Tạp chí Khoa học ĐHQGHN, Khoa học Tự nhiên và Công nghệ 27 (2011) 37-51

Xác thực hộ chiếu sinh trắc với cơ chế PACE và EAC

Vũ Thị Hà Minh, Nguyễn Ngọc Hoá*

Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội, 144 Xuan Thủy, Hà Nội, Việt Nam

Nhận ngày 18 tháng 3 năm 2011

Tóm tắt. Hộ chiếu sinh trắc đã trải qua ba thế hệ phát triển, từ ban đầu chỉ chú trọng lưu ảnh mặt người trên chip, kết hợp thêm một số nhân tố sinh trắc và cơ chế kiểm soát truy cập mở rộng EAC và bổ xung cơ chế thiết lập kết nối có xác thực mật khẩu PACE. Trong bài báo này, chúng tôi trình bày về mô hình xác thực hộ chiếu sinh trắc dựa trên hai cơ chế PACE và EAC và tiến hành thử nghiệm các bước quan trọng trong mô hình này. Một số đánh giá về hiệu năng cũng như tính an ninh/an toàn của mô hình cũng được phân tích trong bài báo này

Từ khoá: xác thực sinh trắc học, hộ chiếu sinh trắc, kiểm soát truy cập mở rộng, kiểm soát truy cập cơ bản, RFID, PKI.

1. Giới thiệu

Hộ chiếu sinh trắc (biometric passport - HCST), hay còn gọi là hộ chiếu điện tử (ePassport) là một giấy căn cước cung cấp thông tin theo thời kỳ (khoảng 10 năm, tuỳ theo mỗi nước quy định) về một công dân, dùng để thay thế cho hộ chiếu truyền thống. Mục tiêu chính của HCST là nâng cao an ninh/an toàn trong quá trình cấp phát/kiểm duyệt/xác thực hộ chiếu [1]. Với mục tiêu đó, hộ chiếu sinh trắc được phát triển dựa trên những chuẩn về hộ chiếu thông thường, kết hợp cùng với (i) các kỹ thuật đảm bảo an ninh/an toàn thông tin, (ii) công nghệ định danh dựa trên tần số radio (Radio Frequency Identification- RFID) và (iii) công nghệ xác thực dựa trên những nhân tố sinh trắc học như ảnh mặt người, vân tay, mống mắt… Hai yếu tố đầu cho phép nâng cao việc chống đánh cắp thông tin cá nhân, chống làm giả hộ chiếu,..; còn hai yếu tố sau cho phép nâng cao hiệu quả quá trình xác thực công dân mang hộ chiếu sinh trắc [2].

HCST đã được nghiên cứu và đưa vào triển khai, ứng dụng thực tế ở một số quốc gia phát triển trên thế giới như: Mỹ, Châu Âu… [3] Gần đây chính phủ Việt Nam cũng đã phê duyệt đề án quốc gia "Sản xuất và phát hành hộ chiếu điện tử Việt Nam" với kỳ vọng bắt đầu từ năm 2011 có thể xây dựng thử nghiệm HCST [4].

Hiện nay trên thế giới, HCST đã trải qua ba thế hệ phát triển: từ việc mới chỉ sử dụng ảnh mặt người số hoá lưu trên một chip RFID (thế hệ thứ nhất) [1], kết hợp thêm một số nhân tố sinh trắc và cơ chế kiểm soát truy cập mở rộng (Extended Access Control – EAC; thế hệ thứ hai) [2] và bổ xung cơ chế thiết lập kết nối có xác thực mật khẩu (Password Authenticated Connection Establishment – PACE; thế hệ thứ 3, bắt đầu từ cuối năm 2009) [5]. Tại Việt Nam, mới chỉ có một số dự án nghiên cứu, tìm hiểu liên quan đến mô hình cấp phát, quản lý, kiểm

* Tác giả liên hệ. ĐT: 84-4-37547813.
E-mail: hoa.nguyen@vnu.edu.vn

duyệt HCST [6]. Các nghiên cứu này bước đầu đã nghiên cứu các cơ chế bảo mật sử dụng trong HCST, đồng thời đề xuất ra mô hình HCST sử dụng tại Việt Nam. Tuy nhiên việc nghiên cứu trên mới dừng ở mô hình phát triển thế hệ thứ hai.

Trong bài báo này, chúng tôi tập trung nghiên cứu, tìm hiểu quy trình xác thực HCST theo chuẩn của tổ chức ICAO (International Civil Aviation Orgnization) ở ***thế hệ thứ ba***, với định hướng đặc biệt chú trọng đến cơ chế PACE và EAC nhằm tăng cường an ninh/an toàn trong quá trình xác thực HCST. Trên thực tế mô hình này chưa được áp dụng ở bất kỳ nước nào trên thế giới, mới dừng ở phạm vi nghiên cứu. Với việc nghiên cứu, tìm hiểu quy trình xác thực sử dụng cơ chế PACE và EAC, từ đó tiến hành thực nghiệm mô hình xác thực nói trên, chúng tôi kỳ vọng có thể tiếp cận được những nghiên cứu mới nhất về HCST trên thế giới, từ đó có thể cung cấp, xây dựng phần nào những cơ sở nền tảng về HCST tại Việt Nam.

Các phần còn lại của bài báo được tổ chức như sau: phần 2 trình bày tổng quan về các công nghệ liên quan và tổ chức của HCST; phần 3 đánh giá các thế hệ của HCST từ đó đưa ra mô hình xác thực HCST sử dụng cơ chế PACE và EAC ở phần 4; phần thử nghiệm và đánh giá được trình bày ở hai phần kế tiếp. Phần cuối cùng là những đánh giá kết luận và một số hướng phát triển kế tiếp.

2. Lý thuyết liên quan

2.1. Các công nghệ trong HCST

HCST được xây dựng kết hợp chủ yếu ba công nghệ chính: định danh sử dụng tần số vô tuyến (RFID), cơ sở hạ tầng khoá công khai (Public Key Infrastructures – PKI) và xác thực sinh trắc học.

a) Định danh sử dụng tần số vô tuyến

RFID là công nghệ nhận dạng đối tượng bằng sóng vô tuyến. Công nghệ này cho phép nhận biết các đối tượng thông qua hệ thống thu phát sóng vô tuyến, từ đó có thể giám sát, quản lý hoặc lưu vết từng đối tượng.

Hệ thống RFID bao gồm thiết bị đơn giản (gọi là thẻ, để lưu dữ liệu, định danh) nhỏ gọn và rẻ, và thiết bị phức tạp (gọi là đầu đọc). Thẻ thường được sản xuất với số lượng lớn và đính vào các đối tượng cần quản lý, điều hành tự động. Đầu đọc có nhiều tính năng hơn và thường kết nối với máy tính hoặc mạng máy tính. Quá trình truyền thông (đọc/ghi dữ liệu) giữa thẻ và đầu đọc đều sử dụng sóng vô tuyến với giải tần 100 kHz đến 10 GHz.

Nhìn chung, HCST đều sử dụng chip RFID loại thụ động, không cần nguồn nuôi, với đặc tả tuân theo chuẩn ISO 14443 và được tổ chức ICAO miêu tả chi tiết trong [7].

b) Cơ sở hạ tầng khoá công khai

PKI có thể được xem như cơ chế cho phép bên thứ ba (thường là nhà cung cấp chứng chỉ số) cung cấp và xác thực định danh của hai bên tham gia vào quá trình trao đổi thông tin. PKI khi triển khai phải đáp ứng được các quá trình dưới đây được an ninh/an toàn:

- Quá trình đầu đọc thẩm định dữ liệu được lưu trong HCST là xác thực hay không.
- Quá trình kiểm tra liệu dữ liệu trong HCST bị thay đổi hay nhân bản hay không.
- Quá trình kiểm tra liệu đầu đọc có được phép truy cập dữ liệu trong chip RFID hay không.

Như vậy, mỗi HCST cũng như các hệ thống cấp phát/thẩm định HCST cũng đều phải có chứng chỉ số. Việc trao đổi chứng chỉ của cơ quan cấp hộ chiếu giữa các quốc gia sẽ được thực hiện bằng đường công hàm và thông qua danh mục khoá công khai của ICAO [8].

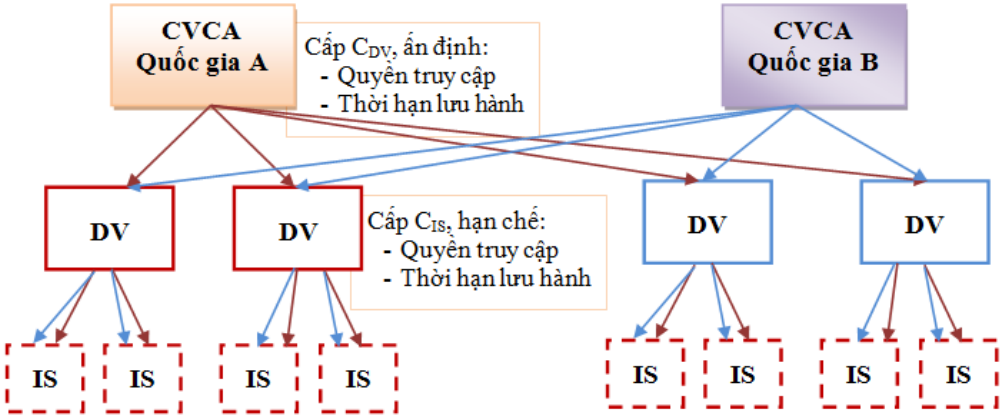
Các thành phần trong PKI cho HCST gồm:

♦ CSCA (Country Verifying Certificate Authorities) cùng với CVCA (Country Verifying Certificate Authority): là CA (Cerfiticate Authority) cấp quốc gia.

♦ DV (Document Verifier): Cơ quan kiểm tra hộ chiếu.

♦ IS (Inspection System): Hệ thống thẩm tra.

Hạ tầng khoá công khai có cấu trúc tầng. Tầng cao nhất tương ứng với mỗi quốc gia được gọi là CSCA. CSCA sinh và lưu giữ cặp khoá (KPu_{CSCA}, KPr_{CSCA}). Khoá bí mật của CSCA (KPr_{CSCA}) được dùng để ký mỗi chứng chỉ Document Verifier (C_{DV}) do quốc gia đó hay quốc gia khác quản lý. Trong mỗi quốc gia có nhiều DV. Mỗi DV sinh và lưu trữ một cặp khoá (KPu_{DV}, KPr_{DV}). Khoá bí mật của DV (KPr_{DV}) được dùng để ký mỗi chứng chỉ đầu đọc (C_{IS}) và SO_D trong mỗi HCST mà nó phát hành. Để chia sẻ các chứng chỉ DV (C_{DV}) giữa các quốc gia, ICAO cung cấp một danh mục khoá công khai PKD (Public Key Directory). PKD chỉ lưu trữ các chứng chỉ của DV (C_{DV}) đã được ký, chính vì vậy nó còn được gọi là kho chứa các chứng chỉ. Kho chứa này có sẵn ở mỗi quốc gia và được cấp quyền bảo vệ cấm đọc. Danh sách thu hồi chứng chỉ CRL (Certificate Revocation List) cũng có thể được lưu trữ trong cùng danh mục khoá công khai PKD. Mỗi quốc gia có trách nhiệm cập nhật thường xuyên các chứng chỉ và CRL bằng cách lấy chúng từ PKD. Mỗi lần làm như vậy, mỗi quốc gia phân phối thông tin mới lấy được đến cho mỗi DV và IS trong thẩm quyền của nó [9].



Hình 1. Mô hình PKI cho HCST.

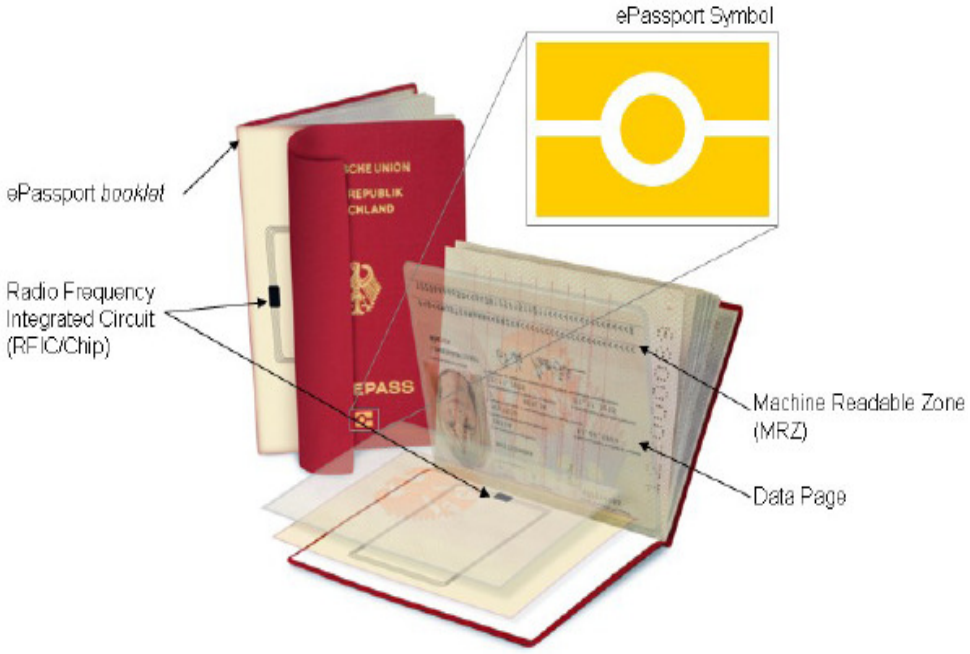
c) Xác thực sinh trắc học

Nói đến sinh trắc học là nói đến nhận dạng và kiểm tra sự giống nhau của con người dựa trên đặc điểm sinh lý nào đó. Các đặc điểm sinh trắc học thường sử dụng bao gồm: vân tay, khuôn mặt, mống mắt, giọng nói, chữ viết tay, hình bàn tay… Nền tảng của lĩnh vực xác thực sinh trắc học chính là tính duy nhất (hoặc có độ đồng nhất vô cùng thấp) của một số đặc trưng sinh trắc mà chúng ta có.

Trong HCST, ICAO đã đưa ra ba đặc trưng sinh trắc có thể sử dụng là ảnh khuôn mặt, ảnh vân tay và ảnh mống mắt của người mang hộ chiếu [6].

2.2. Cấu trúc và tổ chức HCST

Nhìn chung, HCST có cấu trúc giống hộ chiếu thông thường, ngoại trừ việc bổ xung thêm chip RFID để lưu dữ liệu bổ xung.



Hình 2. Cấu trúc hộ chiếu sinh trắc.

Dữ liệu được lưu trong chip RFID phải tuân theo chuẩn được ICAO khuyến nghị đưa ra [7]. Hiện nay, cấu trúc dữ liệu logic (Logical Data Structure - LDS) của chip này bao gồm 16 nhóm, được gán nhãn từ DG1 đến DG16. Trong tương lai, nếu dung lượng chip RFID được tăng lên, ba nhóm nữa có thể sử dụng (DG17-19) phục vụ lưu vết HCST và dữ liệu visa.

Các nhóm dữ liệu này sẽ được lưu trữ trên các vùng dữ liệu của chip RFID. Với các thành phần dữ liệu trong mỗi nhóm (trường thông tin), đầu đọc sẽ nhận diện sự tồn tại của chúng thông qua bản đồ hiển thị phần tử dữ liệu (Data Element Presence Maps), và vị trí lưu trữ dữ liệu thông qua các thẻ [10].

3. Các phiên bản HCST

Quá trình tiến triển của HCST, cho đến nay, có thể chia thành ba thế hệ tương ứng với mô hình ba phiên bản được liệt kê bên dưới.

3.1. HCST thế hệ thứ nhất

Trong thế hệ đầu tiên, vấn đề an ninh/an toàn trong quá trình cấp phát/kiểm tra HCST được ICAO đặc tả qua ba bước sau [7]: xác thực thụ động (Passive Authentication - PA), kiểm soát truy cập cơ sở (Basic Access Control - BAC), và xác thực chủ động (Active Authentication - AA) [6]:

- Xác thực bị động PA là cơ chế cho phép đầu đọc thẩm định liệu dữ liệu của HCST là xác thực hay không. Trong cơ chế này, thẻ không phải thực hiện một xử lý nào, từ đó PA chỉ cho phét phát hiện được dữ liệu là đúng, còn dữ liệu đó có phải do sao chép, nhân bản hay không thì sẽ không phát hiện ra.

- Xác thực chủ động AA là cơ chế tuỳ chọn trong thế hệ này, phục vụ việc phát hiện HCST nhân bản. Yêu cầu này được thực hiện với kỹ thuật *Thách đố - Trả lời* (Challenge - Response). Nếu HCST sử dụng AA, chip sẽ lưu trữ một khoá công khai KPu_{AA} trong DG15 và

giá trị băm của nó trong SO_D. Khoá bí mật tương ứng (KPr_{AA}) được lưu trữ trong vùng nhớ bí mật của chip. Vùng dữ liệu này không cho phép đọc bởi các đầu đọc, chỉ được chip RFID dùng để ký thách đố từ đầu đọc.

- Kiểm soát truy cập cơ sở BAC cũng là cơ chế tuỳ chọn, đảm bảo kênh truyền giữa đầu đọc và HCST được an toàn. Khi đầu đọc truy cập vào HCST, nó cung cấp khoá phiên sinh từ từ dữ liệu trên vùng MRZ.

3.2. HCST thế hệ thứ hai

Năm 2006 một tập các chuẩn cho HCST được đưa ra bởi Cộng đồng Châu Âu (EU), gọi là kiểm soát truy cập mở rộng (Extended Acess Control - EAC), và đã được công nhận bởi New Technologies Working Group (NTWG) [11,12]. Mục đích chính của EAC là đảm bảo xác thực cả chip RFID và đầu đọc, kết hợp sử dụng các đặc trưng sinh trắc mở rộng để nâng cao an ninh/an toàn. Hai cơ chế xác thực chip (Chip Authentication - CA) và xác thực đầu đọc (Terminal Authentication - TA) đã được bổ xung trong mô hình thế hệ này cùng với PA, BAC (thay thế AA ở thế hệ thứ nhất).

i. Xác thực chip CA là cơ chế bắt buộc, được dùng để thay thế AA. Nếu CA thực hiện thành công, nó sẽ thiết lập một cặp khoá mã hoá mới và khoá MAC để thay thế khoá phiên sinh trong BAC. Quá trình này sử dụng giao thức thoả thuận khoá Diffie-Hellman tĩnh. Khoá công khai $TKPu_{CA}$ dùng cho CA được lưu trong DG14 còn khoá bí mật $TKPr_{CA}$ trong vùng nhớ bí mật của chip.

ii. Xác thực đầu cuối TA là cơ chế được thực hiện khi muốn truy cập vào vùng dữ liệu sinh trắc (nhạy cảm) của chip RFID. Đầu đọc sẽ chứng minh quyền truy xuất đến chip RFID bằng cách sử dụng các chứng chỉ số. [13]

3.3. HCST thế hệ thứ ba

Năm 2008, tổ chức Federal Office for Information Security (BSI-Germany) đưa ra một tài liệu miêu tả các cơ chế bảo mật mới cho HCST [12]. Các tài liệu này được xem như cơ sở để phát triển HCST thế hệ thứ ba.

Ngoài CA và TA có sự thay đổi so với mô hình trước, thế hệ này còn có thêm cơ chế PACE (Password Authenticated Connection Establishment). Chúng tôi sẽ giới thiệu chi tiết mô hình thế hệ này ở đây:

i. PACE được dùng để thay thế BAC, cho phép chip RFID thẩm định đầu đọc có quyền truy cập vào HCST hay không. Thẻ và đầu đọc sử dụng một mật khẩu chung (π) kết hợp với giao thức thoả thuận khoá Diffie-Hellman để đưa ra một khoá phiên mạnh.

Toàn bộ quá trình được miêu tả:

1. Chip RFID mã hoá một số ngẫu nhiên *nonce*[1] (s) sử dụng khoá K_π. Với K_π = SHA-1(π||3)
2. Chip RFID gửi *nonce*(*s*) đã mã hoá và các tham số tĩnh trên miền D trong giao thức thoả thuận khoá Diffie-Hellman (DH) đến cho IS.
3. IS sử dụng (π) để khôi phục lại chuỗi đã mã hoá *(s)*.
4. RFID và IS tính các tham số miền DH *(D')* dựa trên D và s.
5. RFID sinh ra một cặp khoá ($PACEKPr_T$, $PACEKPu_T$) và gửi cho IS khoá $PACEKPu_T$.
6. IS sinh ra cặp khoá ($PACEKPr_R$, $PACEKPu_R$) và gửi đến RFID khoá $PACEKPu_R$.
7. RFID và IS đã có đủ thông tin chia sẻ để sinh ra khoá K_{seed}.
8. RFID và IS tính toán các khoá phiên K_{ENC} và K_{MAC}.
9. IS tính: T_R = ***MAC***(K_M, ($PACEPu_T$, D')) và gửi nó đến cho RFID thẩm định
10. RFID tính: T_T = ***MAC***(K_M, ($PACEPu_R$, D')) và gửi nó đến cho IS thẩm định

[1] nonce = number used once

Từ đó, PACE cho phép tạo khoá phiên độc lập so với độ dài mật khẩu và mật khẩu này có thể sử dụng số lượng ký tự vừa phải (chẳng hạn 6 ký tự).

ii. Xác thực đầu đọc TA, trong các đặc tả mới của thế hệ này, phải được thực hiện trước CA để cho phép RFID thẩm định liệu IS có quyền truy cập đến các thông tin sinh trắc nhạy cảm hay không. Việc xác thực này được tiến hành với việc sử dụng chứng chỉ số như sau:

1. IS gửi cho RFID một chuỗi chứng chỉ gồm chứng chỉ DV (C_{DV}), và chứng chỉ IS (C_{IS}).
2. RFID xác thực các chứng chỉ này sử dụng khoá công khai CVCA.
3. RFID lấy khoá công khai của đầu đọc (*RPuK*).
4. IS sinh ra cặp khoá DH ngắn hạn trên miền D: ($RPrK_{TA}$, $RPuK_{TA}$).
5. IS nén khoá công khai $Comp(RPuK_{TA})$ và gửi khoá này cùng dữ liệu bổ trợ thêm A_{TA} đến cho RFID.
6. RFID gửi thách đố ngẫu nhiên R đến IS.
7. IS sử dụng khoá bí mật *RPrK* kí chuỗi $(ID_{TA}||R||Comp(RPuK_{TA})||A_{TA})$ (với ID_{TA} là định danh của chip RFID) và gửi nó đến RFID.
8. RFID thẩm định tính đúng đắn của chữ ký và chuỗi sử dụng khoá công khai *RPuK* và các tham số đã biết khác.

iii. Xác thực chip CA chỉ được thực hiện sau khi TA do CA cần cặp khoá DH ngắn hạn ($RPrK_{TA}$, $RPuK_{TA}$) được sinh ra trong quá trình TA. Các bước thực hiện trong CA như sau:

1. RFID gửi cho IS khoá công khai của nó (*TPuK*).
2. IS gửi khoá công khai ngắn hạn $RPuK_{TA}$ đã được sinh ra trong quá trình TA đến cho RFID.
3. RFID tính $Comp(RPuK_{TA})$ và dữ liệu A_{TA}. Nó sẽ so sánh giá trị *Comp* này với giá trị nó nhận được từ quá trình TA.
4. RFID và IS có đủ thông tin chia sẻ để tính khoá K_{seed}.
5. RFID sinh ra chuỗi ngẫu nhiên (R). Các khoá phiên được tính: $K_{MAC} = SHA\text{-}1(K_{seed}||R||2)$ và $K_{ENC} = SHA\text{-}1(K_{seed}||R||1)$.
6. RFID tính: $T_T = \boldsymbol{MAC}\ (K_{MAC}, (RPuK_{TA}, D))$.
7. RFID gửi R và T_T đến cho IS.
8. IS sử dụng R để tính các khoá phiên từ K_{seed}. Sau đó nó thẩm định thẻ bài xác thực T_T.

3.4. Đánh giá, so sánh các mô hình

Để đánh giá, so sánh các thế hệ trên, chúng ta hãy xem xét các nguy cơ xảy ra với HCST.

♦ Đối với thế hệ đầu tiên:

- *BAC và AA là hai cơ chế tuỳ chọn*: Nếu hai cơ chế này không được sử dụng thì dữ liệu bị đọc trộm, chip bị làm nhái là rất dễ xảy ra.

- *Khoá truy cập BAC còn yếu*: BAC chỉ là một giao thức nhằm bảo vệ HCST khỏi bị đọc trộm và nghe trộm. Nhưng tính bảo mật của toàn bộ giao thức lại dựa trên chiều dài (entropy) của hai khoá truy cập được tính từ các thông tin trên MRZ. Chiều dài các khoá truy cập tối đa là 56 bits, như vậy sẽ rất dễ đoán. Một khi kẻ thù lấy được những khoá này, chúng có thể dễ dàng đọc và lần theo vết của chip RFID trong suốt thời gian sống của HCST.

- *Chưa có các quy tắc truy cập*: Các đặc tả mà ICAO đưa ra chưa bao gồm các nguyên tắc cho việc truy cập vào vùng dữ liệu sinh trắc nhạy cảm (vân tay, mống mắt, ..). Điều đó dẫn đến nguy cơ tấn công truy cập và lấy các thông tin rất riêng tư của người mang hộ chiếu

♦ Đối với thế hệ thứ hai:

- *Còn phụ thuộc vào BAC*: EAC vẫn sử dụng BAC để bảo vệ dữ liệu sinh trắc. Như đã nói trên, các thông tin sinh trắc vẫn có thể dễ dàng bị tấn công.

- *Nguy cơ tấn công ngẫu nhiên bởi các đầu đọc*: chip RFID của HCST là loại chip thụ

động, do đó không có đồng hồ. Chúng thiết lập thời gian hiện tại chỉ dựa trên thông tin nhận được từ đầu đọc cuối cùng kích hoạt chúng. Như thế thì đầu đọc với chứng chỉ đã hết hạn vẫn có thể đọc được nội dung của chip RFID (gồm các thông tin sinh trắc nhạy cảm) nếu thời gian trên HCST chưa được cập nhật trong thời gian dài.

- *Nguy cơ tấn công DoS*: khi TA chỉ được thực hiện sau CA, rất có khả năng một đầu đọc với động cơ nào đó sẽ làm tràn RFID bởi các chứng chỉ không hợp lệ. Khi đó bộ nhớ của RFID bị hạn chế, nó sẽ dừng thực hiện các chức năng đã được yêu cầu.

♦ Đối với mô hình HCST thế hệ thứ ba:

Thế hệ HCST thứ ba ra đời khắc phục được hầu hết các nguy cơ an ninh có thể xảy ra trong các thế hệ HCST trước đó. Tuy nhiên vẫn còn một vấn đề nữa xuất hiện trong mô hình này, đó là nguy cơ tấn công ngẫu nhiên bởi các đầu đọc.

4. Mô hình xác thực HCST thử nghiệm ứng dụng cơ chế PACE và EAC

Dựa trên mô hình HCST thế hệ thứ ba, chúng tôi đã tiến hành xây dựng mô hình xác thực HCST tích hợp cả hai cơ chế PACE và EAC. Mô hình này bao gồm các bước chính sau:

B1: Người mang hộ chiếu xuất trình hộ chiếu cho cơ quan kiểm tra, cơ quan tiến hành thu nhận các đặc tính sinh trắc học từ người xuất trình hộ chiếu.

B2: Kiểm tra các đặc tính bảo mật trên trang hộ chiếu giấy thông qua các đặc điểm an ninh truyền thống đã biết: thuỷ ấn, dải quang học, lớp bảo vệ ảnh…

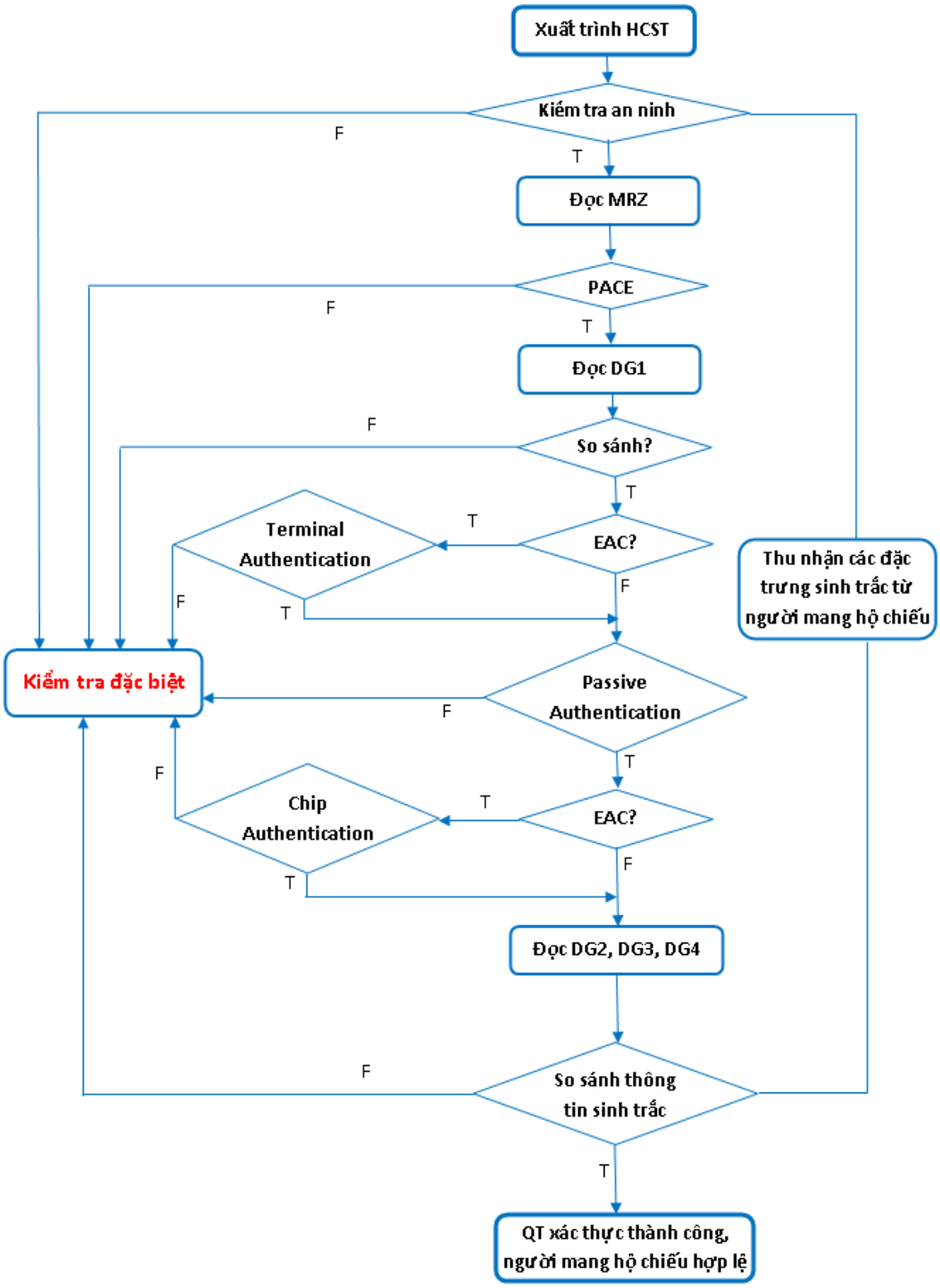
B3: IS và RFID thực hiện quá trình PACE. Sau khi PACE thành công, IS có thể đọc các thông tin trong chip ngoại trừ DG3, DG4 (ảnh vân tay và mống mắt), mọi thông tin trao đổi giữa đầu đọc và chip được truyền thông báo bảo mật, mã hoá sau đó là xác thực theo cặp khoá (K_{ENC}, K_{MAC}) có được từ quá trình PACE.

B4: Tiến hành quá trình TA để chứng mình quyền truy cập của đầu đọc đến phần dữ liệu DG3, DG4.

B5: Thực hiện PA để kiểm tra tính xác thực và toàn vẹn của các thông tin lưu trong chip thông qua kiểm tra chữ ký trong SO_D bằng khoá công khai của cơ quan cấp hộ chiếu. Việc trao đổi khoá thông qua chứng chỉ số theo mô hình khuyến cáo của ICAO.

B6: Tiến hành CA để chứng minh được tính nguyên gốc của chip đồng thời cung cấp khoá phiên mạnh cho truyền thông báo bảo mật.

B7: IS đối sánh dữ liệu sinh trắc thu nhận được trực tiếp từ người xuất trình hộ chiếu với dữ liệu sinh trắc lưu trong chip. Nếu quá trình đối sánh thành công và kết hợp với các chứng thực trên, cơ quan kiểm tra hộ chiếu có đủ điều kiện để tin tưởng hộ chiếu là xác thực và người mang hộ chiếu đúng là con người mô tả trong hộ chiếu. Nếu cơ quan kiểm tra hộ chiếu không triển khai EAC thì IS đó không có quyền truy cập DG3 và DG4. Thông tin sinh trắc học duy nhất dùng để đối sánh chỉ là ảnh khuôn mặt.



Hình 3. Mô hình xác thực Hộ chiếu sinh trắc.

4.1. Kiểm tra an ninh

Công dân mang HCST xuất trình hộ chiếu cho hệ thống kiểm duyệt (IS). Trước tiên HCST cần phải trải qua một số bước kiểm tra an ninh nghiệp vụ truyền thống tại các điểm xuất/nhập cảnh như dùng lớp kim loại bảo vệ để tạo hiệu ứng lồng Faraday nhằm chống khả năng đọc thông tin trong chip RFID ngoài ý muốn của người mang hộ chiếu hay dùng thủy ấn để bảo vệ booklet…

4.2. PACE

PACE thiết lập các thông báo bảo mật giữa chip RFID và IS, sử dụng mật khẩu đơn giản, theo các bước như lược đồ sau:

1. Chip RFID sinh ra ngẫu nhiên s, mã hoá s sử dụng K_π : $z = \mathbf{E}(K_\pi, s)$ với $K_\pi = SHA\text{-}1(\pi||3)$ và gửi bản mã z cùng các tham số miền tĩnh D đến cho IS.
2. IS khôi phục lại bản rõ s = $\mathbf{D}(K_\pi, z)$ sử dụng mật khẩu chung π.
3. Cả RFID và IS cùng thực hiện các bước sau:

- Tính các tham số miền tĩnh *D'* dựa trên *D* và *s*: $D' = \mathbf{Map}(D,s)$

- Thực hiện giao thức thoả thuận khoá Diffie-Hellman dựa trên *D'* và khoá chia sẻ.

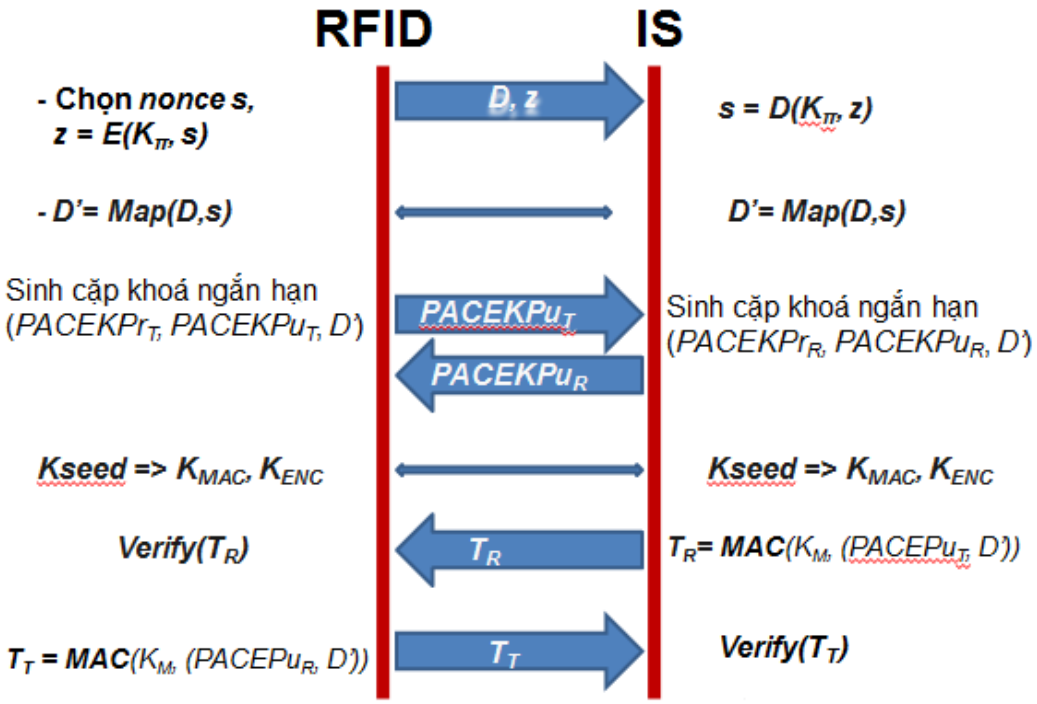
$K=\mathbf{KA}(PACEKPr_T, PACEKPu_R, D')= \mathbf{KA}(PACEKPr_R, PACEKPu_T, D')$

Trong suốt quá trình thoả thuận khoá DH, mỗi bên phải kiểm tra rằng hai khoá công khai $PACEKPu_R$ và $PACEKPu_T$ là khác nhau.

Từ đó cả hai bên tính cá khoá phiên K_{MAC} và K_{ENC}.

RFID tính thẻ xác thực $T_T = \mathbf{MAC}(K_M, (PACEPu_R, D'))$ và gửi đến cho IS thẩm định.

IS tính thẻ xác thực $T_R = \mathbf{MAC}(K_M, (PACEPu_T, D'))$ và gửi đến cho RFID thẩm định.



Hình 4. Lược đồ PACE.

4.3. Đọc vùng dữ liệu DG1

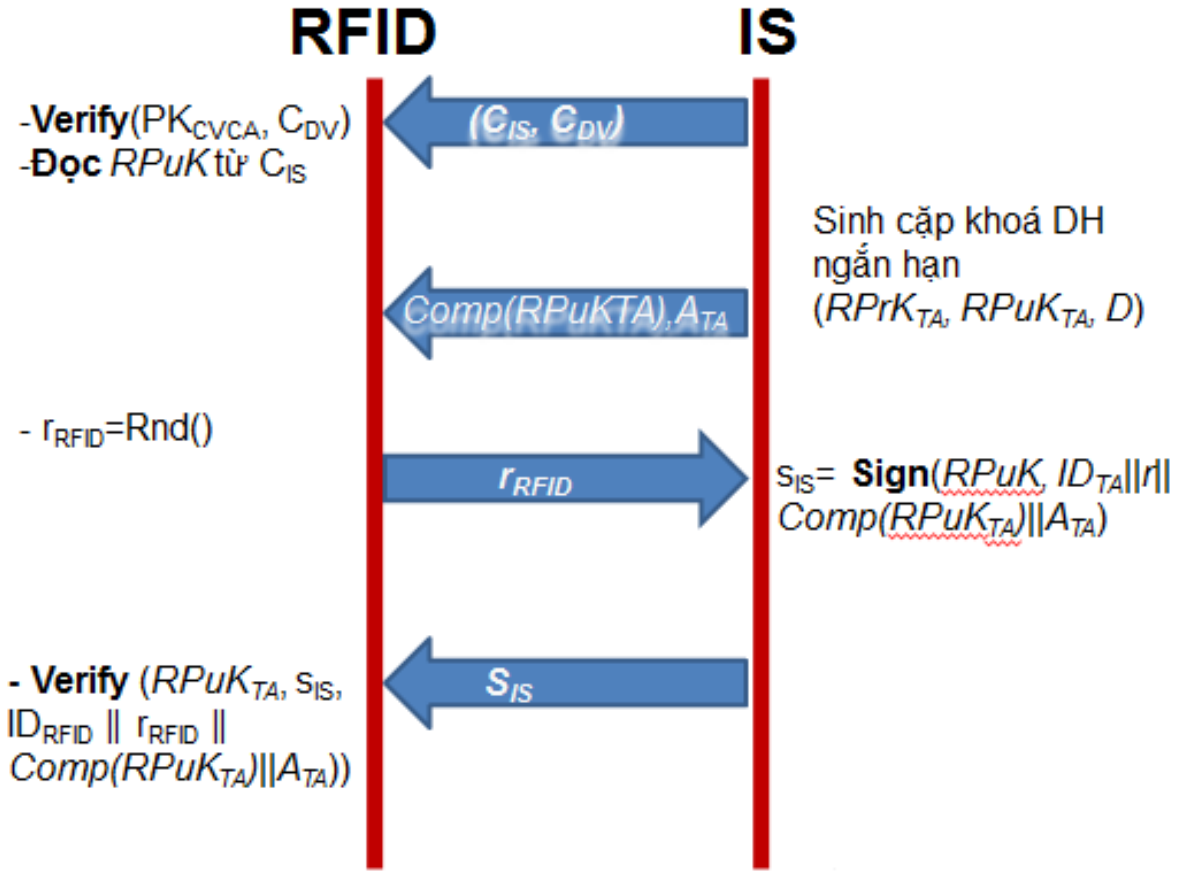
Sau khi PACE thành công, hệ thống xác thực HCST sẽ tiến hành đọc vùng dữ liệu DG1 trong chip RFID của HCST và so sánh với những dữ liệu hệ thống đã đọc được từ vùng MRZ. Nếu dữ liệu trùng nhau thì chuyển sang bước 4, nếu không thì chuyển qua bước kiểm tra đặc biệt.

4.4. Xác thực đầu đọc

TA cho phép chip RFID thẩm định liệu đầu đọc có được quyền truy cập vào vùng dữ liệu nhạy cảm hay không (ảnh vân tay, ảnh mống mắt, …). Các bước trong TA như sau [12].

1. IS gửi chuỗi chứng chỉ đến chip gồm C_{IS} và C_{DV}.
2. RFID kiểm chứng các chứng chỉ này sử dụng PK_{CVCA} và trích khoá công khai của đầu đọc $RPuK$.
3. IS sinh ra cặp khoá DH ngắn hạn trên miền D: $RPrK_{TA}$, $RPuK_{TA}$. Sau nó gửi $Comp(RPuK_{TA})$ và dữ liệu A_{TA} đến cho RFID
4. RFID gửi thách đố ngẫu nhiên r_{RFID} đến IS.
5. IS trả lời bằng chữ ký s_{IS}=**Sign**($RPuK$,ID_{TA}||r||$Comp(RPuK_{TA})$||A_{TA})
6. Chip kiểm tra chữ ký nhận được từ IS bằng khoá $RPuK_{TA}$

   Verify($RPuK_{TA}$, s_{IS}, ID_{RFID} || r_{RFID} || $Comp(RPuK_{TA})$||A_{TA}))



Hình 5. Lược đồ TA.

4.5. Xác thực thụ động

Quá trình PA cho phép kiểm tra tính xác thực và toàn vẹn thông tin lưu trong chip RFID thông qua việc kiểm tra chữ ký lưu trong SO_D bằng khóa công khai của cơ quan cấp hộ chiếu. Việc trao đổi khóa công khai thông qua chứng chỉ số được thực hiện theo mô hình khuyến cáo của ICAO. Thực hiện thành công quá trình *PA* cùng với *CA* trong cơ chế EAC thì có thể khẳng định chắc chắn chip trong hộ chiếu là nguyên gốc [12].

1) Đọc SO_D từ chip RFID.

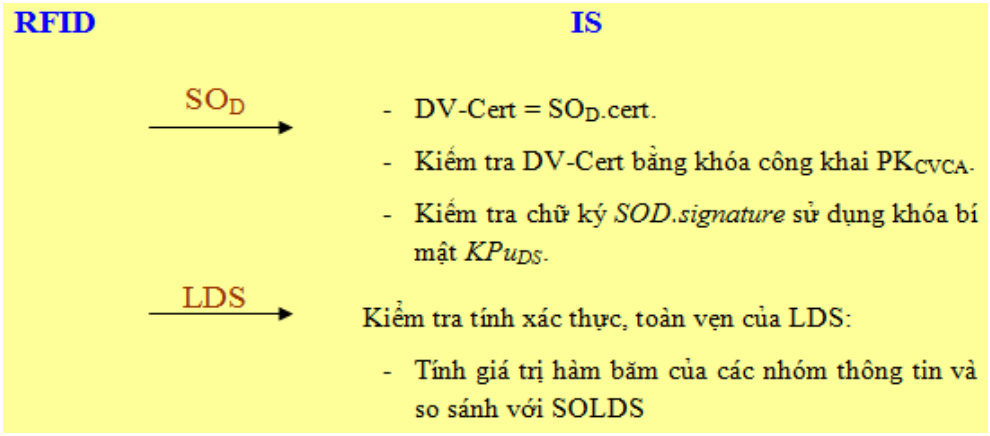
2) Lấy chứng chỉ *DV-Cert* từ SO_D vừa đọc ở trên.

3) Kiểm tra *DV-Cert* từ khóa công khai PK_{CVCA} có được từ PKD hoặc từ cơ sở dữ liệu được trao đổi trực tiếp giữa các quốc gia thông qua đường công hàm.

4) Kiểm tra chữ ký số $SO_D.signature$ sử dụng khóa bí mật KPu_{DS} của DV. Bước này nhằm khẳng định thông tin SO_{LDS} đúng là được tạo ra bởi cơ quan cấp hộ chiếu và SO_{LDS} không bị thay đổi.

5) Đọc các thông tin cần thiết từ LDS.

6) Tính hàm băm cho các thông tin ở bước 4, sau đó so sánh với SO_{LDS}. Qua bước này mới khẳng định được nhóm dữ liệu là xác thực và toàn vẹn.



Hình 6. Lược đồ PA.

4.6. Xác thực chip

CA thiết lập thông báo bảo mật giữa chip MRTD và IS dựa trên cặp khoá tĩnh được lưu trữ trên chip. CA thay thế cơ chế AA mà ICAO đã đưa ra và cung cấp các khoá phiên mạnh [12]. Các bước tiến hành trong CA như sau:

1) RFID gửi cho IS khoá công khai (*TPuK*).

2) IS gửi khoá công khai ngắn hạn $RPuK_{TA}$ đã được sinh ra trong TA đến cho RFID.

3) RFID tính $Comp(RPuK_{TA})$ và dữ liệu A_{TA}. Nó sẽ so sánh giá trị *Comp* này với giá trị nó nhận được từ TA.

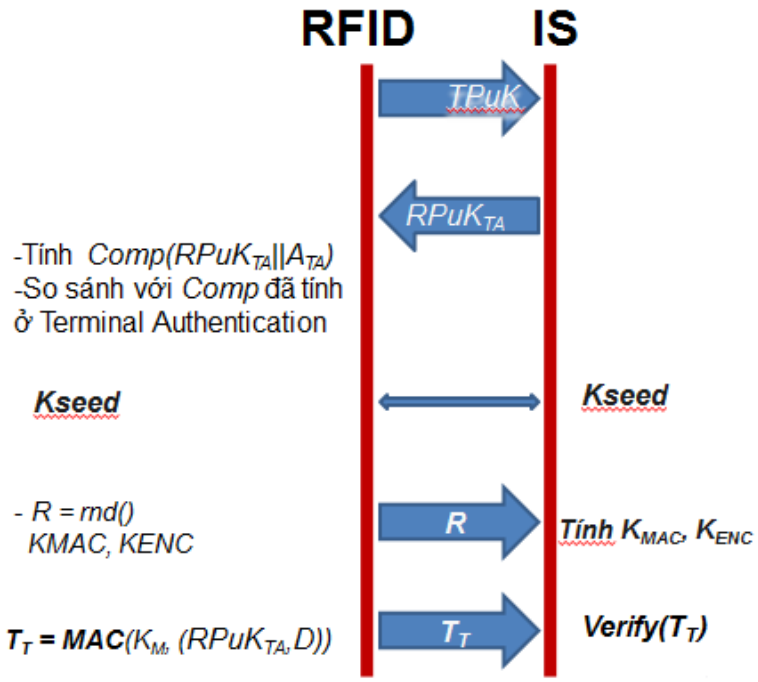
4) RFID và IS có đủ thông tin chia sẻ để tính khoá K_{seed}.

5) RFID sinh ra chuỗi ngẫu nhiên (R). Các khoá phiên được tính: $K_{MAC} = SHA\text{-}1(K_{seed}||R||2)$ và $K_{ENC} = SHA\text{-}1(K_{seed}||R||1)$.

6) RFID tính: T_T = **MAC** (K_{MAC}, ($RPuK_{TA}$,D)).

RFID gửi *R* và T_T đến cho IS.

7) IS sử dụng R để tính các khoá phiên từ K_{seed}. Sau đó nó thẩm định thẻ bài xác thực T_T.



Hình 7. Lược đồ CA.

4.7. Đối sánh đặc trưng sinh trắc

Hệ thống kiểm duyệt có quyền truy cập vào các vùng dữ liệu DG2, DG3, DG4 và tiến hành đọc các dữ liệu sinh trắc của người sở hữu hộ chiếu (ảnh khuôn mặt, dấu vân tay, mống mắt) được lưu trong chip RFID. Cùng lúc đó, bằng các thiết bị chuyên dụng, cơ quan kiểm tra sẽ tiến hành thu nhận các đặc tính sinh trắc học như ảnh khuôn mặt, vân tay, mống mắt… từ công dân. Sau đó, hệ thống sẽ thực hiện quá trình trích chọn đặc trưng của các đặc tính sinh trắc, tiến hành đối chiếu và đưa ra kết quả. Nếu cả ba dữ liệu sinh trắc thu được trực tiếp từ người dùng khớp với dữ liệu thu được từ chip RFID thì cơ quan kiểm tra xác thực có đủ điều kiện để tin tưởng hộ chiếu điện tử đó là đúng đắn và người mang hộ chiếu là hợp lệ [6,14].

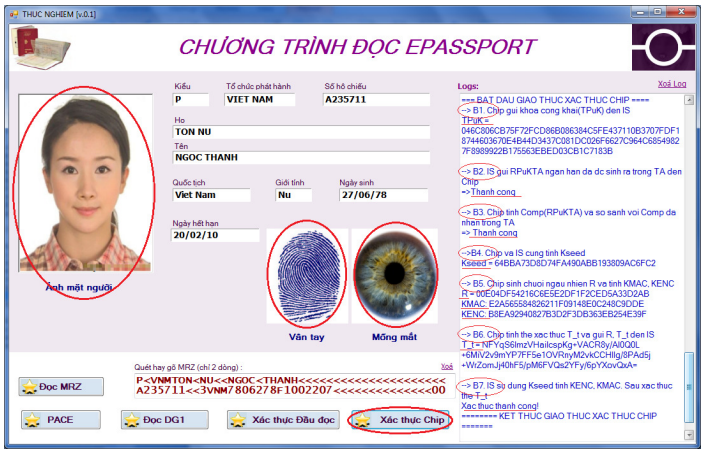
5. Thực nghiệm

Do điều kiện có hạn về cơ sở vật chất, chúng tôi đã tiến hành thử nghiệm mô hình trên theo hướng kiểm thử quy trình xác thực với dữ liệu mô phỏng. Các phần liên quan đến những bước cần xử lý trên chip RFID sẽ được thử nghiệm trong thời gian tới.

Chương trình thử nghiệm chúng tôi phát triển sẽ tập chung vào các chức năng sau:

- Phân tích vùng MRZ trên HCST.
- Đọc vùng DG1 lưu trên chip và so khớp với vùng MRZ vừa đọc trên.
- Mô phỏng quá trình xác thực với cơ chế PACE và EAC (bao gồm cả xác thực đầu đọc và xác thực chip).

Dựa trên số thư viện mã hoá như Org.BouncyCastle, CryptoSys PKI [15], chúng tôi đã tiến hành xây dựng chương trình cung cấp các chức năng nêu trên, phục vụ quá trình kiểm thử mô hình xác thực.



Hình 8. Chương trình thử nghiệm PACE và EAC.

Chương trình thử nghiệm thu được đã có khả năng tiến hành các bước đã nêu trong mô hình xác thực nêu trên. Cụ thể:

- Phân tích và hiển thị thông tin trong vùng MRZ

- Tiến hành PACE, lưu vết kết quả. Nếu thành công, tiến hành tiếp bước sau.

- Đọc DG1 và so khớp với thông tin MRZ như trong mô hình đã nêu.

- Tiến hành xác thực đầu đọc và lưu/hiển thị toàn bộ vết các bước đã thực tiện trong quá trình này.

- Thực hiện xác thực chip với 7 bước và lưu/hiển thị các vết thực hiện. Ở đây, quá trình PA tạm thời chưa tích hợp vào hệ thống vì lý do thiếu hạ tầng khoá công khai PKI.

6. Đánh giá mô hình

Quá trình CA sử dụng lược đồ trao đổi khoá phiên ngắn hạn theo Diffie-Hellman và theo giải thuật tựa Elgamal, phần tính toán trên chip cũng không nhiều. Theo mô hình, chip chỉ cần lưu trữ cặp khoá xác thực Deffie-Hellman tĩnh nên không cần thiết phải trao đổi khoá trước đó giữa IS và RFID. Đây cũng là yếu tố góp phần đảm bảo hiệu năng chung của mô hình.

Trong quá trình CA cần thiết có trao đổi chứng chỉ tuy nhiên, các công việc xử lý liên quan đến phân phối chứng chỉ do CVCA, DV và các IS thực hiện nên khối lượng tính toán xử lý của chip được hạn chế đến mức tối đa và có thể triển khai thực hiện được trong thực tế.

Ngoài ra, với việc sử dụng hệ mật dựa trên đường cong Elliptic (ECC) - hệ mật được đánh giá có độ an toàn cao trong khi kích thước khoá nhỏ, thời gian tính toán nhanh và rất phù hợp để triển khai trên các thiết bị tính toán có năng lực xử lý yếu [16]. Đây là điều kiện tiên quyết đảm bảo hiệu năng của mô hình xác thực.

Ngoài ra, mô hình nêu trên hoàn toàn đáp ứng được những yêu cầu đặt ra đối với HCST như: đảm bảo tính chân thực (quy trình rõ rang); tính không thể nhân bản (sử dụng CA và PA); tính nguyên vẹn và xác thực (PA và PKI), tính liên kết công dân-HCST (sử dụng ba đặc trưng sinh trắc có độ xác thực cao nhất); kiểm soát được truy cập (PACE và EAC)

Mặc dù mô hình xác thực HCST này, được xây dựng dựa trên những đặc tả trong phiên bản thế hệ thứ ba, khắc phục hầu hết các nguy cơ kém an toàn của HCST thế hệ thứ nhất và thứ hai, tuy nhiên nó vẫn tồn tại nhược điểm liên quan đến vấn đề hết hạn của đầu đọc.

7. Kết luận

Việc sử dụng HCST đã minh chứng được những tính ưu việt trong việc nâng cao quá trình cấp phát và kiểm soát hộ chiếu. Với những nghiên cứu và phân tích những thế hệ đã có của HCST, chúng ta có thể nắm bắt tốt hơn ưu/nhược của từng thế hệ, từ đó có được những giải pháp phù hợp với từng loại hộ chiếu. Mặc dù HCST thế hệ thứ nhất vẫn còn được một số nước sử dụng, nhưng những ưu điểm nổi trội về an ninh/an toàn của thế hệ thứ ba cho phép khẳng định được tiềm năng ứng dụng thực tế của mô hình này. Tuy nhiên, vấn đề về hết hạn của đầu đọc trong thế hệ thứ ba này vẫn còn tồn tại.

Với việc thử nghiệm một số chức năng trong mô hình đề xuất, chúng tôi hy vọng những kết quả này sẽ là tiền đề cho những nghiên cứu/đầu tư chuyên sâu hơn, từ đó có thể xây dựng và sản xuất được HCST cho công dân Việt Nam mà không cần phải sử dụng lại những sản phẩm nước ngoài.

Trong thời gian tới, chúng tôi sẽ tích hợp với những modules xác thực các nhân tố sinh trắc và thiết bị thực. Ngoài ra, những vấn đế như cấp/quản lý chứng chỉ số; quản lý cơ sở dữ liệu công dân có kèm theo những đặc trưng sinh trắc, cũng sẽ được chú trọng trong những hướng phát triển tiếp theo của bài báo này.

Lời cảm ơn

Công trình này được tài trợ một phần từ đề tài nghiên cứu mã số QG.09.28, cấp Đại học Quốc gia Hà Nội.

References

[1] Gildas Avoine, Kassem Kalach, and Jean-Jacques Quisquater. *ePassport: Securing international contacts with contactless chips*. In Financial Cryptography 2008, LNCS.Springer-Verlag, 2008.

[2] Moses, T.: *The Evolution of E-Passports: Extended Access Control - Protecting Biometric Data with Extended Access Control*. Entrust. (August 2008)

[3] Wikipedia, "*Biometric Passport*", http://en.wikipedia.org/wiki/Biometric_passport, truy cập ngày 16/12/2010

[4] "*Năm 2011 bắt đầu phát hành hộ chiếu điện tử*", truy cập 24/11/2010, tham khảo tại http://vneconomy.vn/20101124070255463P0C16/nam-2011-bat-dau-phat-hanh-ho-chieu-dien-tu.htm

[5] BSI, *Advanced Security Mechanism for Machine Readable Travel Documents Extended Access Control (EAC)*. Technical Report (BSI-TR-03110) Version 2.02 Release Candidate, Bundesamt fuer Sicherheit in der Informationstechnik (BSI), 2008.

[6] P.T. Long, N.N. Hoa, "*Mô hình xác thực hộ chiếu điện tử*", tại Hội thảo Quốc gia "Một số vấn đề chọn lọc trong CNTT, 06/2008, Huế, Việt Nam.

[7] ICAO, *Machine Readable Travel Documents: Document 9303*, Part 1, Volumes 1 and 2, 6th edition, 2006.

[8] ICAO, *Machine Readable Travel Documents*: *PKI for Machine Readable Travel Documents offering ICC Read-Only Access*. Version 1.1. 2004. http://www.icao.int/mrtd/download/technical.cfm

[9] R. Nithyanand. *A survey on the evolution of cryptographic protocols in epassports*. Cryptology ePrint Archive, Report 2009/200, 2009.

[10] ICAO, *Machine Readable Travel Documents*: *Development of a Logical Data Structure – LDS for Optional Capacity Expansion Technology*, Technical report of International Civil Aviation Organization, Revision 1.7, United States, 2004.

[11] Federal Office for Information Security, *Advanced Security Mechanisms for Machine Readable Travel Documents, Extended Access Control (EAC)*, version 1.01, Technical Guideline TR-03110, BSI, Bonn, Germany, 2006.

[12] Federal Office for Information Security, *Advanced Security Mechanisms for Machine Readable Travel Documents, Extended Access Control (EAC)*, version 2.01, Technical Guideline TR-03110, BSI, Bonn, Germany, 2009.

[13] Dagdelen and Marc Fischlin. *Security analysis of the extended access control protocol for machine readable travel documents*. In Proceedings of the 13th international conference on Information security (ISC'10), Mike Burmester, Gene Tsudik, Spyros Magliveras, and Ivana Ili (Eds.). Springer-Verlag, Berlin, Heidelberg, 54-68, 2010.

[14] D.P Hanh et al, Hộ chiếu điện tử và mô hình đề xuất tại Việt Nam, *Tạp chí Khoa học ĐHQGHN, Khoa học Tự nhiên và Công nghệ* 24 (2008) 28.

[15] Một số thư viện được sử dụng trong ứng dụng thử nghiệm: BouncyCastle - http://www.bouncycastle.org/csharp/ và CryptoSys PKI - http://www.cryptosys.net/pki/pkidotnet.html

[16] D.T. Hien, et al., "Mutual Authentication for RFID tag-reader by using the elliptic curve cryptography", *VNU Journal of Science, Natural Sciences and Technology* 24 (2008) 36.

Using PACE and EAC for biometric passport authentication

Vu Thi Ha Minh, Nguyen Ngoc Hoa

University of Engineering and Technology, VNU, 144 Xuan Thuy, Hanoi, Vietnam

This paper investigates three different generations of biometric passport in order to make advantages of its security/safety. Beginning with the ICAO standards for first biometric passports (2004, used mainly the Basic Access Control - BAC), some European countries additionally used the mechanism EAC (Extended Access Control, 2006) to provide more comprehensive Tag and Reader authentication protocol. Currently, based on the EAC, the PACE (Password Authenticated Connenction Establishment, 2009) mechanism is introduced as a replacement to the Basic Access Control. By using the third generation approach, we propose a model of biometric passport authentication based on PACE and EAC. An experiment is also presented in this paper for validating this model.

Keywords: biometric passport, Extended Access Control, Password Authenticated Connenction Establishment, RFID, PKI.