BẢO MẬT TRUY CẬP DỰA TRÊN HỆ BioPKI VÀ ỨNG DỤNG ĐỂ BẢO MẬT HỆ NHẬN DẠNG VÂN TAY C@FRIS

Nguyễn Văn Toàn
toannv-fit@mail.hut.edu.vn
Viện CNTT&TT,
Đại học Bách khoa
Hà Nội

Nguyễn Thị Hương Thủy
huongthuykta@yahoo.com
Phòng Thí nghiệm
MP&THHT, Tổng cục IV,
Bộ Công an

Nguyễn Ngọc Kỷ
kynguyen22@gmail.com
Phòng Thí nghiệm
MP&THHT, Tổng cục IV,
Bộ Công an

Nguyễn Thị Hoàng Lan
lannth-fit@mail.hut.edu.vn
Viện CNTT&TT,
Đại học Bách khoa
Hà Nội

Tóm tắt: *Trong bài báo này, chúng tôi trình bày đề xuất giải pháp kiểm soát truy cập cơ sở dữ liệu qua mạng dựa trên hệ thống BioPKI của đề tài KC.1.11/06-10 sử dụng thẻ sinh trắc Bio-Etoken kết hợp với mã hóa và chữ ký số, và xây dựng ứng dụng để bảo mật hệ nhận dạng vân tay C@FRIS. Ứng dụng BioPKI nhằm mục tiêu kiểm soát bảo mật truy cập cơ sở dữ liệu qua mạng đồng thời đảm bảo tính mật cho quá trình xác thực cũng như quá trình trao đổi dữ liệu bảo mật hệ nhận dạng vân tay C@FRIS. Các kết quả thử nghiệm bước đầu có nhiều triển vọng phát triển thành giải pháp bảo mật cho hệ C@FRIS triển khai trên thực tế. Với các tính năng của giải pháp BioPKI, việc bảo mật trên hệ C@FRIS được đảm bảo chặt chẽ mà vẫn giữ được tính dễ dùng trong các khâu xây dựng, khai thác và vận hành hệ thống*

Keyword: Biometric Security System, BioPKI System, Bio-Etoken, Remote Access Control to DB, C@FRIS.

I. GIỚI THIỆU

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 cũng như phương diện kỹ thuật và công nghệ. Nhiều các công trình nghiên cứu đã được đưa ra liên quan đến sinh trắc học (Biometric). 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 [1,2,4,6]. Hướng tiếp cận giải pháp an ninh dựa trên các dấu hiệu sinh trắc học kết hợp với hạ tầng khóa công khai thành BioPKI là một trong các hướng nghiên cứu mới đang được thế giới quan tâm phát triển [3,5,8]. Giải pháp BioPKI trên mạng cho phép bảo mật dựa trên cơ chế đảm bảo cho người sử dụng được ký sinh trắc và được xác thực sinh trắc truy cập bảo mật từ xa tới máy chủ thông qua mạng, đồng thời được phép kiểm soát các tiến trình giao dịch, kiểm soát truy cập đến các tệp tin, biết được ai, cái gì, khi nào, ở đâu, tác động như thế nào với các tệp tin và các giao dịch đó. Trong một thời gian dài, công nghệ này mới chỉ được đề cập trên phương diện lý thuyết, và gần đây nó mới được hiện thực hóa [7,10].

Giải pháp hệ thống BioPKI do đề tài KC.01.11/06-10 đề xuất là một trong những cố gắng đó [11]. Trong bài báo này chúng tôi sẽ trình bày về xây dựng ứng dụng kiểm soát truy cập cơ sở dữ liệu qua mạng dựa trên giải pháp hệ thống BioPKI của đề tài KC.1.11/06-10 sử dụng thẻ sinh trắc Bio-Etoken kết hợp với mã hóa và chữ ký số. Ứng dụng BioPKI nhằm mục tiêu kiểm soát bảo mật truy cập cơ sở dữ liệu qua mạng và đảm bảo tính mật cho quá trình xác thực cũng như quá trình trao đổi dữ liệu bảo mật hệ nhận dạng vân tay C@FRIS. Bài báo được trình bày bao gồm 4 phần sau: Sau phần I giới thiệu chung, phần II sẽ tập trung trình bày về giải pháp bảo vệ truy cập mạng dựa trên BioPKI-KC, phần III sẽ giới thiệu về hệ thống nhận dạng vân tay C@FRIS, phân tích các yêu cầu bảo mật hệ thống C@FRIS và CSDL qua môi trường mạng, phần IV sẽ trình bày về xây dựng và triển khai các chức năng bảo mật dùng BioPKI cho hệ C@FRIS, phần V sẽ trình bày mô hình thử nghiệm và kết quả thử nghiệm hoạt động của hệ C@FRIS có tích hợp giải pháp BioPKI, bài báo sẽ kết thúc bằng kết luận và hướng phát triển.

II. GIẢI PHÁP BẢO VỆ TRUY CẬP MẠNG DỰA TRÊN BIOPKI

a/ Giới thiệu hệ thống BioPKI

Hệ thống an ninh thông tin BioPKI-KC là sản phẩm của đề tài KC.01.11/06-10 "Nghiên cứu xây dựng hệ thống kiểm soát truy cập mạng và an ninh thông tin dựa trên sinh trắc học sử dụng công nghệ nhúng". Hệ thống nền BioPKI-KC là một cơ sở hạ tầng khóa công khai tích hợp với hệ xác thực đa sinh trắc chủ thể người dùng sử dụng công nghệ nhúng (thẻ sinh trắc Bio-Etoken) để bảo vệ khóa cá nhân và các thông tin của người dùng [11]. Mô hình kiến trúc của hệ thống BioPKI-KC được trình bày trong hình 1.

Các thành phần của hệ thống bao gồm [11]:

- **Trung tâm phát hành chứng thư số - Certificate Authority (CA):** Chịu trách nhiệm quản lý và cung cấp các dịch vụ liên quan đến chứng thư số như: cấp mới, thu hồi, hủy, gia hạn chứng thư… Để đảm bảo an toàn hệ thống, CA được cách ly hoàn toàn với các thành phần khác trong môi trường mạng của hệ thống, mọi giao dịch của CA với các thành phần khác được thực hiện thông qua các thiết bị lưu trữ cá nhân như đĩa quang, bút nhớ. CA là thành phần hạt nhân quan trọng của hệ thống, được xây dựng bao gồm 2 bộ phận nhỏ sau:
  - **OpenCA:** Đây là lõi CA trong mô hình PKI thông thường, OpenCA là một hệ mã nguồn mở khá nổi

tiếng và đã được sử dụng tác nghiệp trong nhiều hệ thống PKI [11]. Trong hệ BioPKI, khối này cung cấp các dịch vụ lõi PKI liên quan đến quản lý chứng thư và cung cấp một giao diện quản trị

- **CA-Operator:** Đây là phần mềm trên máy PC làm công cụ dành cho người quản trị vận hành CA dùng để quản lý các hoạt động của OpenCA. CA-Operator chuyển các yêu cầu xin cấp phát chứng thư mới lên OpenCA và cũng nhận về từ CA các chứng thư cùng với khóa riêng để chuyển đến người dùng. Máy CA-Operator cũng chịu trách nhiệm ghi thông tin lên thẻ Bio-Etoken cho người dùng sử dụng trong các ứng dụng của hệ thống về sau này.

Hình 1. Mô hình hệ thống BioPKI-KC

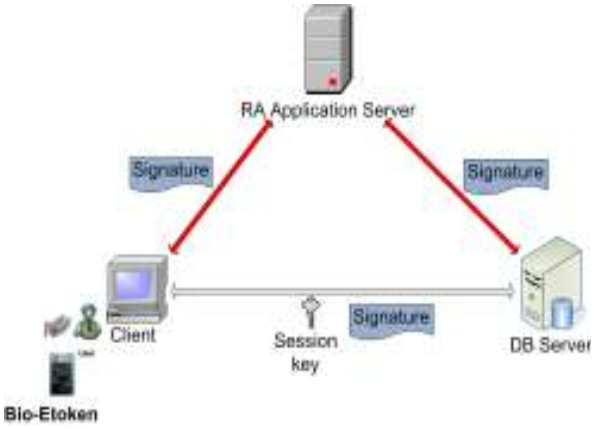
- **Registration Authority (Thẩm quyền đăng ký - RA):** Chịu trách nhiệm tiếp nhận và xử lý các yêu cầu của người dùng. Nó sẽ quyết định kết quả xử lý một yêu cầu xin cấp chứng thư mới (đồng ý hay không), nhận thẻ sinh trắc Bio-Etoken từ CA-Operator và chuyển xuống cho bộ phận dưới của hệ thống (các chi nhánh tiếp nhận đăng ký -LRA). RA cũng cung cấp các dịch vụ liên quan đến việc sử dụng chứng thư của người dùng khi họ giao dịch bằng các ứng dụng của hệ thống. RA được chia thành 3 bộ phận con:
  - **Registration Center:** Trung tâm đăng ký, tiếp nhận mọi yêu cầu về cấp phát và hủy chứng thư số
  - **Certificate Service Center:** Trung tâm dịch vụ chứng thư số, cung cấp các dịch vụ liên quan đến việc sử dụng chứng thư: xác thực chứng thư, download chứng thư…
  - **Website:** cổng thông tin để người dùng tra cứu, tìm kiếm các thông tin về quy trình xin cấp mới chứng thư, biểu mẫu, tra cứu trạng thái các đăng ký, tìm kiếm chứng thư và khóa công khai
- **Local Registration Authority (Chi nhánh tiếp nhận đăng ký - LRA):** đóng vai trò cầu nối giữa người dùng và RA. LRA trực tiếp nhận các yêu cầu đăng ký chứng thư mới, hủy chứng thư của người dùng và chuyển lên RA, nhận thẻ Bio-Etoken và chứng thư trả về cho người dùng.
- **Thẻ sinh trắc Bio-Etoken:** là một thiết bị nhúng cấp cho người dùng của hệ thống, trong đó các thông tin nhạy cảm của người dùng được lưu trữ và bảo vệ an toàn, bảo mật. Dữ liệu lưu trữ bao gồm:
  - Khóa riêng (khóa bí mật) của người dùng
  - Chứng thư số (khóa công khai)
  - Mã PIN để kích hoạt thẻ
  - Mã sinh trắc bảo vệ
  - Các thông tin cá nhân khác

Khi người dùng muốn đọc các thông tin trong thẻ, người đó phải được xác thực sinh trắc sống trực tiếp, nếu quá trình xác thực thành công thì các thông tin trong thẻ mới có thể được giải mã và đọc ra.

b/ Giải pháp bảo mật truy cập từ xa trên nền BioPKI-KC

Trong hạ tầng hệ thống BioPKI-KC, chúng tôi đã đề xuất một giải pháp bảo mật truy cập từ xa để bảo vệ các truy xuất vào một CSDL qua mạng [10]. Mô hình của giải pháp này được trình bày trong hình 2, bao gồm:

- **User**: một người dùng có quyền truy cập vào máy chủ CSDL. Người này đồng thời cũng là một user của hệ thống BioPKI, có một chứng thư số hợp lệ và một thẻ nhúng Bio-Etoken đã được cấp phát bởi CA từ trước.
- **Client:** Máy khách mà từ đây User sẽ truy cập từ xa vào máy chủ CSDL. Trên máy này sẽ được cài đặt một modun client của hệ thống bao gồm các chức năng chính sau: đọc thẻ và xác thực sinh trắc trực tuyến; thiết lập kết nối với thành phần RA Application Server (RAAS) và máy chủ CSDL (DB Server); tạo và xác thực chữ kỹ số; mã hóa và giải mã dữ liệu bằng thuật toán AES...



Hình 2. Giải pháp bảo mật truy cập trên nền hệ thống BioPKI-KC

- **RA Application Server** (Máy chủ dịch vụ - RAAS): Máy chủ ứng dụng là một thành phần trong Trung tâm dịch vụ (Certificate Service Center) của hệ thống BioPKI-KC. Nó cung cấp các chức năng chính sau: Thẩm định, xác thực sinh trắc và chứng thư số; sinh, quản lý và phân phối khóa phiên tới các máy khách client và máy chủ CSDL (DB Server).
- **DB Server**: Trên máy chủ này cài đặt modun server của hệ thống, bao gồm các chức năng sau: đọc thẻ Bio-Etoken và xác thực sinh trắc trực tuyến; kết nối với RAAS; quản lý user và các hoạt động của họ đối với các CSDL được cài đặt trên máy

chủ này; tạo log hệ thống; tạo và xác thực chữ ký số; mã hóa và giải mã dữ liệu bằng thuật toán AES…

Điều kiện tiên quyết:

Cả User của ứng dụng truy cập từ xa và DB Server đều được coi là các user của hệ thống BioPKI, như vậy họ đều phải được cấp một chứng thư số và một thẻ nhúng sinh trắc Bio-Etoken từ trước. Hệ thống BioPKI cung cấp các chứng thư, thẻ nhúng sinh trắc và các dịch vụ liên quan như kiểm tra, xác thực chứng thư... RAAS chịu trách nhiệm sinh và quản lý khóa phiên

c/ Ưu thế bảo mật của giải pháp đề xuất:

- Bảo mật username và password đăng nhập của user: Dùng xác thực sinh trắc với thẻ Bio-Etoken để tăng cường bảo mật cùng với password nhập từ bàn phím dựa trên nguyên tắc đối sánh tại chỗ bộ đặc điểm đa sinh trắc sống trích chọn từ các vân tay thu nhận online của người sử dụng với bộ đặc điểm chi tiết các mẫu thu nhận trước đó tại thời điểm khi người sử dụng lần đầu đăng ký vào hệ thống. Nhờ dùng vân tay để xác minh tại chỗ danh tính người sử dụng khi đăng nhập, truy cập tài nguyên hệ thống nên tránh được các trường hợp người này dùng username và password của người khác.

- Tăng cường bảo mật trên đường truyền: Nhờ sử dụng kênh mật SSL cho các giao dịch phân phối khóa phiên, đồng thời kết hợp thêm chữ ký số để xác thực tính toàn vẹn dữ liệu, giải pháp ngăn ngừa được kiểu tấn công "man-in-the-middle". Với các giao dịch trao đổi dữ liệu sau khi có khóa phiên giữa Client và DB Server, dữ liệu được mã hóa đối xứng, được gắn thêm chữ ký số và có thể tiếp tục truyền qua kênh SSL. Với việc sử dụng chữ ký số ứng dụng còn cung cấp chức năng chống phủ định hay chối bỏ trách nhiệm của người sử dụng, chống các tấn công khác liên quan đến phiên làm việc của người dùng…

III. YÊU CẦU BẢO MẬT HỆ THỐNG C@FRIS VÀ CSDL QUA MÔI TRƯỜNG MẠNG

a/ Đặt vấn đề

Vấn đề xây dựng và ứng dụng hệ C@FRIS để điện tử hóa hệ thống căn cước công dân (CCCD)/căn cước can phạm (CCCP) dùng mô hình mạng Client-Server truyền thống đã cơ bản giải quyết xong. Hệ C@FRIS đã triển khai cài đặt đầy đủ các tính năng từ khâu thu nhận, đăng ký chỉ bản thông tin đầu vào để xây dựng CSDL đến khâu kiểm tra chất lượng dữ liệu, tổ chức dữ liệu đến khâu tra cứu, khai thác hệ thống. Nhiệm vụ đặt ra là tổ chức thiết kế và cài đặt bổ sung cho hệ C@FRIS các tính năng bảo mật dùng công nghệ BioPKI. Để cài đặt các tính năng bảo mật, cần phải xem xét toàn diện tất cả các khâu của hệ thống trên cơ sở một chính sách bảo mật nhất quán, tuy nhiên báo cáo này không có tham vọng trình bày hết toàn bộ giải pháp bảo mật mà chỉ một số kết quả cài đặt cho những công đoạn quan trọng nhất [9]. Trên mô hình truyền thống của một hệ thống căn cước, có hai tiến trình chính hoạt động: Tiến trình xây dựng và tiến trình khai thác.

Đối với tiến trình xây dựng, tức là đăng ký từ đầu hay đăng ký bổ sung đối tượng mới vào CSDL, hệ thống sau khi nhập dữ liệu đầu vào, cần kiểm tra đảm bảo chất lượng dữ liệu, sau đó tiến hành tra cứu đối tượng đăng ký mới để kiểm tra đối tượng đã được cấp số căn cước hay chưa, nếu đã được cấp thì giải quyết cấp lại căn cước với số căn cước cũ và đồng thời cập nhật mới số liệu, nếu chưa được cấp thì giải quyết cấp số căn cước mới.

Đối với tiến trình khai thác, hệ thống tiếp nhận yêu cầu tra cứu từ xa trên mạng để xác minh căn cước. Có hai dạng yêu cầu cơ bản: Dạng thứ nhất là tra cứu chứng minh nhân dân (CMND) theo các trường dữ liệu cơ bản như: Số căn cước, họ, tên, năm sinh, tên bố, tên mẹ, rồi thẩm định (1:1) theo vân tay 2 ngón trỏ; Dạng thứ hai là tra cứu truy tìm danh tính cá thể đối tượng (1:N) chỉ theo chỉ bản 10 ngón (TP/TP). Các yêu cầu khai thác đều được diễn đạt dưới dạng các câu hỏi SQL có sử dụng các hàm đối sánh vân tay theo bộ điểm đặc trưng chi tiết.

Trên môi trường mạng INTERNET/INTRANET, hệ thống CCCD có thể phục vụ công tác cải cách thủ tục hành chính công dưới dạng các dịch vụ sau:

- Dịch vụ đăng ký xin cấp CMND trên mạng INTERNET: Trên trang WEB dịch vụ này, thủ tục xin cấp mới hay cấp đổi lại CMND dự kiến được tiến hành theo các bước sau:
  - Công dân truy cập vào trang WEB, nhập thông tin vào Tờ khai CMND điện tử và ký xác nhận.
  - Hệ thống tiếp nhận tờ khai online, mật mã hoá thông tin tờ khai và thể hiện dưới dạng mã vạch 2 chiều để công dân đăng ký in tờ khai ra máy in (có mã vạch 2 chiều cùng bản rõ tờ khai) cùng giấy hẹn đến trụ sở CA Quận/Huyện để giải quyết tiếp. Lúc này công dân đã khai các thông tin nhân thân cơ bản, chưa có ảnh và vân tay.
  - Tại trụ sở CA Quận/Huyện, công dân chỉ cần trình tờ khai đã in ra, hệ thống giải mã mã vạch và đối chiếu với bản tờ khai rõ, nếu khớp, tiến hành lăn tay chụp ảnh (trong vòng 3-5 phút/1 công dân). Công dân lấy giấy hẹn để đến nhận CMND.
- Dịch vụ Tra cứu xác minh CMND trên mạng INTERNET

Cơ quan công chứng, cơ quan thuế, hàng không, ngoại giao, công an quản lý hành chính, quản lý xuất nhập cảnh, cửa khẩu,... đều có nhu cầu cần kiểm tra, xác minh nhanh danh tính công dân thông qua đối chiếu thông tin trên CMND xuất trình với bản CMND gốc do cơ quan công an quản lý trên mạng để đề phòng các hiện tượng giả mạo danh tính trong giao dịch.

b/ ***Các yêu cầu bảo mật cơ bản***

Để triển khai các ứng dụng trên, hệ thống "hậu trường" cần đáp ứng được hai yêu cầu: Vừa xử lý nhanh chóng, đảm bảo yêu cầu nghiệp vụ hành chính vừa phải đảm bảo an ninh an toàn cho hệ thống. Trên hệ thống căn cước điện tử hóa, việc áp dụng công nghệ bảo mật cần dựa trên các nguyên tắc, chính sách bảo mật nhất quán, tương tự như đối với công tác quản lý bảo mật văn bản hành chính và qui chế bảo mật văn bản hiện hành [9].

Việc ứng dụng công nghệ BioPKI bảo mật cho hệ CCCD, cần đáp ứng một số yêu cầu cơ bản sau:

- Thực hiện việc kiểm soát thẩm quyền truy cập dùng vân tay để đảm bảo đúng danh tính chủ thể, xác thực

mật mã hai chiều cho mỗi phiên làm việc, dùng chữ ký số và chữ ký số sinh trắc để đảm bảo nguồn gốc và sự toàn vẹn dữ liệu, mật mã hóa dữ liệu không chỉ trong quá trình vận chuyển, truyền trên mạng mà còn trong các khâu xây dựng, khai thác và vận hành hệ thống nhằm bảo mật chặt chẽ CSDL tránh bị lợi dụng, xâm nhập trái phép, kể cả khi bị sao chép hay bị lọt ra ngoài.

- Hệ thống phải có khả năng tự động lập nhật ký hệ thống, kiểm soát các tiến trình giao dịch, kiểm soát truy cập đến các tệp tin, biết được ai, cái gì, khi nào, ở đâu, tác động như thế nào với các tệp tin và các giao dịch đó, đảm bảo dễ dàng truy cứu trách nhiệm khi cần.

IV. XÂY DỰNG VÀ TRIỂN KHAI CÁC CHỨC NĂNG BẢO MẬT DÙNG BIOPKI CHO HỆ C@FRIS

Trên cơ sở mô hình nêu trên, các chức năng chính của ứng dụng cần xây dựng sẽ là: (1) Kiểm soát đăng nhập hệ thống, (2) Thiết lập kênh truyền dữ liệu bảo mật, (3) Truyền khóa phiên bảo mật, (4) Kiểm soát truyền dữ liệu bảo mật, bao gồm mật mã hóa/giải mã và ký số/xác thực chữ ký số.

IV.1 Xây dựng và triển khai các chức năng bảo mật

a/ ***Phân tích các chức năng***

- **Chức năng kiểm soát đăng nhập hệ thống:**
  - Kiểm tra mật khẩu đăng nhập vào ứng dụng ở máy client của người dùng.
  - Đối sánh đặc trưng sinh trắc: Sử dụng thiết bị Biometrika để thu nhận vân tay sống của người sử dụng, sau đó trích chọn đặc điểm để đối sánh với bộ đặc điểm lưu trong thẻ Bio-Etoken của người đó.
- **Chức năng thiết lập kênh truyền tin bảo mật:**
  - Thiết lập kênh truyền dữ liệu bảo mật SSL tay ba: giữa RA Application Server và DB Server, giữa Client và RA Application Server, giữa Client và DB Server.
  - Nếu kết quả đăng nhập của người sử dụng là thành công thì lấy được khóa riêng và chứng thư của họ, khóa riêng và chứng thư sẽ được dùng để thiết lập kênh truyền dữ liệu bảo mật SSL giữa Client và RA Application Server, giữa Client và DB Server.
  - Kênh mật chỉ được thiết lập nếu mỗi bên đều được cung cấp chứng thư, khóa riêng. Trong quá trình thiết lập kênh sẽ sử dụng chứng thư của CA để tiến hành kiểm tra hiệu lực của chứng thư và khóa riêng này. Nếu vẫn còn hiệu lực, thì chúng sẽ được sử dụng để mã hóa và giải mã bất đối xứng các thông điệp đã bắt tay.
- **Chức năng truyền khóa phiên bảo mật:**
  - Việc đảm bảo tính mật của khóa phiên có ý nghĩa vô cùng quan trọng.
  - Khóa phiên do RA Application Server sinh ra sẽ được mã hóa khóa bất đối xứng và ký số trước khi được truyền trên kênh mật tới máy Client, DB Server.
- **Chức năng kiểm soát truyền dữ liệu bảo mật:**

Xét quá trình gửi dữ liệu từ DB Server tới Client:

- Đầu tiên DB Server sẽ mã hóa dữ liệu bằng khóa phiên (do RA Server Application gửi sang), sau đó thực hiện ký số lên dữ liệu mã hóa và gửi tới Client thông qua kênh truyền bảo mật SSL.
- Tại phía Client, khi nhận được dữ liệu, đầu tiên sẽ xác thực chữ ký của DB Server, nếu xác thực chữ ký thành công thì Client sẽ sử dụng khóa phiên (do RA Server Application gửi sang) để giải mã.
- Sau khi giải mã, nếu dữ liệu phù hợp với định dạng quy định trước thì kết quả mà người dùng nhận được là chính xác do DB Server gửi sang.

Xét quá trình gửi dữ liệu từ Client đến DB Server:

- Client mã hóa dữ liệu bằng khóa phiên (do RA Server Application gửi sang), sau đó thực hiện ký số lên dữ liệu mã hóa và gửi tới DB Server thông qua kênh truyền bảo mật SSL.
- Tại phía DB Server, khi nhận được dữ liệu, đầu tiên sẽ xác thực chữ ký của Client, nếu xác thực chữ ký thành công thì DB Server sẽ sử dụng khóa phiên (do RA Server Application gửi sang) để giải mã.
- Sau khi giải mã, nếu dữ liệu phù hợp với định danh quy định trước thì kết quả mà DB Server nhận được chính xác là do Client gửi sang.

b/ Xây dựng bộ công cụ phát triển BioPKI SDK

Bộ công cụ SDK này được xây dựng và lập trình dựa trên việc sử dụng sau:

- Sử dụng ngôn ngữ phát triển hệ thống là C++ (VC++, .Framework 3.0) vì nó vừa hỗ trợ hướng đối tượng vừa tích hợp được các hàm viết bằng ngôn ngữ C trong thư viện OpenSSL.
- Thư viện mã nguồn mở OpenSSL để xây dựng các module mật mã hóa, giải mã, ký số, xác thực chữ ký và truyền thông điệp qua kênh SSL. Hơn nữa, thư viện OpenSSL còn là một thành phần của OpenCA.
- Sử dụng 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.
- Ngoài ra, hệ thống cũng sử dụng các API có sẵn do hệ BioPKI-KC cung cấp, cụ thể:
  - Các APIs làm việc với thẻ sinh trắc Bio-Etoken.
  - Các APIs ký và xác thực chữ ký số.
  - Giải pháp hệ thống:

Xây dựng các module phần mềm cho Client, RA Application Server và DB Server.

− **Client**:

- Module đọc thẻ và xác thực sinh trắc (Sử dụng các API có sẵn do hệ BioPKI - KC cung cấp).
- Các hàm băm, mã hóa và giải mã đối xứng bằng thuật toán AES mật khẩu truy cập từ xa bằng khóa phiên, mã hóa và giải mã bất đối xứng. Ở đây thuật toán mã hóa AES cho phép làm việc với khóa có độ

dài bất kỳ. Sử dụng các hàm có sẵn của thư viện OpenSSL để thực hiện mã hóa và giải mã khóa bất đối xứng.
- Module ký và xác thực chữ ký: chữ ký của RA Application Server, chữ ký của DB Server (Sử dụng các API có sẵn do hệ BioPKI-KC cung cấp).
- Module thiết lập kênh mật SSL. Sử dụng các hàm trong thư viện OpenSSL để thiết lập.

− **RA Application Server:**
- Module cung cấp dịch vụ ứng dụng liên quan đến chứng thư số (check valid, download…) tận dụng luôn của RA Server trong hệ thống BioPKI.
- Module sinh khóa phiên, quản lý, phân phối và hủy khóa phiên.
- Module thiết lập kênh mật SSL.

− **DB Server:**
- Các hàm băm, mã hóa và giải mã đối xứng bằng thuật toán AES mật khẩu truy cập từ xa bằng khóa phiên, mã hóa và giải mã bất đối xứng.
- Module ký và xác thực chữ ký.
- Module làm việc với CSDL.
- Module thiết lập kênh mật SSL.

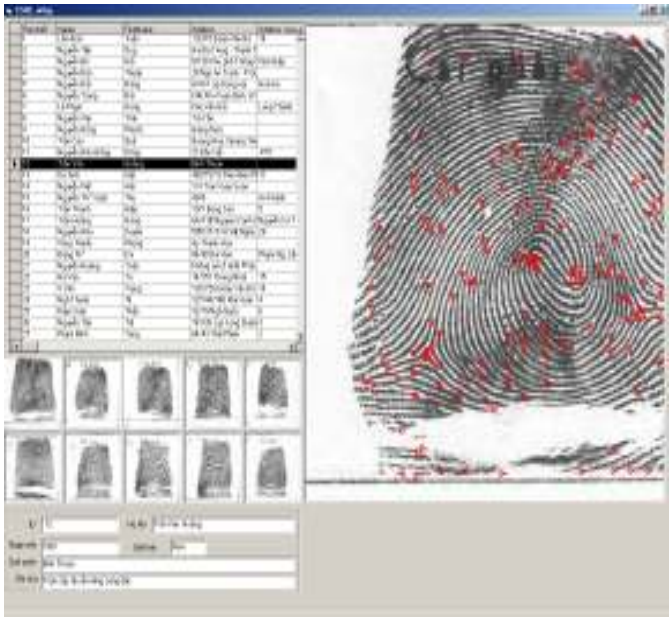
Một số nhóm hàm được xây dựng trong bộ SDK:
- Nhóm hàm sử dụng để thiết lập kênh mật SSL;
- Nhóm hàm thực hiện ký và xác thực chữ ký;
- Nhóm hàm mã hóa/giải mã khóa đối xứng AES;
- Nhóm hàm làm việc với CSDL.

IV.2 Xây dựng bảo mật các phân hệ của hệ C@FRIS

a/ Bảo mật phân hệ C@FRIS Scan

Phân hệ phần mềm nhập chuyển đổi số hóa chỉ bản của hệ C@FRIS được cài đặt trên các máy trạm Client của mạng LAN được kết nối với máy chủ CSDL. Người sử dụng được đăng ký và cấp thẩm quyền với vai trò nhân viên nhập chuyển đổi thông tin số hóa có các quyền sau:
- Được kết nối với máy chủ CSDL, khởi tạo bảng CSDL, điều khiển máy quét scanner nhập chuyển đổi số hóa chỉ bản và lưu kết quả vào CSDL.
- Được tiến hành nhập thông tin thuộc tính về nhân thân đối tượng (số hồ sơ, họ tên, giới tính, năm sinh, nơi đăng ký HKTT, ... của đối tượng). Tiếp đó là nhập các thông tin về vân tay như: Dạng cơ bản, số đếm vân, ... và tự động cắt ảnh chỉ bản thành mười ngón riêng rẽ.
- Được dùng bộ duyệt CSDL (BROWSER) để truy cập, chỉnh sửa, bổ sung các bản ghi dữ liệu thuộc tính.
- Được nhập CSDL hợp chuẩn ANSI/NIST từ các hệ AFIS khác.
- Được xuất CSDL C@FRIS sang dạng chuẩn ANSI/NIST để nhập vào hệ AFIS khác.

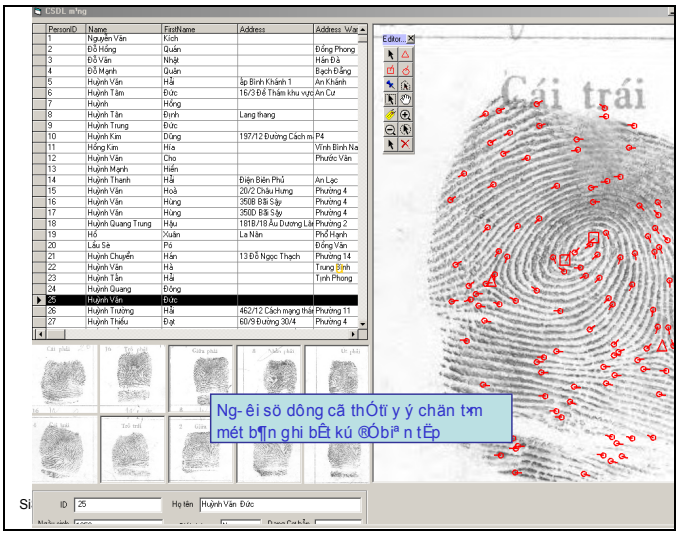
Tính năng bảo mật được cài đặt bổ sung:
- Kiểm soát đăng nhập phần mềm C@FRIS Scan;
- Kiểm soát truy cập máy chủ CSDL;
- Người sử dụng với vai trò là nhân viên chuyển đổi thông tin số hóa cần ký vào các trường, (hay để rút gọn có thể ký chung cho tổ hợp một số trường dữ liệu) do mình tạo ra, cụ thể là các trường: Số căn cước đối tượng, họ tên, giới tính, năm sinh, địa phương, mã số ngón, dạng cơ bản, số đếm vân, ảnh vân tay đối tượng.
- Chức năng xử lý trích chọn đặc điểm tự động do hệ thống thực hiện nên hệ thống là chủ thể chịu trách nhiệm ký, xử lý nén, mật mã hóa dữ liệu của trường lưu đặc điểm chi tiết của record tương ứng.
- Riêng trường ảnh gốc sau khi nhân viên nhập liệu ký chịu trách nhiệm cắt ảnh, hệ thống tiếp tục xử lý nén, mật mã hóa và ký xác nhận.
- Tất cả các giao tác của hệ thống và của nhân viên nhập chuyển đổi thông tin số hóa đều được ghi vào CSDL nhật ký hệ thống. Bản thân cơ sở dữ liệu này được bảo mật như "hộp đen" của hệ thống và chỉ người được cấp thẩm quyền mới truy cập được.



Hình 4. Tất cả các bản ghi CSDL đều được NSD ký sinh trắc, ảnh vân tay công dân và bộ đặc điểm chi tiết được hệ thống xử lý nén, mật mã hóa và ký xác nhận trách nhiệm.

b/ Bảo mật phân hệ "Biên tập và kiểm tra chất lượng"

Phân hệ "**Biên tập và kiểm tra chất lượng**" được trang bị trình duyệt CSDL với nhiều công cụ tiện ích để người sử dụng được cấp thẩm quyền biên tập và kiểm tra chất lượng thực hiện các thao tác truy vấn CSDL trên máy chủ, truy cập đến từng bản ghi để biên tập các thông tin thuộc tính và đồ họa.



Hình 3. Biên tập đặc điểm chi tiết và ký sinh trắc vào bản ghi trước khi lưu vào CSDL.

- Bộ đặc điểm chi tiết ban đầu do hệ thống tự động xử lý nên hệ thống là chủ thể ký bảo mật trường dữ liệu này. Trường hợp bộ đặc điểm chi tiết được biên tập lại thì người có thẩm quyền biên tập là người ký (dùng chữ ký số) chịu trách nhiệm phần biên tập.
- Sau khi biên tập và ký lưu, chính hệ thống là chủ thể xử lý nén, mật mã hóa, nên hệ thống tiến hành ký xác nhận công đoạn này.
- Các bảng dữ liệu sau kiểm tra chất lượng được coi là hoàn chỉnh, cũng được hệ thống ký xác nhận để đảm bảo tính toàn vẹn dữ liệu.

c/ Bảo mật phân hệ "Tổ chức cơ sở dữ liệu"

Phân hệ này đảm bảo chức năng quản lí và tổ chức CSDL cài đặt trên máy chủ của một mạng LAN tổ chức theo mô hình Client-Server để phục vụ khai thác.

Người sử dụng được cấp thẩm quyền Tổ chức CSDL được phép truy cập CSDL trên máy chủ, được phân loại, tổ chức thành nhiều bảng dẫn xuất, được đánh chỉ số phân cấp nhằm tăng tốc truy xuất dữ liệu. Các kết quả tổ chức CSDL đều được ký sinh trắc bởi quản trị viên và bởi hệ thống.

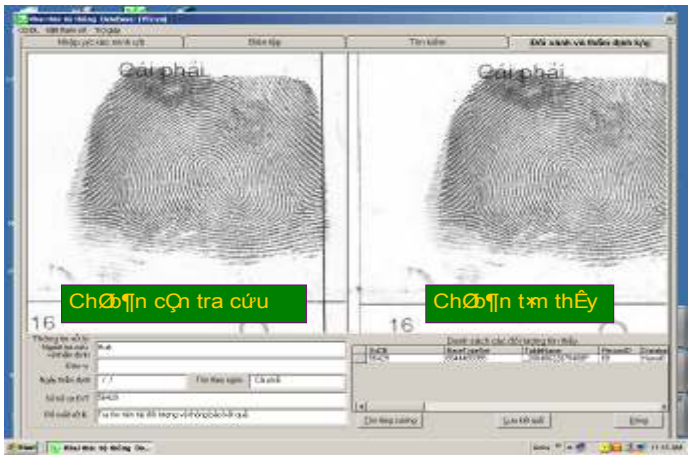
Trên các máy trạm, người được cấp thẩm quyền Tổ chức CSDL được phép truy vấn CSDL bằng câu lệnh SQL, xử lý kết nối các bảng, đánh chỉ số, lập báo cáo, thống kê, kiểm kê hệ thống.

Tất cả các giao tác của quản trị viên được hệ thống tự động lưu vào CSDL nhật ký hệ thống.

d/ Phân hệ "Tra tìm, Đối sánh"

Người được cấp thẩm quyền Tra tìm, Đối sánh để xác minh căn cước, được phép đăng nhập phần mềm, truy cập đến máy chủ CSDL để tiến hành hai dạng yêu cầu chủ yếu sau:

- Xác minh theo chỉ bản vân tay 10 ngón.
- Xác minh theo số căn cước, họ tên, ngày tháng năm sinh, sau đó thẩm định theo vân tay 2 ngón trỏ.

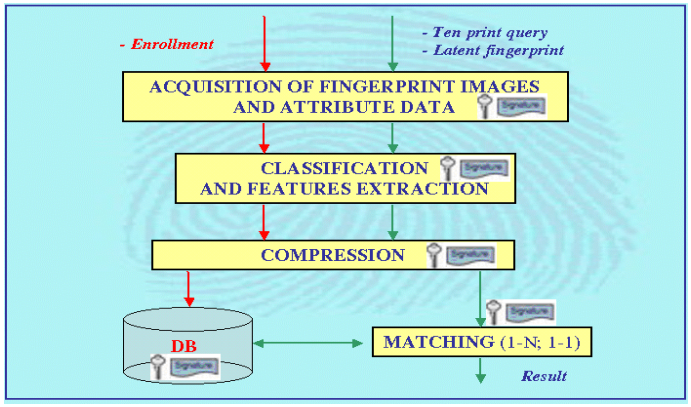


Hình 5. Kết quả Tra tìm, Đối sánh TP-TP được ký sinh trắc, lưu vào CSDL kết quả tra cứu.

Người sử dụng với vai trò tra cứu, đối sánh được yêu cầu ký xác nhận lập yêu cầu tra cứu, xác nhận việc nhận kết quả tra cứu. Hệ thống ký xác nhận đã tiếp nhận yêu cầu, đã tra cứu và cung cấp kết quả.

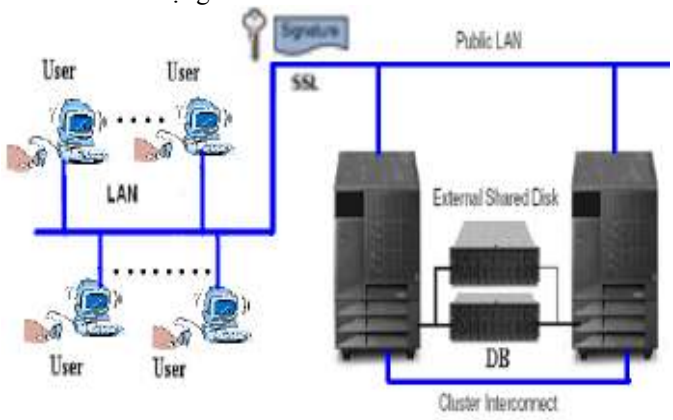
V. KẾT QUẢ THỰC NGHIỆM

Sơ đồ mô hình thử nghiệm hoạt động của hệ C@FRIS có tích hợp giải pháp BioPKI được trình bày trong các hình dưới đây.



Hình 6. Mô hình thử nghiệm hệ C@FRIS có tích hợp giải pháp BioPKI

Sơ đồ kết nối mạng:



Hình 7. Sơ đồ kết nối mạng

So sánh các kết quả thử nghiệm hệ thống C@FRIS trước và sau khi tích hợp giải pháp bảo mật BioPKI. Các kết quả so sánh trong các trường hợp thử nghiệm được trình bày trong các bảng dưới đây.

STT	Các tính năng	Hệ C@FRIS cũ	Hệ C@FRIS mới
1	Kiểm soát thẩm quyền tạo lập CSDL, quét nhập, mã hoá và cập nhật chỉ bản 10 ngón	Dùng password	Dùng vân tay và chữ ký số
2	Kiểm soát thẩm quyền tạo lập CSDL	Không có	Ký lên file CSDL
3	Lưu bảo mật ảnh và kiểm tra tính hợp lệ (thứ tự) ảnh các ngón tay trên chỉ bản.	Không có	Ký lên ảnh nén
4	Nhập và bảo mật đường truyền trong quá trình truyền/ nhận dữ liệu	Không có	Đang thực hiện…
5	Nhập thông tin thuộc tính, dạng cơ bản,…	Không có	Ký lên các trường tương ứng.
6	Duyệt browser CSDL	Không có	Xác thực thẩm quyền sử dụng xác thực chứng thư số
7	Biên tập CSDL	Không có	Xác thực thẩm quyền sử dụng xác thực chứng thư số
8	Nhập/ xuất CSDL hợp chuẩn ANSI/NIST của các hệ AFIS khác	Không có	Xác thực thẩm quyền sử dụng xác thực chứng thư số

Bảng 1. Bảng đánh giá so sánh các tính năng đạt được, tính năng đang nâng cấp của phân hệ tạo lập CSDL

STT	Các tính năng	Hệ C@FRIS cũ	Hệ C@FRIS mới
1	Kiểm soát thẩm quyền mã hoá dữ liệu	Dùng password	Dùng vân tay và chữ ký số
2	Theo dõi và quy trách nhiệm	Không có	Có
3	Lưu bảo mật bộ đặc điểm chi tiết	Không có	Có
4	Bảo mật đường truyền trong quá trình truyền/ nhận dữ liệu	Không có	Có

Bảng 2. Bảng đánh giá so sánh các tính năng đạt được, tính năng đang nâng cấp của phân mã hoá đặc điểm chi tiết tự động sau khi đưa vào thử nghiệm thực tế

STT	Các tính năng	Hệ C@FRIS cũ	Hệ C@FRIS mới
1	Kiểm soát thẩm quyền biên tập	Không có	Có
2	Theo dõi và quy trách nhiệm	Không có	Có
3	Bảo mật bộ đặc điểm chi tiết	Không có	Có
4	Bảo đảm tính toàn vẹn dữ liệu	Không có	Có
5	Bảo mật đường truyền trong quá trình truyền/ nhận dữ liệu	Không có	Có
6	Phục hồi bản ghi bị xoá gần nhất	Không có	Có

Bảng 3. Bảng đánh giá so sánh các tính năng đạt được của phân hệ "Biên tập và kiểm tra chất lượng"qua quá trình đánh giá thử nghiệm thực tế

STT	Các tính năng	Hệ C@FRIS cũ	Hệ C@FRIS mới
1	Kiểm soát thẩm quyền	Không có	Sử dụng BioPKI
2	Bảo mật các bảng dẫn xuất	Không có	Có
3	Bảo đảm tính toàn vẹn dữ liệu	Không có	Có
4	Bảo mật đường truyền trong quá trình truyền/ nhận dữ liệu	Không có	Có

Bảng 4. Bảng đánh giá so sánh các tính năng đạt được của phân hệ "Tổ chức cơ sở dữ liệu" qua quá trình đánh giá thử nghiệm thực tế

STT	Các tính năng	Hệ C@FRIS cũ	Hệ C@FRIS mới
1	Kiểm soát thẩm quyền đăng nhập, tạo lập CSDL quản lý YC	Không có	Dùng vân tay và chữ ký số
2	Lưu bảo mật ảnh và kiểm tra tính hợp lệ (thứ tự) ảnh các ngón tay trên chỉ bản vào CSDL YC.	Không có	Ký lên ảnh nén
3	Nhập và bảo mật đường truyền trong quá trình	Không có	Có

	truyền/ nhận dữ liệu		
4	Nhập thông tin thuộc tính, dạng cơ bản,… cho CSDL YC	Không có	Ký lên các trường tương ứng.
5	Duyệt browser CSDL YC	Không có	Xác thực thẩm quyền sử dụng xác thực chứng thư số
6	Biên tập CSDL YC	Không có	Xác thực thẩm quyền sử dụng xác thực chứng thư số
7	Gửi YC tra cứu	Không có	Ký vào bản ghi YC
8	Nhận và phân phối YC tra cứu	Không có	Có

Bảng 5. Bảng đánh giá so sánh các tính năng đạt được, tính năng đang nâng cấp của phân hệ "Tra tìm, đối sánh

STT	Các tính năng	Bảo mật Phân hệ tiếp nhận, xử lý và trả lời của hệ C@FRIS cũ	Bảo mật Phân hệ tiếp nhận, xử lý và trả lời của hệ C@FRIS mới
1	Xác thực YC	Không có	Xác thực chữ ký số
2	Bảo mật kết quả	Không có	Ký lên ảnh nén
3	Bảo mật đường truyền trong quá trình truyền dữ liệu	Không có	Có

Bảng 6. Bảng đánh giá so sánh các tính năng đạt được, tính năng đang nâng cấp của phân hệ "Tiếp nhận, xử lý và trả lời các yêu cầu"

VI. KẾT LUẬN

Trong bài báo này chúng tôi đã đề xuất giải pháp bảo mật kiểm soát truy cập CSDL qua mạng dựa trên hệ thống BioPKI trong khuôn khổ đề tài KC.01.11/06-10 và triển khai thử nghiệm các tính năng bảo mật cho hệ C@FRIS trên cơ sở ứng dụng bộ công cụ bảo mật BioPKI của đề tài. Báo cáo đã trình bày một số kết quả cài đặt tính năng bảo mật như: kiểm soát đăng nhập hệ thống, kiểm soát truy cập CSDL, tính năng dùng chữ ký số sinh trắc để ký vào dữ liệu mức bản ghi, mức cấu trúc các bảng CSDL, xác thực chữ ký và tính năng mật mã hóa/giải mã các giao dịch trên đường truyền, khi sao lưu bảo quản, bảo mật, bảo hiểm CSDL.

C@FRIS là sản phẩm phần mềm nhận dạng vân tay tự động của Phòng Thí nghiệm Mô phỏng và Tích hợp hệ thống Bộ Công an, đã được xây dựng và đưa vào ứng dụng để điện tử hóa các loại tàng thư chỉ bản vân tay của hệ thống căn cước công dân (CCCD) và căn cước can phạm (CCCP). Do tính chất cơ mật của thông tin căn cước và thông tin nhân thân của đối tượng đưa vào quản lý, hệ C@FRIS có nhu cầu bức thiết phải bổ sung tính năng bảo mật mang tính chuyên nghiệp để bảo mật hệ thống. Kết quả thử nghiệm đạt được nhiều triển vọng ứng dụng trong thực tế. Nhờ ứng dụng các tính năng của giải pháp BioPKI, việc bảo mật trên hệ C@FRIS sẽ được đảm bảo chặt chẽ mà vẫn giữ được tính dễ dùng trong các khâu xây dựng, khai thác và vận hành hệ thống trên thực tế.

LỜI CẢM ƠN

Công trình nghiên cứu này được triển khai trong khuôn khổ đề tài nghiên cứu KHCN cấp nhà KC.01.11/06-10 thuộc Chương trình KH &CN trọng điểm cấp nhà nước giai đoạn 2006-2010 "Nghiên cứu, phát triển và ứng dụng Công nghệ Thông tin và Truyền thông", mã số KC.01/06-10. Nhóm tác giả trân trọng cảm ơn sự hỗ trợ của đề tài, sự cộng tác nghiên cứu và các ý kiến đóng góp của tất cả các chuyên gia và các đồng nghiệp.

REFERENCES

[1] Alex Stoianow, Ann Cavoukian, Biometric Encryption: A positive – Sum Technology that Achieves Strong Authentication, Security AND Privacy, Information and Privacy Commissioner/Ontario, March 2007

[2] 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.

[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] Uludag, Anil K. Jain et al "Biometric Cryptosystems: Issues and Challenges", Proceedings of the IEEE, Vol.92, No. 6, pp. 948-960, June 2004

[6] [D.Maltoni, D.Maio, A.K.Jain, S.Prabhakar, Handbook of Fingerprint Recognition, Springer, New York, 2003.

[7] W. J. Scheirer and T. E. Boult, "Bio-cryptographic protocols with bipartite biotokens", Biometrics Symposium (BSYM)Tampa, Florida, 23-25 September 2008.

[8] William Stallings, "Cryptography and Network Security Principles and Practices, Fourth Edition". Prentice Hall, November 16, 2005

[9] Nguyễn Ngọc Kỷ, Nguyễn Thị Hương Thủy, Nguyễn Thanh Phương, Nguyễn Việt Tiệp, "Kết quả nghiên cứu ứng dụng công nghệ nhận dạng vân tay để tự động hóa các hệ thống căn cước công dân và căn cước can phạm". Kỷ yếu Hội nghị CNTT CAND, Hà Nội 9-2004

[10] Nguyen Thi Hoang Lan, Nguyen Van Toan, "BioPKI model and Remote Access Control using Bio-Etoken in BioPKI System", IEEE-RIVF 2010 Addendum Contribution Proceeding, pp.50-53. November 1-4, 2010.

[11] Nguyễn Thị Hoàng Lan và các cộng sự, "Nghiên cứu ứng dụng hệ thống kiểm soát truy cập mạng và an ninh thông tin dựa trên sinh trắc học sử dụng công nghệ nhúng". Báo cáo đề tài nghiên cứu KH&CN cấp nhà nước KC.01.11/06-10, Hà Nội 11/2010, Cục Thông tin khoa học và công nghệ quốc gia, số đăng ký: 2011-52-402 /KQNC.