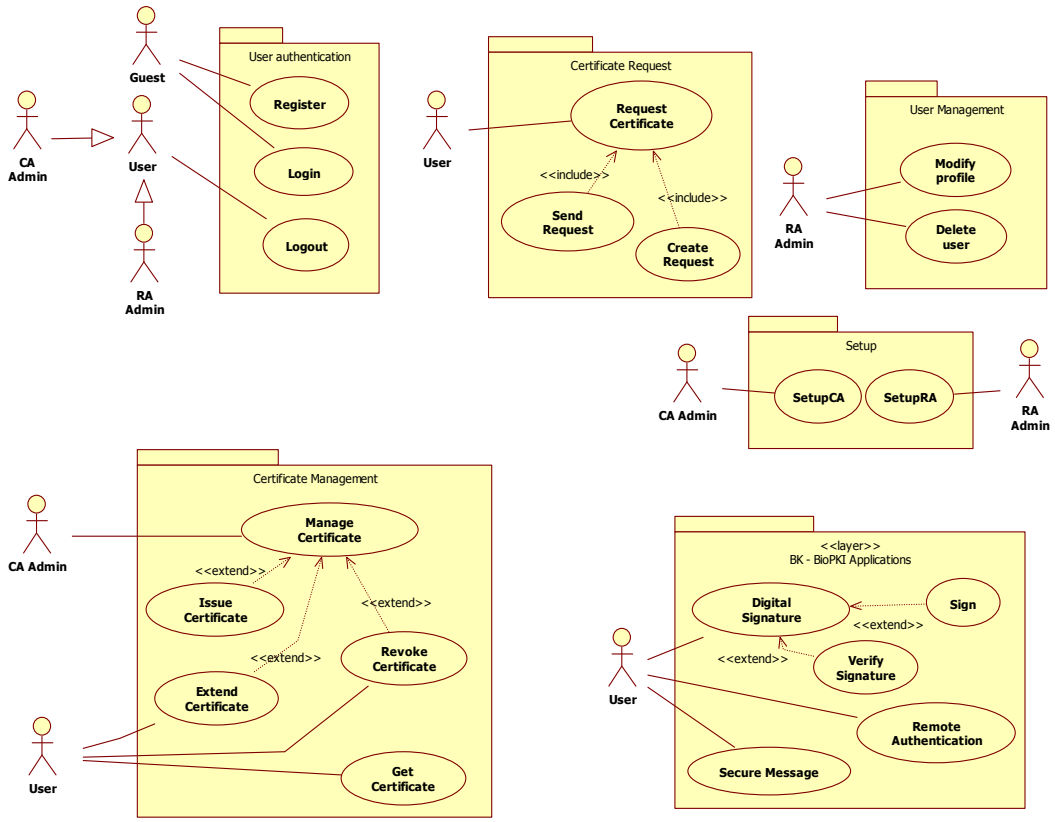
- Quá trình phân tích thiết và xây dựng hệ thống BK-BioPKI bao gồm các nội dung: Thiết kế xây dựng hệ thống lõi PKI; Thiết kế xây dựng phần mềm hệ sinh trắc vân tay dùng thiết bị quét Futronic's FS82 USB 2.0 Fingerprint scanner; Thiết kế xây dựng và cài đặt lập trình hệ thống tích hợp BK-BioPKI theo mô hình tích hợp đã đề xuất.
- Hệ thống BK-BioPKI bao gồm một cơ sở hạ tầng khóa công khai PKI với CA đơn, có các chức năng PKI cơ bản: tạo yêu cầu xin cấp chứng chỉ, cấp phát chứng chỉ, quản lý việc gia hạn chứng chỉ và hủy bỏ chứng chỉ và tích hợp các chức năng của phân hệ sinh trắc học.
- Phần dưới đây sẽ trình bày một số sơ đồ chính của hệ thống BK-BioPKI (đã trình bày chi tiết trong báo cáo tổng hợp ở các chương 5, 6, 7 trong báo cáo tổng hợp).
    - Biểu đồ phân cấp chức năng hệ thống BK-BioPKI phần CA (Hình 3).
    - Biểu đồ phân cấp chức năng hệ thống BK-BioPKI phần RA-Client Hình 4).
    - Biểu đồ các tình huống sử dụng các giao dịch cơ sở trong hệ thống BK-BioPKI (Hình 5).
    - Sơ đồ mô hình tích hợp thẩm định xác thực sinh trắc vân tay (Phân hệ sinh trắc 1) vào quá trình đăng nhập và thẩm định người dùng user (Hình 6).
    - Sơ đồ mô hình tích hợp thẩm định xác thực sinh trắc vân tay trực tuyến kết hợp với mật mã trong quá trình xin cấp chứng chỉ, sử dụng chứng chỉ trong hệ BK-BioPKI (Hình 7).



Hình 3. Biểu đồ phân rã chức năng của hệ thống BK – BioPKI (bộ phận CA)

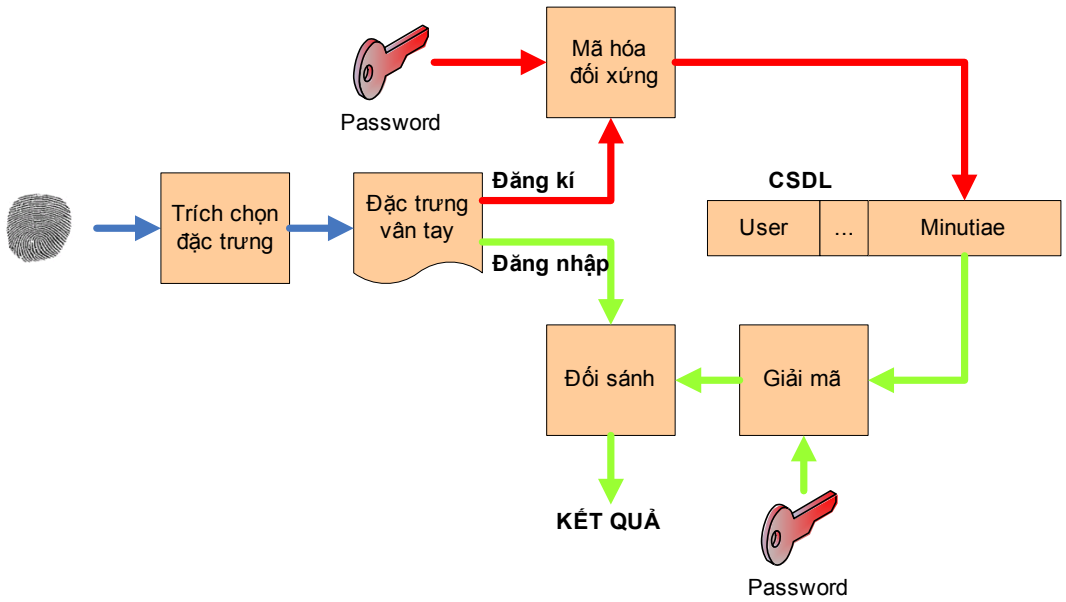


Hình 4. Biểu đồ phân cấp các chức năng RA-Client

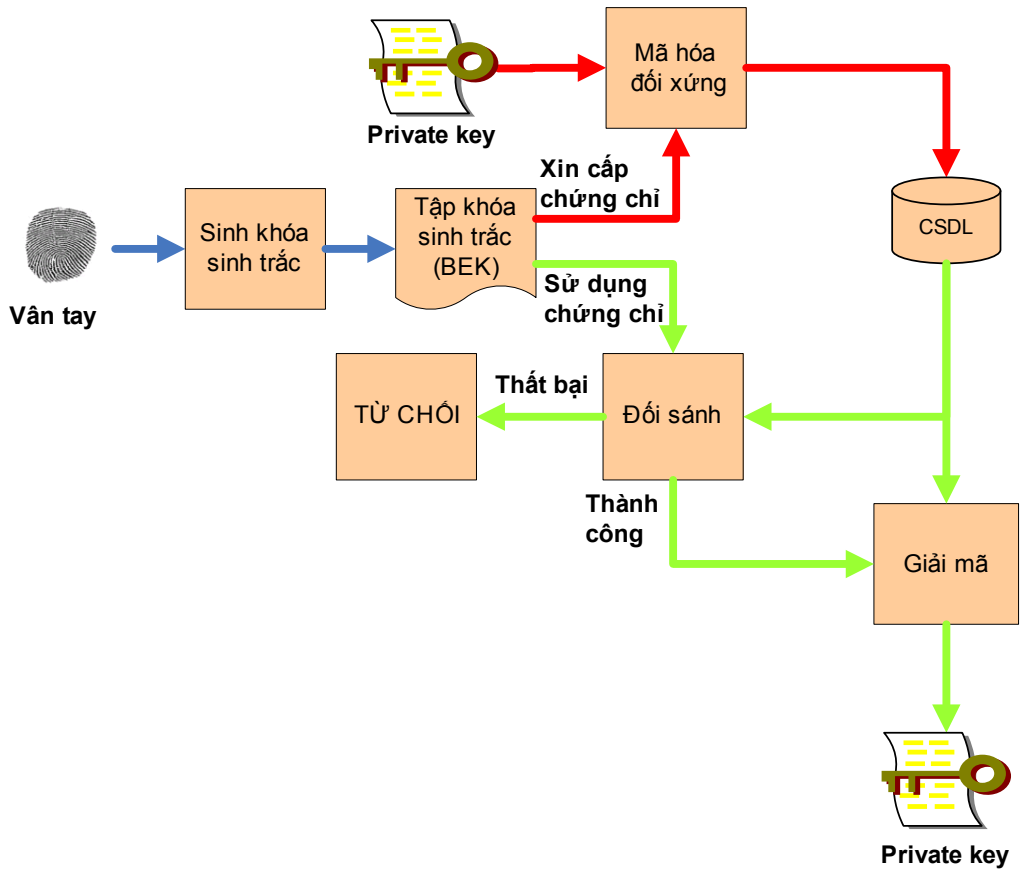


Hình 5. Các tình huống sử dụng giao dịch trong hệ thống BK-BioPKI

Trong biểu đồ này, các chức năng của hệ thống gắn liền với các tác nhân bao gồm: người quản trị CA (CA Amin), người quản trị RA (RA Admin) và các người sử dụng (Users) của hệ thống.



Hình 6. Tích hợp phân hệ sinh trắc 1 thẩm định đăng nhập người dùng trong hệ thống



Hình 7. Mô hình tích hợp phân hệ sinh trắc 2 sinh khóa bảo vệ khóa cá nhân trong hệ thống.

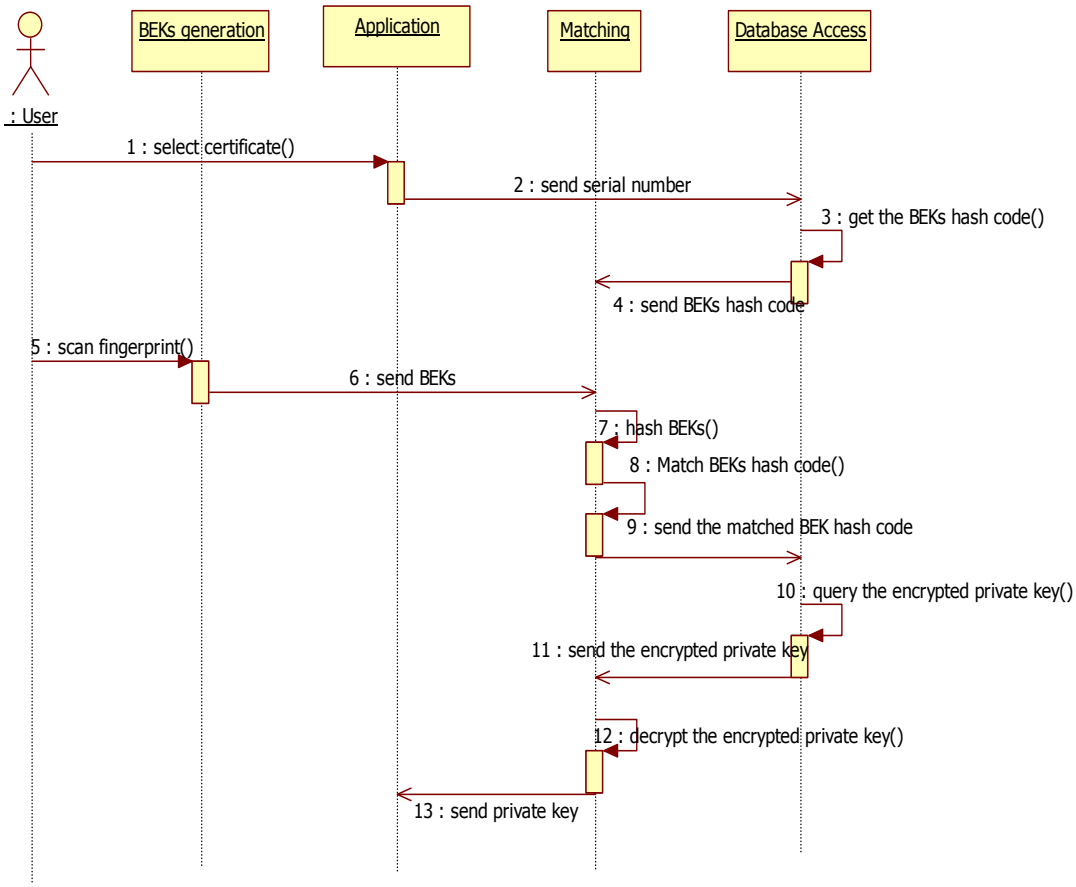
VI.3. Kết quả phần mềm máy tính cho hệ thống BioPKI

Đề tài đã xây dựng và cài đặt toàn bộ phần mềm cho hệ thống BK-BioPKI bao gồm các bộ phần mềm sau:

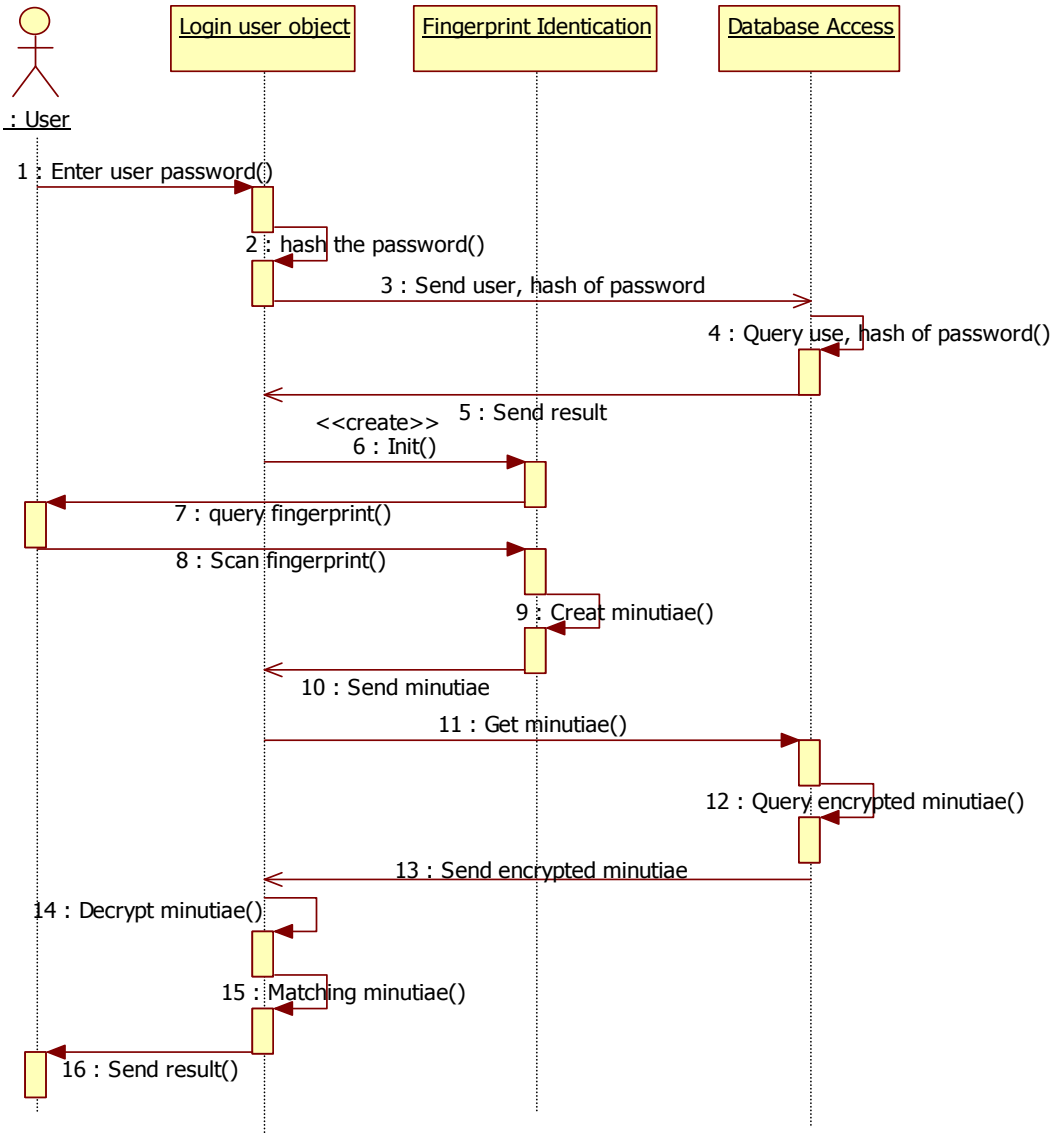
- **Bộ phần mềm cơ sở hệ lõi PKI** đảm bảo được các chức năng cơ bản của một cơ sở hạ tầng khóa công khai PKI với CA đơn: tạo yêu cầu xin cấp chứng chỉ, cấp phát chứng chỉ, quản lý, gia hạn chứng chỉ và hủy bỏ chứng chỉ.
- **Bộ phần mềm hệ thẩm định xác thực vân tay sống, trực tuyến** gồm các chức năng chủ yếu:
  + Phần mềm đăng ký sinh trắc học vân tay BioPKI
  + Phần mềm mã hóa
  + Phần mềm xác thực thẩm định vân tay BioPKI

Bộ phần mềm sinh trắc trong hệ thống BioPKI được xây dựng thành 2 phân hệ thống sinh trắc tương ứng với mô hình kết hợp 2 phân hệ sinh trắc vào các hoạt động trong hệ BioPKI.

- **Bộ phần mềm tích hợp hệ thống an ninh sinh trắc học Bio-PKI:** Thực hiện tích hợp hệ thẩm định xác thực vân tay vào hoạt động các giao dịch đăng nhập, xin cấp chứng chỉ và sử dụng chứng chỉ trong hệ thống. Các hình vẽ dưới đây trình bày 2 sơ đồ diễn tiến lập trình trong số nhiều sơ sồ diễn tiến đã được thiết kế và thực hiện các bước trong các giao dịch hoạt động trong hệ thống BioPKI.
- **Chương trình thử nghiệm sinh trắc lòng bàn tay**: Cài đặt thuật toán trích chọn đặc trưng, thẩm định xác thực sinh trắc lòng bàn tay và thử nghiệm với CSDL ảnh lòng bàn tay (xem chi tiết phần phụ lục Báo cáo tổng hợp.



Hình 8. Sơ đồ diễn tiến kịch bản sử dụng chứng chỉ trong BioPKI



Hình 9. Sơ đồ diễn tiến kịch bản đăng nhập người dung trong BioPKI.

VI.4. Phần mềm thử nghiệm ứng dụng

Đề tài đã xây dựng thử nghiệm 3 kịch bản ứng dụng an toàn bảo mật thông tin trong môi trường hệ thống BK-BioPKI (trình bày chi tiết trong chương 7 và chương 8 của báo cáo tổng hợp), gồm có:

- Xác thực chữ ký số
- Ký và mã hóa bảo mật thông điệp
- Kiểm soát bảo vệ truy cập vào CSDL trên mạng

Các kịch bản này đã được thiết kế chi tiết, được lập trình cài đặt và thủ nghiệm trong môi trường mạng của hệ thống BK-BioPKI tại PTN.

VI.5. Các kết quả thực nghiệm trong phòng thí nghiệm

VI.5.1. Mô tả kịch bản thử nghiệm

Hiện nay toàn bộ hệ thống tích hợp BK-BioPKI được xây dựng trong môi trường mạng trong PTN theo cấu hình đã trình bày ở trên. Tại các máy người sử dụng, dùng thiết quét vân tay Futronic's FS82 USB 2.0 Fingerprint để lấy vân tay sống trực tuyến dùng cho 2 pha của hệ thống: pha đăng ký và pha thẩm định xác thực liên quan đến chứng chỉ.

Quá trình thử nghiệm hệ thống bao gồm 2 nội dung chủ yếu: Thử nghiệm các hoạt động giao dich trong hệ thống BK-BioPKI thông qua các ứng dụng và thử nghiệm đánh giá thống kê thực nghiệm các chất lượng hệ thống thông qua các độ đo FRR (False Rejection Rate) và FAR (False Acceptance Rate)

Tính toán thực nghiệm các thông số đánh giá hệ thống (%):

$$\text{FRR} = \frac{So\ truong\ hop\ loai\ bo\ sai}{Tong\ so\ truong\ hop}$$

$$\text{FAR} = \frac{So\ truong\ hop\ chap\ nhan\ sai}{Tong\ so\ truong\ hop}$$

a. Thử nghiệm các giao dịch cơ sở trong hệ BK-BioPKI và đánh giá mức độ trơn của các hoạt động giao dịch trong hệ thống:

- Thực hiện các quá trình cài đặt CA và RA (5 lần) để kiểm tra mức độ lỗi trong chương trình.
- Đăng ký người sử dụng (10 người), kiểm tra các lỗi phát sinh trong quá trình từ lúc đăng ký người dùng vào hệ thống đến khi lấy được chứng chỉ.
- Thống kê các lỗi nếu xảy ra trong quá trình thực hiện giao dịch

b. Thử nghiệm các ứng dụng và đánh giá thực nghiệm thông số chất lượng thẩm định xác thực sinh trắc vân tay trong hoạt động hệ BK-BioPKI

Trong mỗi hoạt động hệ sinh trắc bao gồm 2 pha: Đăng ký và thẩm định xác thực sinh trắc. Theo mô hình giải pháp hệ BK-BioPKI đã trình bày ở trên, hệ sinh trắc bao gồm 2 phân hệ kết hợp: phân hệ thẩm định sinh trắc đăng nhập đầu vào và phân hệ thẩm định sinh trắc để giải mã lấy khóa cá nhân (private key) để thực hiện các giao dịch: ứng dụng chữ ký số hoặc ứng dụng bảo mật thông điệp

- Thử nghiệm thẩm định sinh trắc trong hoạt động đăng nhập vào hệ thống:
  - Thực hiện lấy mẫu của 10 người sử dụng
  - Để đánh giá FAR: với mỗi người dùng, thử nghiệm với 10 mẫu vân tay không dùng để đăng ký
  - Để đánh giá FRR: dùng vân tay đăng ký để thử nghiệm 10 lần và đo số trường hợp sai

- Thử nghiệm thẩm định xác thực sinh trắc vân tay người dùng truy xuất khóa cá nhân trong ứng dụng chữ ký số:
  - Lấy chứng chỉ của 5 người sử dụng
  - Để đánh giá FAR: với mỗi người dùng, thử nghiệm với 10 mẫu vân tay không dùng để đăng ký
  - Để đánh giá FRR: dùng vân tay đăng ký để thử nghiệm 10 lần và đo số trường hợp sai

VI.5.2. Kết quả thực nghiệm

5.2.1 Kết quả thực nghiệm đánh giá quá trình thẩm định sinh trắc trong hoạt động đăng nhập (login)

Số lần thực hiện	Số từ chối sai/ Số chấp nhận sai	Tỉ lệ FRR(%)	Tỉ lệ FAR (%)
100	29	29	
100	27		27

Bảng 1: Kết quả thực nghiệm Tỷ lệ FRR và FAR khi đăng nhập

5.2.2 Kết quả thực nghiệm đánh giá quá trình thẩm định sinh trắc để truy xuất lấy khóa cá nhân dung trong hoạt động chữ ký số

Số lần thực hiện	Số từ chối sai/ Số chấp nhận sai	Tỉ lệ FRR(%)	Tỉ lệ FAR (%)
50	23	46	
50	7		14

Bảng 2: Kết quả thực nghiệm Tỷ lệ FRR và FAR khi xác thực khóa sinh trắc vân tay song trực tuyến đề giải mã truy xuất khóa cá nhân trong hoạt động ký chữ ký số

5.2.3. Kết quả thử nghiệm độ trơn trong hoạt động của hệ thống và tính thực nghiệm tỷ lệ các lỗi phát sinh

- Kết quả cho thấy hầu hết các giao dịch của hệ thống (từ cài đặt CA, RA, đăng nhập, ….) không xảy ra lỗi, hoạt động trơn tru đặc biệt là các kết nối giữa CA-RA (các giao dịch về chứng chỉ) và giữa các RA với nhau (chữ ký số)

Số lần cài đặt	Số lần lỗi	Tỉ lệ (%)
5	5	0

Bảng 3 . Kết quả đánh giá quá trình cài CA

Số lần cài đặt	Số lần lỗi	Tỉ lệ (%)
5	5	0

Bảng 4. Kết quả đánh giá quá trình cài RA

- Tuy nhiên trong quá trình thực hiện cho thấy có một lỗi xảy ra trong quá trình đăng ký vân tay khi tạo yêu cầu (request) để gửi lên CA. Đây là lỗi quá trình đăng ký sinh trắc (enrollment) vân tay người dùng vào yêu cầu và là lỗi liên quan đến thuật toán sinh trắc. Lỗi này hoàn toàn có thể khắc phục được thông qua việc cải thiện thuật toán trích chọn đặc trưng và chương trình xử lý sinh trắc

Số lần thực hiện	Số lần lỗi	Tỉ lệ (%)
10	2	20

Bảng 5. Tỉ lệ lỗi với quá trình đăng ký sinh trắc (enrollment)

5.2.4 Đánh giá kết quả thực nghiệm

Qua các kết quả thử nghiệm trong phòng thí nghiệm về hệ thống BK-BioPKI có thể cho thấy hệ thống nền tảng lõi PKI được thực hiện tốt, hoạt động khá hoàn thiện, các giao dịch từ cài đặt, cấp chứng chỉ, xác thực chứng chỉ, nhìn chung hoạt động ổn định và không có lỗi. Các chức năng của một hệ thống BioPKI được thực hiện tương đối hoàn chỉnh và đảm bảo các hoạt động xác thực sinh trắc vân tay sống trong hệ thống BK-BioPKI ở các mức khác nhau. Điều đó chứng tỏ mô hình giải pháp hệ thống BioPKI và quá trình phân tích thiết kế hệ thống đã đạt kết quả tốt. Hoạt động toàn bộ hệ thống BK-BioPKI đã được kiểm nghiệm qua các thực nghiệm với các sinh trắc vân tay sống trực tuyến và đạt bước đầu khả quan.

Tuy nhiên, về đánh giá các tham số hiệu năng hệ thống vẫn còn có lỗi ở quá trình sinh trắc, thể hiện tỷ lệ lỗi do xử lý chưa hết các trường hợp ngoại lệ. Thực nghiệm với vân tay sống cho thấy tỷ lệ lỗi FRR và FAR trong cả 2 quá trình hoạt động xác thực sinh trắc tỷ lệ lỗi vẫn còn tương đối cao. Đó chính là vấn đề cần tiếp tục cải tiến về hệ thẩm định xác thực sinh trắc

Trong điều kiện cấu hình hệ thống trong môi trường phòng thí nghiệm, thời gian thực hiện thuật toán còn lớn (khoảng gần 40s). Hiệu năng về thời gian xử lý sinh trắc còn chậm thể hiện chủ yếu do phần tích hợp các thuật toán sinh trắc (viết bằng Matlab) vào hệ PKI chỉ ở mức mô hình tích hợp.

VI.6. Kết quả hợp tác với Malaysia

VI.6.1. Đặc điểm quá trình hợp tác

- Về tiến độ thời gian bắt đầu thực hiện nhiệm vụ nghị định thư của 2 phía Malaysia và Việt Nam có sự chênh lệch: Nhiệm vụ của phía Malaysia đã thực hiện từ 2005, nhiệm vụ của phía Việt nam được chính thức bắt đầu 6-2006, MMU đã thực hiện trước một năm so với nhiệm vụ của phía Việt Nam.
- Khi nhiệm vụ phía Việt Nam chính thức bắt đầu thì phía Malaysia đang là giai đoạn cuối của nhiệm vụ đề tài phía Malaysia đề xuất trong nhiệm vụ hợp tác Nghị định thư và phía Malaysia đã kết thúc đề tài này 2006.

- Phía bạn tiếp tục nghiên cứu về lĩnh vực này và từ 6-2007 phía Malaysia có kinh phí thực hiện đề tài khác (theo tài liệu bạn cung cấp, thời gian là từ 15/6/2007 đến 30/5/2008), bởi vậy đến 5/2007 phía bạn mới xúc tiến tiếp tục các hoạt động trao đổi hợp tác qua mail.
- Chủ nhiệm đề tài phía Malaysia có thay đổi, hiện nay là ông Dr. Ong Thian Song, Giám đốc điều hành trung tâm nghiên cứu CBB và phía Malaysia tiếp tục nhiệt tình trong hợp tác thực hiện nhiệm vụ NĐT với Việt Nam
- Phía bạn chưa thực hiện cử đoàn ra sang Việt Nam như đã dự kiến vì lý do phía bạn chưa thu xếp được kinh phí.

VI.6.2. Các hoạt động hợp tác phối hợp nghiên cứu

- Phía MMU tổ chức Hội thảo trao đổi phối hợp nghiên cứu 2 bên tại Malaysia trong thời gian 20-21/9/2007 để xúc tiến tăng cường hợp tác, gặp gỡ trao đổi cụ thể và phối hợp các công việc nghiên cứu của cả hai bên

  MMU-HUT Joint Seminar, 20th - 21th September 2007

  CBB-FIST, Multimedia University (Melaka Campus), Malaysia
- Phía Đại học Bách khoa Hà nội đã tham gia trình bày 3 báo cáo trao đổi nghiên cứu tại hội thảo này, bao gồm:
  - H.Lan Nguyen, "BioPKI based information security system using fingerprint biometric authentication"
  - Q.Trung HA, "Using online fingerprint authentication to protect private key for digital signature".
  - H.Lan Nguyen and Q.Trung Ha, "BioMetric verification based remote authentication"
- Tháng 12/2007 và tháng 5/2008: Theo kế hoạch đã duyệt, phía VN đã cử 2 đoàn công tác sang Malaysia làm việc phối hợp nghiên cứu về hệ thống thẩm định sinh trắc (chi tiết đã nêu trong báo cáo ở phần phụ lục)
- Kết quả nghiên cứu phối hợp là trao đổi về phương án, xây dựng mô hình và trao đổi các thuật toán, hiện chưa có sự trao đổi kết hợp phần mềm cụ thể nào trong hệ BK-BioPKI hiện nay.
- Để thực hiện được trao đổi phần mềm hoặc tích hợp kết quả 2 bên, theo đề nghị của phía trường MMU cần chuẩn bị để ký bản cam kết (MMA) giữa MMU và HUT (ĐHBK HN). Hiện nay cho đến tháng 12-2008, hai bên đã trao đổi bản thảo và đợi điều kiện để ký. Cho đến nay, phía MMU chưa có đoàn sang ĐHBK HN vì lý do kinh phí và thời gian.
- Hai bên MMU và HUT đã nhất tiếp tục phát triển Hợp tác với Malaysia trong thời gian tới trong khuôn khổ đề tài KC0111 tiếp tục nghiên cứu phát triển hệ thống BioPKI trong giai đoạn tiếp từ 2008-2009.

VI.7. Kết quả đào tạo

VI.7.1. Đào tạo thạc sĩ

Theo hướng của đề tài cho đến nay đã có 6 luận văn Thạc sĩ bảo vệ tốt nghiệp:

1. Trần Tuấn Vinh Khóa 2003-2005 đã bảo vệ 2006
   Tên luận văn: "Nghiên cứu giải pháp an ninh thông tin dựa trên hướng tiếp cận sinh trắc học kết hợp mã công khai PKI với đặc điểm sinh trắc vân tay"
2. Nguyễn Anh Tài Khóa 2004-2006 đã bảo vệ 2006
   Tên luận văn: "Nghiên cứu phương pháp thẩm định xác thực sinh trắc chữ ký viết tay ứng dụng trong giao dịch điện tử"
3. Vũ Thanh Thắng Khóa 2005-2007 đã bảo vệ 12- 2007
   Tên luận văn: "Nghiên cứu thuật toán mã hóa bảo mật nâng cao AES và xây dựng ứng dụng thuật toán dựa trên công nghệ nhúng"
4. Lê Quang Tùng Khóa 2006-2008 đã bảo vệ 11- 2008
   Tên luận văn: "Xây dựng giải pháp ứng dụng xác thực sinh trắc học trong cơ sở hạ tầng khóa công khai dựa trên hệ thống OpenCA"
5. Lê Trần Vũ Anh Khóa 2006-2008 đã bảo vệ 11- 2008
   Tên luận văn: "Nghiên cứu giải pháp ứng dụng hạ tầng khóa công khai PKI trong hệ thống thanh toán điện tử liên ngân hàng"
6. Hà Tiến Dũng Khóa 2006-2008 đã bảo vệ 11- 2008
   Tên luận văn: "Hệ mật khóa công khai và chữ ký số"

VI.7.2. Đào tạo bậc đại học

Nhiều đồ án kỹ sư tốt nghiệp ngành CNTT- ĐHBK HN đã thực hiện theo hướng đề tài: Một số lượng đông đảo khoảng 20 đồ án tốt nghiệp của sinh viên các khóa (K46, K47, K48) có trong danh sách tham gia đề tài đã bảo vệ tốt nghiệp Kỹ sư CNTT – ĐHBK HN, tất cả đều đạt kết quả khá hoặc giỏi.

VI.8. Các bài báo khoa học

[1] Thi Hoàng Lan NGUYEN, Thi Thu Hang NGUYEN "*An Approach to Protect Private Key using Fingerprint Biometric Encryption Key in BioPKI based Security System*", trình bày và đã đăng trong kỷ yếu Hội nghị quốc tế: IEEE-10th International Conference on Control, Automation, Robotics and Vision (ICARCV 2008), December 17-20, 2008 Hanoi-Vietnam, ISBN-1-4244-2287-6 Library of Congress: 2008902134, 2008 IEEE.

[2] Nguyễn Thị Hoàng Lan, Bùi Thành Đạt, Lê Tiến Dũng, "X*ây dựng hệ thống an ninh thông tin dựa trên sinh trắc vân tay và hạ tầng khóa công khai BioPKI*", Trình bày tại Hội thảo Quốc gia lần thứ tư về Nghiên cứu phát triển và ứng dụng Công nghệ thông tin và Truyền thông ICT.rda' 2008, Hà Nội 8- 9/8/2008.

[3] Nguyễn Thị Hoàng Lan, Trần Hải Anh, "*Một giải pháp thẩm định vân tay trực tuyến trong hệ thống BK-BioPKI và ứng dụng kiểm soát truy cập từ xa*", Trình bày tại Hội thảo Quốc gia lần thứ tư về Nghiên cứu phát triển và ứng dụng Công nghệ thông tin và Truyền thông ICT.rda' 2008, Hà Nội 8- 9/8/2008.

[4]. Nguyễn Thị Hoàng Lan, Hoàng Trần Đức, "Về một ứng dụng mã hóa bảo mật thông điệp trong hệ thông BK-BioPKI", Trình bày tại Hội thảo Quốc gia lần thứ tư về Nghiên cứu phát triển và ứng dụng Công nghệ thông tin và Truyền thông ICT.rda' 2008, Hà Nội 8-9/8/2008.

[5]. Hà Quốc Trung, Nguyễn Trung Dũng, *"Trao đổi thông tin an toàn và bảo mật trên hạ tầng SMS"***,** Trình bày tại Hội thảo Quốc gia lần thứ tư về Nghiên cứu phát triển và ứng dụng Công nghệ thông tin và Truyền thông ICT.rda' 2008, Hà Nội 8- 9/8/2008.

[6]. Nguyễn Linh Giang, Vũ Ngọc Hà, *"Một giải pháp kết hợp chứng chỉ sinh trắc vào hệ thống PKI",* Trình bày tại Hội thảo Quốc gia lần thứ tư về Nghiên cứu phát triển và ứng dụng Công nghệ thông tin và Truyền thông ICT.rda'2008, Hà Nội 8- 9/8/2008.

VII. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

VII.1. Nhận xét đánh giá chung

- **Đề tài đã hoàn thành nhiệm vụ đã đề ra** đảm bảo về số lượng và chất lượng đã đăng ký về các sản phẩm KHCN. Toàn bộ hệ thống đã được thử nghiệm đạt kết quả trong môi trường mạng phòng thí nghiệm (đã trình bày chi tiết trong phần VI ở trên).
- **Đề tài đã phát triển** thêm các nội dung dưới đây so với nội dung đã đăng ký về các phần mềm máy tính:
    - Về phần mềm tích hợp sinh trắc trong hệ thống: hệ thống BK-BioPKI đã xây dựng bao gồm 2 phân hệ sinh trắc kết hợp 2 giải pháp trong hệ BioPKI
    - Về phần mềm thử nghiệm ứng dụng: hiện nay đã xây dựng thử nghiệm 3 kịch bản ứng dụng an toàn bảo mật thông tin trong môi trường hệ thống BK-BioPKI gồm: Xác thực chữ ký số; Ký và mã hóa bảo mật thông điệp; Kịch bản thử nghiệm kiểm soát bảo vệ truy nhập CSDL trên mạng.
    - Về sinh trắc lòng bàn tay: Đã xây dựng thử nghiệm chương trình trích chọn đặc trưng và thẩm định sinh trắc lòng bàn tay
- **Tính mới, tính sáng tạo của đề tài**: hướng nghiên cứu BioPKI là vấn đề đang được quan tâm trên thế giới, các tài liệu và hệ thống an ninh thông tin dựa trên sinh trắc học hiện chưa nhiều và thường đóng kín do yêu cầu bảo mật. Kết quả của đề tài đã đóng góp tính mới trên mô hình giải pháp tích hợp hệ thống BioPKI thẩm định xác thực sinh trắc vân tay sống. Đó là hệ thống mới, đến hiện nay dựa trên các thông tin đã công bố đây là những kết quả đầu được triển khai nghiên cứu ở Việt Nam về lĩnh vực này.

VII.2. Tiến độ thực hiện

- Để tăng cường có hiệu quả trong hợp tác với Malaysia và để đề tài có điều kiện thử nghiệm và hoàn thành tốt nhiệm vụ theo nghị định thư, đề tài đã làm văn bản đề nghị xin phép được điều chỉnh gia hạn thời gian thực hiện tài đến 6/2008 trong điều kiện toàn bộ kinh phí đã được duyệt, không bổ sung thêm kinh phí.
- Nhiệm vụ đề tài đã được phép của Bộ KHCN, theo có công văn số 3397/BKHCN-XHTN, ký ngày 27/12/2007 cho phép gia hạn thời gian thực hiện nhiệm vụ đề tài đến

6/2008, như vậy đề tài có điều kiện thời gian đầy đủ 24 tháng để thực hiện như dự kiến ban đầu.

- Đề tài đã hoàn thành các công việc nghiên cứu theo đúng kế hoạch đã được phép đến 6-2008. Kết quả nghiên cứu của đề tài đã được trình bày trong Hội thảo mở rộng báo cáo kết quả nghiên cứu đã được tổ chức và thông báo trên mạng vào 20-6-2008.

VII.3. Hướng phát triển

- Kết quả đề tài đã đạt các kết quả khá quan trọng bước đầu phòng thí nghiệm mở ra một triển vọng nghiên cứu phát triển mới có ý nghĩa ứng dụng thực tế
- Kết quả của đề tài nhiệm vụ nghị thư là cơ sở để được tiếp tục theo hướng nghiên cứu này trong giai đoạn tiếp theo trong khuôn khổ Đề tài KC0111.
- Các hướng phát triển nghiên cứu trong thời gian tới trong Đề tài KC0111
    - Xây dựng hệ lõi PKI theo các công nghệ và chuẩn công nghiệp đề phù hợp với các khả năng sẽ triển khai hệ PKI ở Việt Nam
    - Nghiên cứu phát triển mô hình BioPKI và xây dựng hệ tích hợp BioPKI trên cơ sở hệ lõi PKI thông dụng (ví dụ hệ PKI trên cơ sở OpenCA)
    - Ứng dụng công nghệ nhúng cho hệ sinh trắc (Etoken USB)
    - Khảo sát và xây dựng các ứng dụng thực tế để có thể đưa hệ thống ra ứng dụng.