Tạp chí Khoa học Đại học Quốc gia Hà Nội, Khoa học Tự nhiên và Công nghệ 24 (2008) 28-35

Hộ chiếu điện tử và mô hình đề xuất tại Việt Nam

Dư Phương Hạnh*, Trương Thị Thu Hiền, Nguyễn Ngọc Hoá

Khoa Công nghệ Thông tin, Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội
144 Xuân Thủy, Hà Nội, Việt Nam

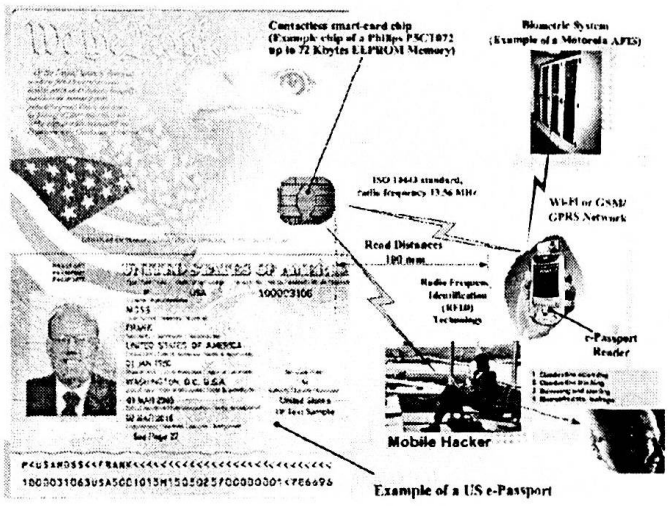
Nhận ngày 25 tháng 12 năm 2007

Tóm tắt. Hộ chiếu điện tử đã và đang được sử dụng phổ biến tại nhiều nước trên thế giới. Bài báo này đề cập đến thực trạng hiện nay của việc ứng dụng kết quả của ngành xác thực dựa trên các đặc trưng sinh trắc trong vấn đề kiểm soát người mang hộ chiếu thông qua hộ chiếu điện tử. Mô hình đề xuất của hộ chiếu điện tử ở Việt Nam sẽ dựa trên ba đặc trứng sinh trắc : ảnh mặt người, ảnh mống mắt và ảnh vân tay. Với việc sử dụng mô hình xác thực hai chiều dựa trên hệ mật đường cong Elliptic, mô hình đề xuất đảm bảo chống được những nguy cơ đe dọa đối với hộ chiếu điện tử.

Từ khoá: RFID, xác thực hai chiều, xác thực sinh trắc học, mô hình hộ chiếu điện tử.

1. Giới thiệu

Hộ chiếu điện tử (e-passport), hay còn gọi là hộ chiếu sinh trắc học (biometric passport) [1,2] là một giấy căn cước cung cấp thông tin theo thời kỳ (khoảng 10 năm theo một số nước phát triển hộ chiếu quy định) về một người, sử dụng các nhân tố sinh trắc học để xác thực quyền công dân của người đi lại giữa các quốc gia. Thông tin chủ chốt của hộ chiếu lưu trữ trong một thẻ thông minh đặc biệt không cần tiếp xúc (được gọi là Contactless SmartCard - CSC), và dữ liệu được truyền tải giữa máy đọc và hộ chiếu thông qua công nghệ RFID (Radio Frequency Identification) [3,4]. Thẻ thông minh không cần tiếp xúc này được nhúng vào bên trong thân hộ chiếu, và toàn bộ dữ liệu sinh trắc học bên trong nó sẽ được mã hoá, được đảm bảo tính nguyên vẹn thông qua những chuẩn đặc biệt liên quan.



Hình 1. Một ví dụ về hộ chiếu điện tử [5].

* Tác giả liên hệ. ĐT: 84-4-7547813.
E-mail: hanhdp@vnu.edu.vn

Các yếu tố sinh trắc học thường được sử dụng hiện nay trong các hệ thống xác thực sinh trắc học là vân tay, khuôn mặt, màng mống mắt, võng mạc mắt...[6]. Để lưu trữ dữ liệu sinh trắc trên thẻ nhớ CSC, nó được trang bị một bộ nhớ dung lượng nhỏ theo kiểu EEPROM (bộ nhớ lưu trữ chỉ đọc có thể lập trình lại), và ứng dụng công nghệ RFID với chuẩn ISO-14443 để thực hiện việc truyền dữ liệu.

Để có thể xác định rõ những ưu/nhược điểm của việc sử dụng hộ chiếu điện tử, việc nghiên cứu tìm hiểu sâu về mô hình cũng như tổ chức của các hệ thống hỗ trợ hộ chiếu điện tử là rất quan trọng. Với tiêu chí đó, trong bài báo này, chúng tôi hướng đến việc phân tích, đánh giá một số mô hình hộ chiếu điện tử đã được triển khai ở một số nước phát triển trên thế giới. Từ đó, đề xuất mô hình hộ chiếu theo ngữ cảnh ở Việt Nam.

Phần còn lại của bài báo này được tổ chức như sau : phần 2 giới thiệu mô hình hộ chiếu điện tử của một số nước trên thế giới. Phần 3 đề cập đến nhu cầu và thực trạng vấn đề hộ chiếu điện tử tại Việt Nam để từ đó đề xuất mô hình hộ chiếu điện tử cho công dân Việt Nam ở phần 4. Phần kết luận sẽ tóm lược lại những nội dung chính của bài báo này.

2. Các kiểu hộ chiếu điện tử

Để có cái nhìn thực trạng cũng như sự cần thiết của hộ chiếu điện tử, phần này sẽ đề cập đến một số mô hình hộ chiếu đang được nghiên cứu tìm hiểu cũng như vừa triển khai tại một số nước trên thế giới.

2.1. Hộ chiếu điện tử ở Châu Âu

Hộ chiếu điện tử ở Châu Âu được Ủy ban thường vụ của Cộng đồng chung EC rất quan tâm với định hướng triển khai sử dụng rộng rãi tại các nước thành viên. Việc sử dụng hộ chiếu điện tử cũng đã được phát triển tại nhiều nước ở châu Âu như Đức, Anh, Pháp.

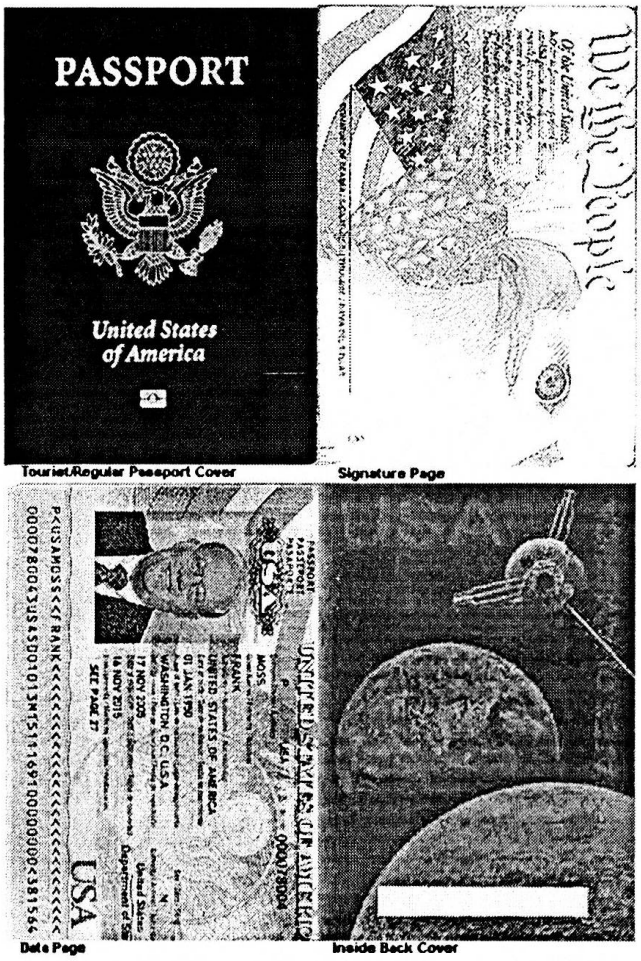
Nhìn chung, hộ chiếu điện tử đã và sẽ được sử dụng, như tại các nước Châu Âu đều sử dụng chuẩn do ICAO (International Civil Aviation Organization) đề xuất [7]. Các đặc trưng sinh trắc được chú trọng ở đây đều dựa trên ảnh mặt người và vân tay của công dân kết hợp lưu giữ cùng những thông tin cá nhân của họ trên một thẻ RFID [8,9].

2.2. Hộ chiếu điện tử ở Mỹ

Việc triển khai sử dụng hộ chiếu điện tử ở Mỹ tương đối chậm hơn so với một số nước khác như Singapore hay Đức, Pháp. Tuy nhiên, Mỹ lại là nước đầu tiên khởi xướng chương trình Visa Waiver Program (VWP) với 27* nước thành viên tham gia với ý tưởng chính : tất cả những công dân của những nước tham gia chương trình này sở hữu hộ chiếu điện tử sẽ được nhập cảnh vào 26 nước khác mà không cần phải xin thị thực. Kể từ tháng 8/2007, Mỹ chỉ còn cấp hộ chiếu điện tử cho công dân thay vì những kiểu hộ chiếu truyền thống trước đây.

Theo chuẩn hộ chiếu điện tử của Mỹ, các thông tin cá nhân và ảnh mặt người của công dân sẽ được lưu trong một thẻ RFID. Các dữ liệu sinh trắc và cá nhân trong chip RFID này sẽ được tổ chức và cài đặt bên trong trang bìa cuối của hộ chiếu.

* 27 nước này gồm : Andorra, Australia, Austria, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland và United Kingdom.



Hình 2. Hộ chiếu điện tử của Mỹ.

Việc xác thực một hộ chiếu điện tử, theo chuẩn ICAO, vẫn phải dựa trên sự kết hợp cả kiểm soát viên và hệ thống xác thực tự động thông qua việc so khớp ảnh mặt người. Dĩ nhiên, quá trình so khớp ảnh mặt người dựa trên ảnh chụp tự động khi xác thực công dân và dữ liệu sinh trắc đã được lưu trong chip RFID.

3. Thực trạng và nhu cầu tại Việt Nam

Trên thế giới có một số nước đã triển khai hệ thống hộ chiếu điện tử cho điều khiển xuất nhập cảnh như đã nói ở phần trên. Điển hình vẫn là các nước tham gia chương trình VWP của Mỹ Nhằm mục đích chống giả mạo hộ chiếu, thuận tiện và nâng cao độ chính xác.

Ở Việt Nam điều đó càng cần thiết trong con đường hội nhập và phát triển, nhất là khi đã tham gia tổ chức thương mại quốc tế WTO. Vấn đề kiểm soát hiệu quả việc xuất nhập cảnh của công dân, không những đối với người Việt Nam mà còn cả đối với công dân ngoài nước đang trở nên thời sự. Sớm muộn gì chúng ta cũng phải có chương trình xây dựng và triển khai hộ chiếu điện tử để phù hợp với các nhu cầu phát triển của xã hội, tăng tính an toàn/an ninh cũng như chống giả mạo hộ chiếu/thị thực.

Với những nhu cầu đó, chương trình nghiên cứu, xây dựng và triển khai hộ chiếu điện tử ở Việt Nam là một bài toán cần có sự đầu tư nghiên cứu và từng bước xây dựng. Chúng tôi nghĩ rằng với sự đầu tư thích đáng, chúng ta có đủ khả năng để xây dựng và phát triển hoàn thiện hệ thống hộ chiếu điện tử tại Việt Nam, trước tiên là ở các sân bay sau đó là phát triển ở các cửa khẩu và hải cảng. Hơn nữa, lĩnh vực sinh trắc học đã và đang được có nhiều thành tựu khoa học trên thế giới, từ đó chúng ta có thể tiếp thu công nghệ, trình độ và kinh nghiệm triển khai, ứng dụng cho hệ thống hộ chiếu điện tử ở Việt Nam.

4. Mô hình đề xuất

Việc xây dựng một mô hình đầy đủ cho hệ thống kiểm soát người mang hộ chiếu điện tử rất phức tạp và cần có sự đầu tư ở mức vĩ mô. Trong bài báo này, chúng tôi chủ yếu hướng đến việc đề xuất mô hình tổ chức những dữ liệu sinh trắc quan trọng trong hộ chiếu điện tử và quy trình kiểm soát người mang hộ chiếu điện tử. Những vấn đề khác như xây dựng quy trình xác thực, hệ thống cở sở khóa công khai, .. sẽ được nghiên cứu và báo cáo trong những bài báo sắp tới.

Định hướng chung của mô hình chúng tôi đề xuất luôn bám sát mô hình chuẩn của tổ chức

ICAO đề ra. Dựa trên những kết quả nghiên cứu từ [10,11] về vấn đề an toàn bảo mật thông tin trong hộ chiếu điện tử, việc kết hợp hệ thống PKI trong [12,13] và kỹ thuật xác thực hai chiều chúng tôi đề xuất trong [14] cho phép khẳng định tiềm năng bảo đảm an toàn/an ninh của mô hình chúng tôi đề xuất ở đây.

4.1. Thông tin lưu trữ

Ngoài những thông tin cá nhân liên quan đến công dân như hộ chiếu truyền thống, hộ chiếu điện tử theo mô hình đề xuất còn có thêm hai dữ liệu sinh trắc học khác: ảnh hai vân tay ngón trỏ và ảnh mống mắt. Tất cả những dữ liệu sinh trắc này phải được gói gọn trong một thẻ nhớ thông minh không cần tiếp xúc (chuẩn ISO 14443B) có dung lượng tối thiểu là 128KB. Vị trí của thẻ nhớ thông minh không cần tiếp xúc cần phải được phủ kín trong trang bìa sau của hộ chiếu.

4.2. Tổ chức dữ liệu

Theo mô hình đề xuất, hộ chiếu điện tử sẽ được tổ chức và cài đặt theo các đặc tả của ICAO [15]. Cấu trúc dữ liệu logic sẽ tuân theo tài liệu đặc tả của tổ chức ICAO số 9303 [16].

Để đảm bảo dữ liệu lưu trong thẻ nhớ được xử lý một cách hiệu quả, một số yêu cầu sau phải được đảm bảo trong quá trình thu nhập dữ liệu:

- Kích thước của ảnh mặt người sau khi nén theo chuẩn JPEG2000 phải đảm bảo bé hơn 20KB,
- Kích thước đặc trưng hai ảnh mống mắt phải đảm bảo bé hơn 60KB.
- Kích thước hai ảnh vân tay ngón trỏ phải bé hơn 20KB.

4.3. Quy trình xử kiểm soát hộ chiếu điện tử

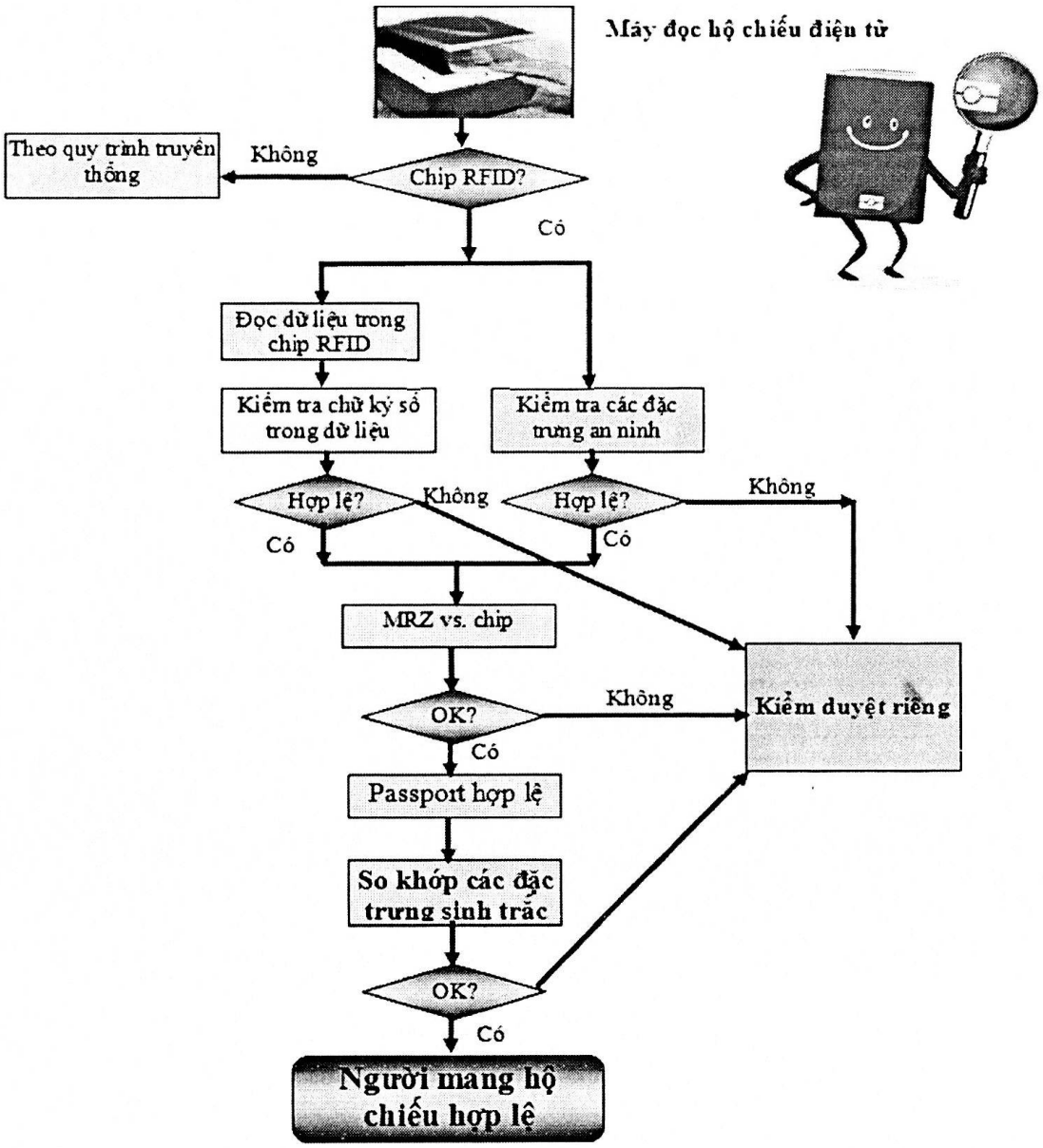
Công dân mang hộ chiếu điện tử sẽ được nhân viên kiểm soát cửa khẩu xuất/nhập cảnh tiến hành thực hiện việc kiểm tra hộ chiếu tuân theo quy trình minh họa ở hình dưới đây:

B1. Máy đọc hộ chiếu điện tử trước tiên sẽ kiểm tra sự tồn tại của chip RFID (thẻ nhớ thông minh không cần tiếp xúc), nếu không có, hộ chiếu này sẽ được coi như hộ chiếu truyền thống và quy trình kiểm tra sẽ tuân thủ đúng quy trình truyền thống. Nếu có, chuyển sang B2.

B2. Hệ thống kiểm tra sẽ tiến hành đọc dữ liệu trong thẻ nhớ không cần tiếp xúc của hộ chiếu điện tử và kiểm tra tính hợp lệ của những dữ liệu đó thông qua các chữ ký số (chẳng hạn như Country Signing Certification Authority (CSCA), Document Signer (DS), ...). Song song với bước này, kiểm soát viên cũng phải kết hợp tiến hành kiểm tra an ninh của hộ chiếu điện tử (về mặt trực quan như quy trình truyền thống). Nếu cả quá trình kiểm tra này đều có kết quả hợp lệ, hệ thống sẽ chuyển sang bước B3. Nếu không, người mang hộ chiếu này sẽ phải được kiểm soát kỹ lưỡng hơn bằng những biện pháp nghiệp vụ riêng đối với người mang hộ chiếu không hợp lệ.

B3. Hệ thống tiến hành so khớp những dữ liệu lưu trong thẻ nhớ không cần tiếp xúc và những dữ liệu trong vùng MRZ ở trang chứa thông tin cá nhân. Nếu kết quả không khớp, người mang hộ chiếu này cũng phải được kiểm soát riêng đối với trường hợp hộ chiếu không hợp lệ. Nếu trùng khớp, hệ thống chuyển sang bước B4.

B4. Ở bước này, hệ thống tiến hày so khớp những đặc trưng sinh trắc học đã lưu trong thẻ nhớ không cần tiếp xúc và những đặc trưng thu trích trực tiếp từ người mang hộ chiếu. Quá trình này là so khớp 1-1 với những đặc trưng cụ thể là ảnh hai vân tay, ảnh mặt người và ảnh mống mắt. Nếu kết quả so khớp hợp lệ, người mang hộ chiếu điện tử này chính là người chủ hộ chiếu đó và quy trình kiểm tra kết thúc với kết quả hợp lệ. Nếu không, kiểm soát viên phải tiến hành kiểm tra riêng như đối với trường hợp người mang hộ chiếu không hợp lệ.



Hình 3. Quy trình kiểm soát hộ chiếu điện tử đề xuất.

4.4. Bảo mật trong hộ chiếu điện tử

Vấn đề bảo mật thông tin lưu trong thẻ nhớ không cần tiếp xúc của hộ chiếu điện tử chủ yếu liên quan đến những nguy cơ chính của công nghệ RFID. Theo [17], có 5 nguy cơ mất an toàn/bảo mật thông tin đối với công nghệ RFID như sau:

- **Clandestine Tracking**: nguy cơ này liên quan đến định danh của một thẻ RFID. Việc xác định được ID của một thẻ nhớ không cần tiếp xúc có thể cho phép những nghe lén xác định được nguồn gốc của hộ chiếu điện tử, chẳng hạn như quốc tịch của người mang hộ chiếu.

- **Skimming and Cloning**: nguy cơ này liên quan đến khả năng nhân bản của chip RFID. Từ đó, nguy cơ nhân bản hộ chiếu điện tử là một trong những nguy cơ quan trọng cần phải được cân nhắc trong quá trình phát hành và sử dụng.

- **Eavesdropping**: nguy cơ nghe lén phức tạp luôn được coi là nguy cơ có tính nguy hiểm nhất trong an toàn, bảo mật hộ chiếu điện tử. Nguy cơ diễn ra trong quá trình đọc dữ liệu từ thẻ nhớ không cần tiếp xúc đến máy đọc. Lý do chủ yếu xuất phát từ khả năng những thông tin được truyền bằng công nghệ RFID giữa chip-reader có thể bị nghe lén trong một khoảng cách nhất định (khoảng vài mét). Tuy nhiên, trong trường hợp đối với những cửa khẩu xuất/nhập cảnh, việc kiểm soát nguy cơ này lại có thể thực hiện tốt với việc kiểm tra tự động những thiết bị đọc thẻ RFID khác.

- **Biometric Data-Leakage**: nguy cơ lộ dữ liệu sinh trắc. Nguy cơ này liên quan mật thiết đến vấn đề đảm bảo an toàn đối với những dữ liệu sinh trắc nói riêng và những dữ liệu được lưu trong chip nói chung của các thẻ nhớ không cần tiếp xúc.

- **Cryptographic Weaknesses**: nguy cơ này liên quan đến mô hình đảm bảo an toàn, bảo mật thông tin lưu trong chip RFID. Việc sử dụng các kỹ thuật đảm bảo an toàn bảo mật dữ liệu phải đảm bảo giải quyết được những vấn đề đặt ra liên quan đến 4 nguy cơ nêu trên.

Cơ chế bảo mật thông tin trong [13] được khuyến cáo sử dụng độ dài các khóa như sau với giao thức BAC (Basic Access Control):

- RSA:
  - Country Signing CA Keys: modulus n 3072 bits
  - Document Signer Keys: modulus n 2048 bits
  - Active Authentication Keys: modulus n 1024 bits
- DSA – Digital Signature Algorithms:
  - Country Signing CA Keys: modulus p 3072 bits, modulus q 256 bits
  - Document Signer Keys: modulus p 2048 bits, modulus q 224 bits
  - Active Authentication Keys: modulus p 1024 bits, modulus q 160 bits
- ECDSA – Elliptic Curve DSA:
  - Country Signing CA Keys: base point order 256 bits
  - Document Signer Keys: base point order 224 bits
  - Active Authentication Keys: base point order 160 bits

Với mô hình xác thực hai chiều giữa thẻ nhớ không cần tiếp xúc và máy đọc dựa trên bài toán ECDLP (Elliptic curve discrete logarithm problem) của hệ mật dựa trên đường cong Elliptic, kết hợp với cở sở hạ tầng khóa công khai đã được nêu trong [14], vấn đề an toàn bảo mật dữ liệu trong hộ chiếu điện tử được đảm bảo để giải quyết chống lại năm nguy cơ nêu trên.

5. Kết luận

Bài báo này đề cập chủ yếu đến một số khái niệm cơ bản của hộ chiếu điện tử và mô hình đề xuất việc sử dụng hộ chiếu điện tử ở Việt Nam. Từ những phân tích về tiềm năng ứng dụng của ngành xác thực dựa trên các đặc trưng sinh trắc, những tìm hiểu về mô hình hộ chiếu điện tử đã được nhiều nước trên thế giới áp dụng, mô hình đề xuất đã đáp ứng được những yêu cầu cả về

bảo đảm an toàn/an ninh cho hộ chiếu điện tử lẫn quá trình kiểm soát người mang hộ chiếu.

Lời cảm ơn: *Công trình này được tài trợ một phần từ đề tài mang mã số QC.06.03, và một phần từ đề tài mang mã số QC.07.11, Đại học Quốc gia Hà Nội.*

Tài liệu tham khảo

[1] Department of Foreign Affairs and Trade: *The Australian ePassport*, Australia, 2006 , http://www.dfat.gov.au/dept/passports/

[2] U.S. Department of State, *Issuance of an Electronic Passport*, 2006, http://www.state.gov/r/pa/prs/ps/2006/61538.htm.

[3] Cavoukian, Ann, *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology,* Information and Privacy Commissioner of Ontario, 42 pages, 2004.

[4] Klaus Finkenzeller, *The RFID handbook,* ISBN: 0-470-84402-7, 464 Pages, 2nd edition Wiley & Sons, Germany, 2003.

[5] Ari Juels, David Molnar, and David Wagner, Security and Privacy Issues in E-passports, in *Security and Privacy for Emerging Areas in Communications Networks*, IEEE (2005) 74.

[6] D.P. Hanh, N.N. Hoá, Biometric Authentication: state of the art and some perspectives in Vietnam, *National Conference on Modern Topics in Information Technology*, Dalat, 06/2006.

[7] ICAO Tag MRTD/NTWG, *Biometric Deployment of Machine Readable Travel Documents*, Technical report of International Civil Aviation Organization, May 2004.

[8] Ministry of Swedish Police, *About Biometric Passports,* Presentation document to citizens, 2007. (http://www.polisen.se/inter/nodeid=33373&pageversion=1.html).

[9] Ministry of Danish Police: *About Biometric Passports,* Presentation document to citizens (http://www.politi.dk/da/borgerservice/pas/biometrisk_pas/).

[10] Matt Bishop, *Computer Security; Art and Science,* 1st Edition. Addison Wesley, 2003.

[11] Juels, Ari, *RFID Security and Privacy: A Research Survey*. RSA Laboratories Edition, 2005.

[12] ICAO TAG MRTD, *PKI for Machine Readable Travel Documents offering ICC Read-Only Access*, Technical specification, United States, 2004.

[13] ICAO Secretariat, *Information Paper – Issues of the ICAO Public Key Directory (PKD),* Technical specification, United States, 2006.

[14] H.Nguyen et al, Mutual Authentication between RFID tag & reader by using the elliptic curve cryptography, accepted to presence at the International *Workshop on Computational Intelligence and Security – CIS, 2007*", Hong Kong, China (2007).

[15] ICAO MRTD/LDS, *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.

[16] ICAO MRTD Supplement, *Machine Readable Travel Documents; Supplement to Doc 9303-Part 1-Sixth Edition,* Technical report of International Civil Aviation Organization, Release 3, United States, 2005.

[17] Dale R. Thompson, Neeraj Chaudhry, and Craig W. Thompson, RFID Security Threat Model, *Conference on Applied Research in Information Technology ALAR* (2006) 11.

Proposal for e-passport in Viet Nam

Du Phuong Hanh, Truong Thi Thu Hien, Nguyen Ngoc Hoa

Department of Information Technology, College of Technology, VNU
144 Xuân Thủy, Hanoi, Vietnam

This paper investigates both of the techniques and the implementation of e-passport in order to figure out a model of e-passport in Vietnam. Based on the ICAO standard, by combining three biometric features: a face, two iris and two fingerprints, our proposal model profits the best of the technological evoluation. Moreover, by using the model « Mutual Authentication of RFID Tag-Reader using Elliptic Curve Cryptography », our model will protect all threats related an e-passport and brings it more safety/security.