TĂNG CƯỜNG AN NINH TRONG CÁC HỆ THỐNG BẢO MẬT NHỜ CÔNG NGHỆ MATCH-ON-CARD

Trần Thị Thu Hà*

Ngày nhận: 27/10/2014
Ngày nhận bản sửa: 6/11/2014
Ngày duyệt đăng: 25/11/2014

Tóm tắt:

Công nghệ sinh trắc học và công nghệ thẻ thông minh ngày càng được biết là những phương tiện nhận dạng và xác thực một cách chính xác. Các công nghệ này giúp giảm bớt rủi ro so với các phương pháp xác thực thông thường như kiểm tra giấy tờ tùy thân, so sánh chữ ký, mã PIN,... Sự kết hợp hai công nghệ này làm tăng tính linh hoạt, tính bảo mật và tính xác thực mạnh trong các hệ thống bảo mật. Công nghệ Nhận dạng sinh trắc học chạy ngay bên trong thẻ thông minh (Match-on-Card, viết tắt là MoC) đã được ứng dụng trong các hệ thống bảo mật trên thế giới trong những năm gần đây. Bài viết này tổng hợp và phân tích những ưu điểm nổi bật của công nghệ MoC với mục đích cung cấp cho các tổ chức một giải pháp có hiệu quả để giúp tăng cường tính bảo mật trong các hệ thống xác thực. Nghiên cứu cũng đưa ra một số khuyến nghị để có thể áp dụng thành công công nghệ này trong các hệ thống bảo mật.

Từ khóa: Hệ thống xác thực, công nghệ nhận dạng sinh trắc học trên thẻ thông minh, lưu trữ trên thẻ thông minh, nhận dạng dấu vân tay, sinh trắc học.

Enhancing security in the secure systems by Match-on-Card technology

Abstract:

The Biometric technology and the Smartcard technology are becoming increasingly popular as a means of accurate identity authentication. These technologies help reduce the risk in comparison with the common authentication methods such as verifying personal papers (e.g. ID card, driving license, passport), using a password and using PIN, etc. The combination of both technologies offers the advantages of mobility, security and strong identity authentication in the security systems. The Match-on-Card (MoC) technology has been used in the secure system density in the world in recent years. This article summarizes and analyzes the key advantages of the MoC to provide organizations an effective solution to enhance the security of the authentication system. The author also provides a number of recommendations to the successful application of this technology in the security system.

Keywords: identity authentication, authentication system, Match-on-Card technology

1. Đặt vấn đề

Trong thời đại ngày nay, các giao dịch điện tử trong các hoạt động ngân hàng, chứng khoán, dịch vụ công,… ngày càng trở nên phổ biến. Việc xác thực chính xác khách hàng hoặc người sử dụng trong các giao dịch thông thường hay giao dịch điện tử là vấn đề quan trọng mà các tổ chức cần quan tâm. Các phương pháp xác thực thường hay được sử dụng trong các hệ thống giao dịch có thể là kiểm tra giấy tờ tùy thân (ví dụ như chứng minh thư nhân dân, hộ chiếu, bằng lái xe,…), so sánh chữ ký của người giao dịch với chữ mẫu đã được đăng ký, nhập mật khẩu để truy cập vào hệ thống, nhận dạng cá nhân qua mã PIN. Tuy nhiên các phương pháp này có những bất tiện và tiềm ẩn các rủi ro vì các lý do sau đây:

- *Phương pháp kiểm tra giấy tờ tùy thân:* đây là phương pháp phổ biến, được sử dụng rộng rãi tại những điểm giao dịch trực tiếp. Người làm nhiệm vụ xác thực sẽ kiểm tra giấy tờ tùy thân và đối chiếu với người xuất trình giấy tờ để xác minh đúng người có quyền thực hiện giao dịch. Độ chính xác của phương pháp này phụ thuộc vào kinh nghiệm, tình trạng sức khỏe và trạng thái tinh thần,… của người kiểm tra. Mặt khác, phương pháp này có thể gây bất tiện cho khách hàng nếu họ quên giấy tờ tùy thân hoặc bị mất mà chưa kịp làm lại. Trong trường hợp giấy tờ tùy thân bị xuống cấp theo thời gian (ví dụ như, bị nhòe ảnh và chữ) sẽ gây khó khăn trong việc xác thực.

- *Phương pháp so sánh chữ ký*: khi giao dịch, khách hàng được yêu cầu ký tên và chữ ký này được so sánh với chữ ký mẫu đã đăng ký. Phương pháp này có thể gây bất tiện cho những khách hàng ký không hoàn toàn giống chữ ký mẫu và có thể xảy ra rủi ro khi kẻ xấu sử dụng chữ ký giả.

- *Phương pháp sử dụng mật khẩu*: phương pháp này yêu cầu người sử dụng phải nhớ mật khẩu và phải giữ bí mật về mật khẩu của mình. Tuy nhiên, mật khẩu cũng có khả năng bị kẻ gian lấy cắp.

- *Phương pháp nhận dạng qua mã số cá nhân (PIN):* việc ghi nhớ mã PIN cũng gây ra không ít phiền phức cho người sử dụng khi một cá nhân có nhiều tài khoản khác nhau. Mã PIN cũng có khả năng bị lộ và bị lấy cắp.

Để tránh được những rủi ro nói trên, ngày nay nhiều hệ thống nhận dạng và xác thực người dùng đã sử dụng công nghệ sinh trắc học và công nghệ thẻ thông minh được coi là các công nghệ trợ giúp tính an toàn và chính xác cao hơn. Việc kết hợp hai công nghệ này tăng cường độ bảo mật và an toàn thông tin trong các hệ thống xác thực lên mức cao hơn nữa. Câu hỏi đặt ra là nên chọn công nghệ nào trong các công nghệ kết hợp giữa sinh trắc học và thẻ thông minh cho các hệ thống xác thực người dùng sao cho vừa đảm bảo tính an toàn cao, tránh được các rủi ro và với chi phí có thể chấp nhận được.

Bài viết này sẽ giới thiệu công nghệ Match-on-Card (viết tắt là Moc) là một trong các công nghệ kết hợp công nghệ sinh trắc học và thẻ thông minh có thể đáp ứng yêu cầu đó. Bằng cách tổng hợp các nghiên cứu về các phân tích những ưu điểm vượt trội của của công nghệ MoC và minh họa bằng các ứng dụng thành công công nghệ MoC trong các hệ thống xác thực trên thế giới trong những năm gần đây, tác giả chỉ ra lý do tại sao nên chọn công nghệ này trong các hệ thống xác thực. Nội dung chính của bài báo gồm những phần sau đây: (1) Giới thiệu tổng quan về các công nghệ sinh trắc học, thẻ thông minh, các giải pháp kết hợp giữa sinh trắc học và thẻ thông minh được sử dụng trong các hệ thống xác thực; (2) Giải thích lý do tại sao lại lựa chọn công nghệ MoC trong các hệ thống xác thực; (3) Đưa ra những khuyến nghị về việc áp dụng và những nhân tố cần thiết để ứng dụng thành công công nghệ MoC trong các hệ thống xác thực, đặc biệt là trong các giao dịch điện tử trong các hoạt động dịch vụ công, ngân hàng, chứng khoán,…

Nội dung của bài báo được viết dựa trên việc nghiên cứu và tổng hợp tài liệu từ các bài báo nghiên cứu liên quan đến vấn đề này, từ các website trên internet và phỏng vấn Giám đốc kỹ thuật và các chuyên viên phòng Phần mềm của Công ty Cổ phần Thông minh MKsmart (http://mksmart.com.vn).

2. Tổng quan về công nghệ sinh trắc học, thẻ thông minh và các công nghệ kết hợp thẻ thông minh và sinh trắc học

2.1. Công nghệ sinh trắc học và ứng dụng trong việc nhận diện và xác thực người sử dụng

Sinh trắc học hay Công nghệ Sinh trắc học (Biometric)- là công nghệ nhận diện một con người bằng cách phân tích những thuộc tính vật lý, đặc điểm sinh học riêng của mỗi cá nhân. Các phương pháp sinh trắc học có sẵn hiện nay là nhận dạng vân tay, phân tích khuôn mặt, giọng nói, dáng đi, mẫu mống mắt,… (Maltoni và các cộng sự, 2003).

Bản thân mỗi con người có thể trở thành mật khẩu. Bởi vì mỗi người có một đặc điểm sinh học duy nhất. Dữ liệu sinh trắc học của từng cá nhân sẽ được kết hợp với nhau bằng phần mềm để tạo ra mật khẩu dành cho những giao dịch điện tử. Phương thức đó là Công nghệ sinh trắc đa nhân tố (Minh Long, 2011).

Theo Smart Card Alliance (2011) thì một hệ thống sinh trắc học thường có bốn thành phần sau: (1) Một thiết bị để quét và thu được các đặc điểm sinh trắc học "sống" của người dùng; (2) Một phần mềm để xử lý các dữ liệu thô thành dạng mẫu sinh trắc học để lưu trữ và đối chiếu; (3) Phần mềm đối chiếu để so sánh mẫu sinh trắc học đã được lưu trữ trong hệ thống với mẫu được lấy từ cơ thể sống và (4) Một giao diện với hệ thống ứng dụng để trao đổi kết quả đối chiếu.

Đăng ký (Enrollment) và Đối chiếu (Matching) là hai quy trình khác nhau trong hệ thống sinh trắc học (Smart Card Alliance, 2011).

- *Đăng ký:* mẫu đặc điểm sinh trắc học của một cá nhân được thu nhận nhờ các thiết bị đặc biệt. Ví dụ như mẫu vân tay được lấy qua đầu đọc vân tay, giọng nói được thu qua micro, khuôn mặt, mống mắt được thu nhận qua camera,… Sau đó những đặc điểm duy nhất được trích rút để tạo ra mẫu sinh trắc học của người sử dụng. Mẫu sinh trắc học này được lưu trữ trong một cơ sở dữ liệu hoặc trong một thẻ nhận dạng cá nhân để được sử dụng sau này.

- *Đối chiếu*: Khi tiến hành giao dịch, mẫu sinh trắc học của cá nhân lại được thu nhận, xử lý và trích rút để tạo ra mẫu sinh trắc học "sống" của người đó. Sau đó, mẫu sinh trắc học "sống" này được so sánh với mẫu (hoặc các mẫu) sinh trắc học đã được lưu trữ trước đó để tìm ra những điểm chung giữa hai mẫu và xác nhận người sử dụng hiện thời có đúng là người đã đăng ký hay không.

Các hệ thống bảo mật sử dụng xác thực (Authentication) bằng sinh trắc học với hai mục đích: nhận dạng (identification) và kiểm chứng (verification) (Smart Card Alliance, 2011; Gobi và các cộng sự, 2014).

- *Nhận dạng (so sánh một-nhiều)* là xác định xem liệu một người có tồn tại trong số những người đã đăng ký hay không bằng cách so sánh mẫu sinh trắc học "sống" của người đó với tất cả các mẫu đã được lưu trong hệ thống. Ví dụ, chức năng nhận dạng này được sử dụng trong hệ thống Tuyển sinh để biết một thí sinh đã ghi danh hay chưa.

- *Kiểm chứng (so sánh một-một)* là xác định xem mẫu sinh trắc học "sống" có phù hợp với mẫu sinh trắc học đã được lưu trữ hay không. Ví dụ, chức năng này được sử dụng để xác thực một người có được phép truy nhập vào hệ thống hay không.

2.2. Công nghệ nhận dạng vân tay và ứng dụng trong các hệ thống bảo mật

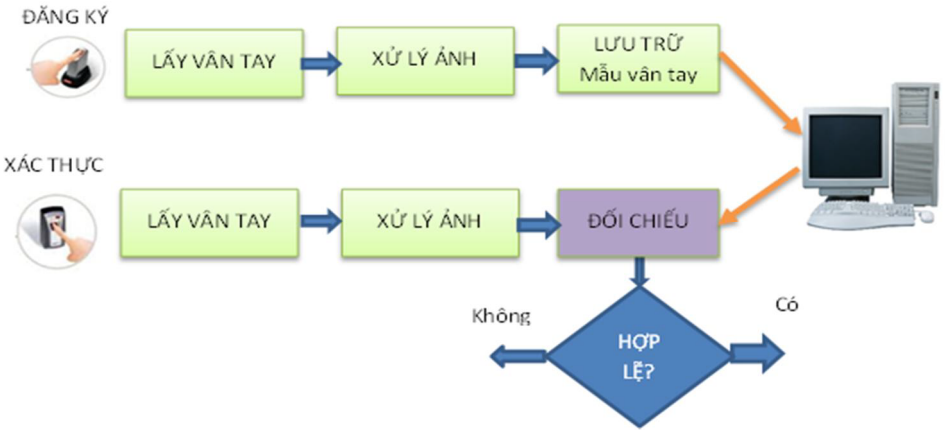
Dấu vân tay là một đặc điểm quan trọng để phân biệt giữa người này và người khác. Việc lưu trữ vân tay đã thay đổi nhờ sự phát triển của công nghệ. Thời gian đầu, mẫu vân tay được lấy bằng cách lăn tay trên mực và lưu trữ trên giấy. Cách này hiện nay vẫn đang đang được áp dụng ở Việt Nam khi cấp mới hoặc làm lại chứng minh thư cho một người nào đó. Với công nghệ hiện đại, hiện nay nhiều hệ thống cho phép quét vân tay trên máy, xử lý và lưu trữ mẫu vân tay trong các thiết bị kỹ thuật số.

Trong các công nghệ sinh trắc học, công nghệ nhận dạng vân tay được lựa chọn nhiều nhất vì đó là công nghệ sinh trắc học lâu đời nhất, có số người chấp nhận sử dụng nhiều nhất và các thiết bị đọc dấu vân tay riêng có sẵn với giá cả hợp lý. Dựa vào đặc điểm cấu tạo hình dạng vân tay của mỗi người là duy nhất và không thay đổi từ khi mới sinh ra cho đến khi về già, các nhà sinh trắc học sẽ biến nó thành chiếc chìa khoá riêng mà chỉ mỗi cá nhân mới có thể sử dụng. Chiếc chìa khóa riêng này giúp mỗi người tránh được việc bị trộm cắp, lạm dụng hoặc giả mạo các loại giấy tờ tuỳ thân, thẻ ngân hàng, hộ chiếu,... Hệ thống sinh trắc học truyền thống sẽ ghi nhận mẫu vân tay của người sử dụng, số hóa và lưu trữ trong một hệ thống cơ sở dữ liệu trung tâm cùng với các thông tin nhận dạng khác.

Hình 1 mô tả quy trình đăng ký mẫu vân tay lần đầu và xác thực mẫu vân tay theo truyền thống. Khi đăng ký, mẫu vân tay của người sử dụng được lưu trữ vào cơ sở dữ liệu trong hệ thống máy tính. Khi người sử dụng thực hiện một giao dịch nào đó, việc xác thực yêu cầu cần phải lấy dấu vân tay của người đó và so sánh, đối chiếu với mẫu vân tay đã được lưu trong hệ thống. Quá trình xử lý dữ liệu sẽ được thiết bị chuyển sang các dữ liệu số và ra thông báo rằng dấu vân tay đó là hợp lệ hay không hợp lệ để cho phép hệ thống thực hiện các chức năng tiếp theo.

Ưu điểm của việc ứng dụng công nghệ nhận dạng vân tay trong các hệ thống bảo mật là đáp ứng được các yêu cầu bảo vệ dữ liệu, đảm bảo an ninh an toàn

Hình 1: Quy trình đăng ký mẫu vân tay và xác thực dấu vân tay theo truyền thống



Nguồn: tác giả xây dựng dựa trên kiến thức tổng hợp từ các tài liệu của Moon và các cộng sự, 2014; Gobi và các cộng sự, 2014.

với độ chính xác cao hơn các phương pháp xác thực nhờ sử dụng mật khẩu hoặc mã số PIN và tiện lợi cho người sử dụng vì không cần phải nhớ và giữ bí mật về mật khẩu hoặc mã số PIN của mình. Tuy nhiên, phương pháp này yêu cầu mẫu sinh trắc học phải lưu trữ trong cơ sở dữ liệu của hệ thống. Việc bảo mật sẽ an toàn nếu chỉ những ai được gán quyền mới được truy nhập vào cơ sở dữ liệu này. Rủi ro sẽ xảy ra nếu cơ sở dữ liệu này bị các tội phạm máy tính (hacker) đánh cắp hoặc phá hỏng. Bên cạnh đó tính riêng tư trong các hệ thống xác thực sinh trắc học cũng là vấn đề cần bàn đến (Maltoni và các cộng sự, 2003).

Thẻ thông minh (Smartcard) là loại thẻ nhựa được gắn chip chuyên dùng có bộ vi xử lý (Micro-processor) và các loại bộ nhớ ROM (Read Only Memory), RAM (Random Access Memory), EEP-ROM (Electrically Erasable Programmable Read Only Memory) (*Daesung Moon và các cộng sự, 2014)* hoặc FLASH, I/O (Input/Output) Control (Kiểm soát Vào/Ra)… có thể lập trình được như trên máy tính để nhận/gửi, lưu trữ và xử lý dữ liệu ngay bên trong thẻ. Với cấu trúc như vậy, thẻ thông minh có chức năng lưu trữ thông tin và xử lý thông tin tương tự như một máy tính thu nhỏ. Chức năng lưu trữ thông tin của thẻ thông minh tạo khả năng chống lại sự tấn công mà không cần phụ thuộc vào bất kỳ yếu tố trợ giúp bên ngoài nào.

Sử dụng thẻ thông minh có thể cung cấp chứng thực bảo mật mạnh mẽ cho đăng nhập một lần SSO (Single Sign-On) trong các tổ chức lớn rất tiện lợi khi sử dụng điện toán đám mây (Cloud Computing). Với chức năng lưu trữ được nhiều thông tin hơn và độ an toàn thông tin cao hơn nhiều các loại thẻ từ,… thẻ thông minh thường được sử dụng với trong các ứng dụng nhận dạng, xác thực, lưu trữ dữ liệu và xử lý ứng dụng (Henry, 2007).

2.3. Các công nghệ kết hợp thẻ thông minh và sinh trắc học

Như phần trên đã trình bày, thẻ thông minh đã được thừa nhận là một trong những hình thức xác thực điện tử an toàn nhất và đáng tin cậy và công nghệ sinh trắc học được coi là cần thiết khi thiết kế hệ thống nhận dạng có tính bảo mật cao.

Thay cho việc phải lưu trữ cơ sở dữ liệu sinh trắc học trên một hệ thống máy chủ trung tâm và nhà cung cấp dịch vụ thì mỗi người có thể giữ các dữ liệu sinh trắc học của chính mình trong tay nhờ chiếc thẻ thông minh. Chiếc thẻ thông minh này có thể được mang theo người một cách thuận tiện tới bất kỳ nơi nào mà không phụ thuộc vào hệ thống máy chủ và nhà cung cấp dịch vụ. Việc kết hợp công nghệ thẻ thông minh với công nghệ sinh trắc học cho phép xác thực danh tính của chủ thẻ một cách an toàn và tin cậy rất cao và tính riêng tư được bảo đảm ở mức độ cao (Jaracz, 2013).

Có ba công nghệ chính kết hợp thẻ thông minh và sinh trắc học (Terry, 2002; Pożgaj và Đurinek, 2007):

- *Công nghệ ToC (Template-on-card)* cho phép toàn bộ việc lấy dữ liệu, rút trích các đặc điểm và đối chiếu mẫu sinh trắc học đều được thực hiện bên ngoài thẻ ngoại trừ việc lưu trữ mẫu sinh trắc học ban đầu bên trong thẻ. Khi đăng ký, các mẫu sinh trắc học (ví dụ như vân tay) được nạp và lưu trữ trên

thẻ thông minh. Khi cần xác thực chủ thẻ thì mẫu sinh trắc học được chuyển từ thẻ thông minh tới hệ thống sinh trắc học bên ngoài để so sánh với mẫu sinh trắc học "sống" của chủ thẻ. Các thiết bị bên ngoài có thể là máy tính (PC, Laptop) hoặc POS (Point of the Sale) có đầu đọc vân tay (Finger Print Reader) và chương trình xác thực chạy trong PC/POS này.

- *Công nghệ MoC (Match-on-Card)* khác với công nghệ ToC ở chỗ các công việc lấy mẫu dữ liệu và trích rút các đặc điểm sinh trắc học được thực hiện bên ngoài thẻ trong khi việc đối chiếu được thực hiện ngay bên trong thẻ. Với công nghệ MoC, khi đăng ký các đặc điểm sinh học của chủ thẻ sẽ được số hóa và lưu trữ trên bộ nhớ được bảo mật của thẻ thông minh. Khi cần xác thực, các thiết bị bên ngoài thẻ sẽ đọc mẫu sinh trắc học "sống" đưa vào thẻ thông minh. Việc lưu trữ và đối chiếu mẫu vân tay được thực hiện ngay bên trong thẻ thông minh và kết quả đối chiếu được đưa ra các thiết bị bên ngoài. Phương pháp này bảo vệ các mẫu được đăng ký ban đầu vì nó được duy trì trong các thẻ thông minh và không bao giờ được truyền ra bên ngoài thẻ. Tính riêng tư của chủ thẻ được bảo đảm nhờ kỹ thuật này vì thông tin mẫu sinh trắc học của chủ thẻ không cần lấy ra từ các thẻ thông minh.

- *Công nghệ SoC (System-on-Card)* tích hợp toàn bộ các công việc lấy dữ liệu, trích rút các đặc điểm sinh trắc học và đối chiếu mẫu sinh trắc học ngay bên trong thẻ thông minh. Cả hai mẫu sinh trắc học được đăng ký ban đầu và mẫu cần xác thực đều được tính toán trong thẻ thông minh và không được lấy ra khỏi thẻ.

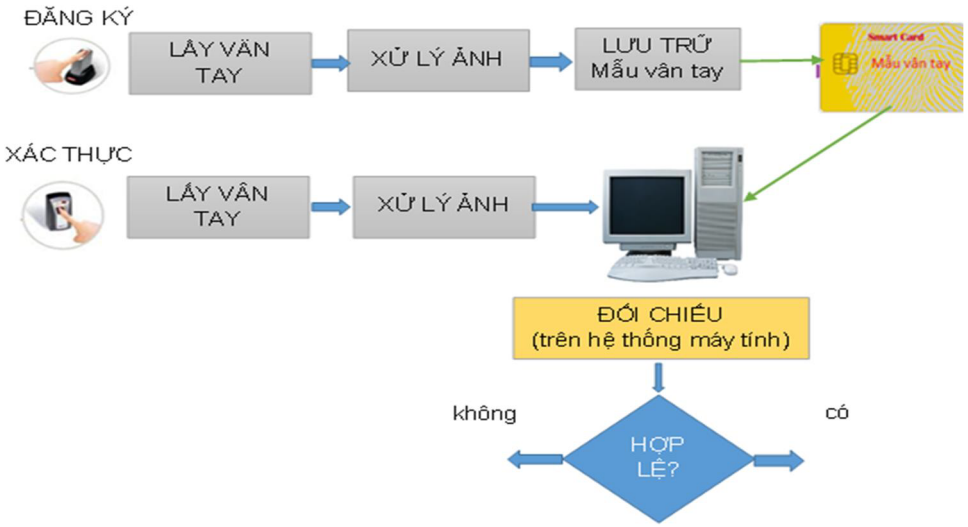
3. Lý do nên chọn công nghệ Moc trong các hệ thống bảo mật

Tính bảo mật của các hệ thống sinh trắc học phụ thuộc nhiều vào nơi xử lý ảnh và đối chiếu các đặc điểm sinh trắc học. Trong ba công nghệ kể trên công nghệ ToC cho môi trường kém bảo mật nhất trong khi công nghệ SoC cho môi trường bảo mật cao nhất. Tuy nhiên, công nghệ SoC có chi phí cao và không được phổ biến (*Bălănoiu, 2009*; *Yau Wei Yun và các cộng sự, không năm xuất bản)*. Ngoài ra, công nghệ ToC và MoC không chỉ áp dụng cho dấu vân tay mà có thể áp dụng cho các đặc điểm sinh học khác, trong khi công nghệ SoC chỉ áp dụng được cho dấu vân tay (*Bălănoiu, 2009)*. Vì vậy phần sau đây tập trung so sánh quy trình đăng ký và xác thực của các hệ thống dựa trên công nghệ ToC và MoC. Từ đó chỉ ra ưu điểm vượt trội của MoC so với ToC.

3.1. So sánh quy trình đăng ký và xác thực nhờ công nghệ ToC và MoC

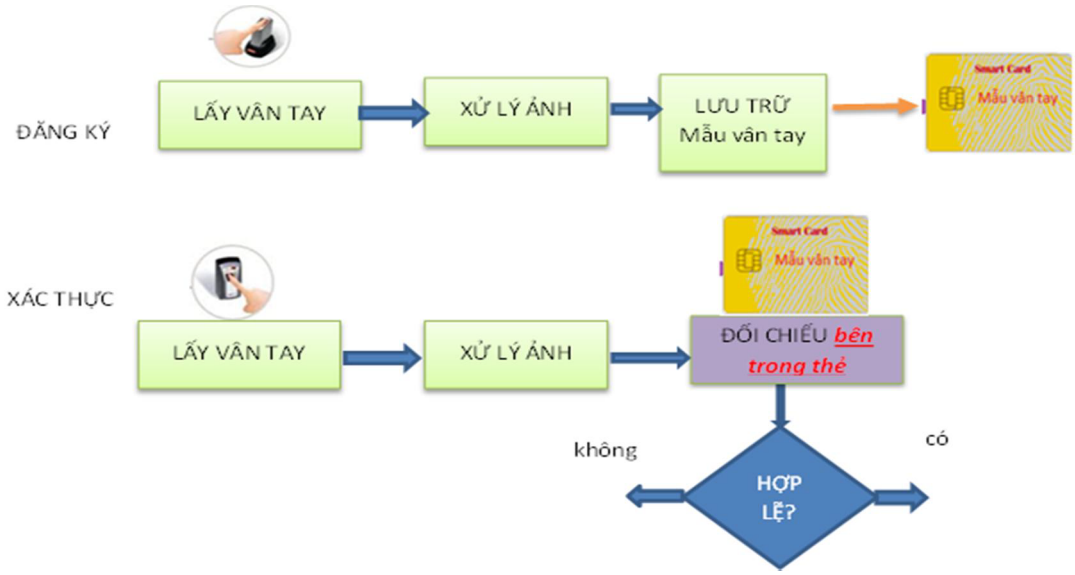
Hình 2 mô tả quy trình đăng ký và xác thực vân tay nhờ công nghệ ToC. Quy trình này khác quy trình trắc sinh học truyền thống trên hình 1 ở chỗ mẫu vân tay được lưu trữ trên thẻ thông minh và việc đối chiếu xác thực được thực hiện trên hệ thống máy tính (ở ngoài thẻ). Ưu điểm của công nghệ ToC là ở chỗ làm tăng tính bảo mật khi mọi thông tin của chủ thẻ được lưu trữ trên chính chiếc thẻ của người đó. Tuy nhiên công nghệ này vẫn tiềm ẩn một số rủi ro về an toàn thông minh liên quan đến truyền tải

Hình 2: Quy trình đăng ký và xác thực mẫu vân tay nhờ phương pháp "đối chiếu ngoài thẻ"



Nguồn: tác giả xây dựng dựa trên mô tả từ các tài liệu của Bălănoiu, 2009; Yau Wei Yun và các cộng sự, không năm xuất bản.

Hình 3: Quy trình đăng ký và xác thực mẫu vân tay nhờ công nghệ MoC



Nguồn: tác giả xây dựng dựa trên mô tả từ các tài liệu của Băläneiu, 2009; Yau Wei Yun và các cộng sự, không năm xuất bản.

mẫu đăng ký từ thẻ thông minh ra hệ thống bên ngoài để đối chiếu các đặc điểm sinh trắc học. Giai đoạn này cần phải có các biện pháp an ninh thích hợp để đảm bảo tính bảo mật và tính toàn vẹn của mẫu được phát hành. Ngoài ra, quá trình xác thực trên hệ thống máy tính có thể không an toàn nếu bị Virus, Spam, Spy… tấn công.

Hình 3 mô tả quy trình đăng ký và xác thực dấu vân tay nhờ công nghệ MoC. Khác với công nghệ ToC, việc lưu trữ mẫu vân tay và đối chiếu được thực hiện ngay bên trong thẻ. Công nghệ này đã khắc phục được nhược điểm của công nghệ ToC nói trên. Do đó mức độ bảo mật của công nghệ MoC cao hơn công nghệ ToC.

Các tác giả *Băläneiu (2009), Smart Card Alliance (2011)* và *Yau Wei Yun và các cộng sự (không năm xuất bản)* đều phân tích và khẳng định rằng công nghệ MoC là giải pháp đáng lựa chọn nhất vì có mức độ bảo mật cao và chi phí có thể chấp nhận được.

3.2. Các lợi ích của việc áp dụng công nghệ MoC trong các hệ thống bảo mật

Smart Card Alliance (2011) đã phân tích bốn lợi ích của việc kết hợp công nghệ trắc sinh học và thẻ thông minh: (1) tăng cường tính riêng tư của người dùng, (2) tăng cường tính bảo mật, (3) tăng cường hiệu suất và tính sẵn sàng của hệ thống và (4) tăng cường tính hiệu quả của hệ thống. *MKGroup (không năm xuất bản c)* đã phân tích sáu lý do nên chọn giải pháp Match on Card TM: (1) tính linh hoạt, (2) hiệu quả về mặt chi phí, (3) khả năng mở rộng, (4) tính sẵn có, (5) Đáng tin cậy và (6) Tính toàn vẹn.

Công nghệ MoC thừa kế các lợi ích của việc kết hợp thẻ thông minh và sinh trắc học nói chung và bổ sung thêm những lợi ích của riêng mình. Có thể tóm tắt các lợi ích khi áp dụng công nghệ MoC trong các hệ thống bảo mật như sau:

- *Giảm bớt các hành động lấy cắp và gian lận trong việc nhận dạng chủ thẻ*: vì các đặc điểm sinh trắc học được lưu trữ trên thẻ và được sử dụng khi xác thực không thể được cho mượn, bị mất hoặc bị mất cắp như mật khẩu và mã PIN,…

- *Tăng cường tính riêng tư của người sử dụng:* Những thông tin cá nhân được lưu trữ trên thẻ được bảo mật cao vì công nghệ thẻ thông minh có thể ngăn chặn việc thay đổi hoặc thay thế các dữ liệu sinh trắc học và ngăn ngừa sự nhân bản thẻ. Các đặc điểm sinh trắc học được lưu trữ trên thẻ thông minh đảm bảo tính cá nhân và tính riêng tư của chủ thẻ và là ràng buộc duy nhất và chặt chẽ giữa chủ thẻ và cơ sở dữ liệu cá nhân trong thẻ giúp xác thực chủ thẻ thực sự. Chủ thẻ có thể kiểm soát được việc ai có quyền truy nhập vào các thông tin lưu trữ trên thẻ.

- *Thuận tiện cho người sử dụng*: chủ thẻ không cần phải nhớ mật khẩu, mã PIN, không phụ thuộc vào cơ sở dữ liệu mẫu sinh trắc học trên hệ thống máy chủ và nhà cung cấp.

- *Tăng cường tính bảo mật, tạo khả năng truy*

xuất nguồn gốc và khả năng kiểm định: việc xác thực dựa trên các thông tin sinh trắc học được lưu trữ trong thẻ với mẫu sinh trắc học sống của chủ thẻ thay cho (hoặc kết hợp với) việc kiểm tra mã PIN đã làm tăng cường sự bảo mật của toàn bộ hệ thống cũng như cải thiện độ chính xác, tốc độ và kiểm soát được việc xác thực chủ thẻ.

- *Tăng cường hiệu suất và khả năng của hệ thống:* nhờ việc chỉ cần một đầu đọc thẻ để lấy mẫu sinh học sống và đối chiếu ngay bên trong thẻ thông minh mà không cần thực hiện việc truy cập, tìm kiếm và đối chiếu với một cơ sở dữ liệu từ xa qua mạng cho phép giảm thời gian xác thực danh tính của một cá nhân chỉ trong một giây (hoặc ít hơn). Nhờ việc xác thực cục bộ này mà việc kiểm tra an ninh được thực hiện nhanh hơn và làm giảm sự cần thiết làm việc trực tuyến với hệ thống trung tâm của đầu đọc thẻ.

- *Có tính linh hoạt:* Với thẻ thông minh MoC, người dùng không bị giới hạn về thẻ, các ứng dụng hay đầu đọc dấu vân tay riêng biệt mà có thể lựa chọn, pha trộn hoặc thay thế chúng sao cho phù hợp với các yêu cầu thay đổi hệ thống, ngân sách và nhu cầu cụ thể.

- *Cải thiện hiệu quả về mặt chi phí của hệ thống:* công nghệ MoC giúp giảm chi phí của hệ thống nhờ tính linh hoạt của mình vì nó cung cấp khả năng thay thế các yếu tố khác nhau trong hệ thống để phù hợp với yêu cầu ngân sách. Người dùng có thể chọn giải pháp tốt nhất phù hợp với nhu cầu của mình.

- *Có khả năng nâng cấp:* Một yêu cầu quan trọng đối với bất kỳ hệ thống nhận dạng và xác thực là khả năng nâng cấp hệ thống mà không cần đầu tư lớn vào cơ sở hạ tầng mới. Thẻ thông minh có thể được cập nhật thêm thông tin sau khi phát hành nếu được phép. Cụ thể là bộ nhớ của thẻ có đủ chỗ để cập nhật thêm hoặc thay thế bằng những mẫu sinh trắc học mới. Các thông số nhận dạng (ID) trên thẻ thông minh có thể được chia thành các phần khác nhau được sử dụng bởi các hệ thống an ninh khác nhau.

- *Có khả năng mở rộng:* Giải pháp MoC được thực hiện và sử dụng trong cả hai loại dự án có quy mô lớn (ví dụ như, trong các chương trình thẻ công dân (ID card) của quốc gia) và quy mô nhỏ (ví dụ như, trong các đề án doanh nghiệp).

3.3. Ứng dụng của công nghệ MoC trong các hệ thống xác thực

Hiện nay, nhiều quốc gia trên thế giới như Mỹ, Thụy Sỹ, Bồ Đào Nha, Canada, Hồng Kông, Thái Lan,… đã áp dụng công nghệ MoC trong nhiều ngành công nghiệp khác nhau để tăng cường an ninh trong các hệ thống xác thực. Sau đây là một số ví dụ về ứng dụng công nghệ này trên thế giới:

- *Thẻ công dân, chứng minh thư:* chính quyền Thái Lan đã lực chọn công nghệ MoC để làm thẻ công dân của họ với các mục tiêu giảm sự giả mạo, gian lận trong việc nhận dạng và xác thực danh tính. Đây là dự án lớn nhất thế giới sử dụng công nghệ này với mục tiêu cung cấp 64 triệu thẻ công dân Thái Lan (Precise Biometrics, 2014).

- *Thẻ nhập cảnh:* Chính phủ Singapore đã thiết lập một hệ thống thông quan tự động nhập cảnh (Immigration Automated Clearance System, viết tắt là IACS) sử dụng thẻ thông minh lưu trữ vân tay tại 25 điểm kiểm tra trên toàn quốc đảo (Smart Card Alliance, 2011).

- *Các thẻ kiểm soát/truy cập*: Các thẻ thông minh kết hợp sinh trắc học đã được sử dụng trong các hệ thống an ninh ở 29 sân bay Canada vào năm 2004; trong các hệ thống kiểm soát an ninh tại sân bay Schiphol ở Amsterdam, Hà Lan vào năm 2006; trong các hệ thống an ninh và truy cập không cần khóa tại Đại học Arizona đặt tại Tucson, Arizona, Hoa Kỳ; trong hệ thống kiểm soát an ninh sử dụng thẻ nhận dạng cá nhân (Personal Identity Verification (PIV) Card) FIPS 201 của Mỹ và hệ thống truy cập tại Bộ quốc phòng Mỹ (Smart Card Alliance, 2011).

- *Hộ chiếu điện tử:* tại Mỹ và nhiều nước khác, thẻ thông minh kết hợp với sinh trắc học được sử dụng làm hộ chiếu điện tử (ePassports). Một số nước đã và đang có kế hoạch sử dụng hộ chiếu điện tử là: Mỹ, Úc, Bosnia and Herzegovina, Brunei, Canada, Croatia, Cộng hòa Dominica, Iran, Iraq, Malaysia, Moldova, Montenegro, Morocco, New Zealand, Nigeria, Singapore, Thụy Sĩ, Tajikistan, Thái Lan, Thổ Nhĩ Kỳ, Turkmenistan, và Venezuela (Smart Card Alliance, 2011).

Ở Việt Nam, công nghệ MoC bắt đầu được các tổ chức, doanh nghiệp quan tâm trong những năm gần đây. Từ năm 2010 Công ty Cổ phần Thông minh MKsmart đi tiên phong đang đẩy mạnh ứng dụng công nghệ MoC không chỉ với vân tay mà cả với các thông số sinh trắc học khác như mống mắt, mạch máu lòng bàn tay, DNA… trong các thẻ Ngân hàng, thẻ BHYT/BHXH, thẻ ID… không chỉ ở Việt Nam, mà cả các nước trong khu vực và trên toàn thế giới

(MKGroup, không năm xuất bản a,b).

3.4. Một số kiến nghị khi áp dụng công nghệ MoC trong các hệ thống xác thực

Như trên đã tổng hợp và phân tích, công nghệ MoC được khuyến cáo nên sử dụng trong các hệ thống bảo mật, đặc biệt là trong các hệ thống xác thực danh tính của con người do mức độ bảo mật cao và chi phí hợp lý. Công nghệ này đã được nhiều nước trên thế giới áp dụng và đã mang lại nhiều lợi ích kinh tế và xã hội. Tuy nhiên, việc lựa chọn công nghệ chỉ là một trong các yếu tố để thực hiện thành công một hệ thống. Trong thực tế, để áp dụng công nghệ này thành công trong các hệ thống xác thực cần phải lưu ý những điểm sau:

3.4.1. Sự quyết tâm của các nhà lãnh đạo

Đây là một trong những nhân tố quan trọng nhất của việc xây dựng thành công một hệ thống thông tin nói chung và hệ thống xác thực nói riêng. Công nghệ mới luôn cần các nhà lãnh đạo nhìn nhận rõ lợi ích và thấu hiểu mọi khó khăn có thể xảy ra trong quá trình triển khai quyết tâm áp dụng thực tế vào đơn vị mình quản lý. MoC là công nghệ mới hiện đại tiên phong thay đổi cách thức LƯU TRỮ và XỬ LÝ SỐ LIỆU SINH TRẮC HỌC BÊN TRONG THẺ THÔNG MINH AN TOÀN GẦN NHƯ TUYỆT ĐỐI không theo lối mòn truyền thống lưu trữ trong cơ sở dữ liệu trên máy tính cá nhân hay máy chủ có thể dễ bị lấy trộm. Nếu Hacker muốn lấy số liệu sinh trắc học này thì phải "chui" được vào bên trong con chip, đó là việc cực kỳ khó khăn. MoC còn thay đổi cả lối suy nghĩ sáo mòn kinh điển cứ phải lo đầu tư tốn kém rất nhiều tiền bạc và thời gian để xây dựng xong kho dữ liệu sinh trắc học xong mới thực hiện các bài toán xử lý, nó không cần cơ sở dữ liệu mà lưu trữ số liệu sinh trắc học ngay vào bên trong thẻ thông minh. Nếu cần lưu trữ lại số liệu sinh trắc học vào kho dữ liệu chung thì vẫn có thể thực hiện đồng thời khi lấy mẫu để lưu vào thẻ thông minh. Vì vậy, sự quyết tâm của các nhà lãnh đạo càng đặc biệt quan trọng khi áp dụng MoC.

3.4.2. Năng lực và chi phí hợp lý của toàn bộ hệ thống

Như đã trình bày ở trên, mức độ bảo mật MoC cao hơn ToC nhưng không bằng SoC, tuy nhiên chi phí chấp nhận được. Trong thực tế tùy vào yêu cầu bảo mật cụ thể với chi phí phù hợp với hệ thống có sẵn đang hoạt động và khả năng nâng cấp tương lai có thể tích hợp MoC với các công nghệ bảo mật khác như OTP (One-Time-Password), PKI (Public Key Infrastructure)… tạo ra hệ thống xác thực mạnh đa nhân tố an toàn và hiệu quả hơn rất nhiều. Ví dụ, ngân hàng có thể chỉ yêu cầu khách hàng dùng OTP để xem số dư và chuyển khoản trực tuyến trên mạng dưới 10 triệu đồng, nhưng với số tiền trên 500 triệu đồng thì phải dùng MoC hoặc PKI…

3.4.3. Các vấn đề về văn hóa và sự chấp nhận của người dùng

Việc thay đổi nhận thức và thói quen của người dùng khó khăn hơn việc thay đổi công nghệ, nên cần phải đào tạo để người sử dụng hiểu được ích lợi, chấp nhận và sử dụng được hệ thống mới. Ví dụ như, nhiều người về hưu rất ngại nhận lương hưu qua thẻ vì phải nhớ số PIN khi rút tiền qua cây ATM, khi này MoC thay thế số PIN sẽ rất tiện cho họ. Sử dụng công nghệ MoC phải phù hợp quy trình xác thực trong các hệ thống giao dịch. Việc lưu trữ vân tay của cả Giám đốc và Kế toán trưởng trên cùng 1 thẻ MoC chỉ cho phép thực hiện được những bút toán quan trọng khi có mặt cả 2 người. Nếu thiếu vân tay của một trong hai người thì thẻ MoC cũng không hoạt động vì bắt buộc phải là vân tay sống trên cơ thể của họ. Còn nhiều ví dụ khác để thấy rằng nắm rõ thói quen môi trường làm việc sinh hoạt của người dùng mới có thể tự nhiên sử dụng công nghệ MoC hàng ngày và lâu dài.

4. Kết luận

Như đã phân tích, việc sử dụng thẻ thông minh với kết quả sinh trắc học nói chung và công nghệ MoC tăng cường khả năng bảo mật trong các hệ thống an ninh với các ưu điểm nổi bật như đã trình bày ở trên về tính bảo mật, tính riêng biệt và duy nhất, tốc độ đối chiếu/so sánh (Matching) nhanh, không cần cơ sở dữ liệu trung tâm, tương thích với cách thức xác minh PIN và giá thành thấp. Công nghệ này sẽ giúp tối ưu hóa bảo mật, đảm bảo sự linh hoạt, tiết kiệm và giúp loại trừ rủi ro giả mạo, tiết kiệm chi phí và đã được nhiều quốc gia, tổ chức áp dụng trong thực tế.

Trong khuôn khổ bài báo này, tác giả tổng hợp và phân tích các ưu điểm về tính bảo mật cũng như chi phí hợp lý của công nghệ MoC và những điểm cần lưu ý khi các tổ chức muốn áp dụng công nghệ này trong các hệ thống bảo mật của mình. Các tổ chức quan tâm đến công nghệ này cần đi sâu tìm hiểu, phân tích để tìm ra giải pháp tối ưu ứng dụng trong hoàn cảnh cụ thể của mình.❐

Tài liệu tham khảo

Bălănoiu, P. (2009), 'Enhancing Privacy for Biometric Identification Cards', *Informatica Economica*, Tập 13 số 1, trang 100-107.

Gobi, M và Kannan, D. (2014), 'A Secured Public Key Cryptosystem for Biometric Encryption', *International Journal of Computer Science and Information Technologies*, Tập 5 số 1, trang 184-191.

Jaracz, Jill (2013), *Tech 101: Match-on-card biometrics, Use grows rapidly for this privacy-protecting technology*, truy cập ngày 28 tháng 7 năm 2014, từ <http://secureidnews.com/news-item/tech-101-match-on-card-biometrics>.

Henry, M. (2007), *Multi-application Smart Cards- Technology and Applications,* Cambridge University Press. Cambridge.

Maltoni, D., Maio, D., Jain, A. vaf Prabhakar, S. (2003). *Handbook of fingerprint recognition*. Springer. NewYork.

Minh Long (2011), *4 công nghệ sẽ thay đổi cuộc sống*, truy cập ngày 28 tháng 7 năm 2014, từ <http://vnexpress.net/tin-tuc/khoa-hoc/4-cong-nghe-se-thay-doi-cuoc-song-2213994.html>.

MKGroup (không năm xuất bản a), *Giải pháp xác thực nhân thân sinh trắc học trên thẻ thông minh MoC*, truy cập ngày 15 tháng 8 năm 2014, từ <http://mk.com.vn/home/?act=sanpham_chitiet&muc=45&sub=71&sanpham=146.>

MKGroup (không năm xuất bản b), *Ứng dụng của giải pháp Match-on-Card*, truy cập ngày 15 tháng 8 năm 2014, từ <http://mk.com.vn/home/?act=sanpham_chitiet&muc=45&sub=71&sanpham=148>

MKGroup (không năm xuất bản c), *Những lý do nên chọn giải pháp Match-on-CardTM của MK Group*, truy cập ngày 15 tháng 8 năm 2014, từ < http://mk.com.vn/home/?act=sanpham_chitiet&muc=45&sub=71&sanpham=147>

Moon, Daesung, Chung, Yongwha, Seo, Changho, Kim, Sung-Young và Kim, Jeong-Nyeo (2014), 'A practical implementation of fuzzy fingerprint vault for smart cards', *Journal of Intelligent Manufacturing*, Tập 25 số 2, trang 293-302.

Požgaj, Ž. và Đurinek, I. (2007), *Smart Card in Biometric Authentication*, in Proc. of Information and Intelligent Systems, Faculty of Organization and Informatics, University of Zagreb, Varaždin. Zagreb.

Precise Biometrics (2014), *Case study*, truy cập ngày 29 tháng 01 năm 2015, từ <http://precisebiometrics.com/wp-content/uploads/2014/11/case-study-match-on-card-thailand.pdf>

Smart Card Alliance (2011), *Smart Cards and Biometrics*, truy cập ngày 15 tháng 8 năm 2014, từ <http://www.smartcardalliance.org/resources/pdf/SmartCards_and Biometrics_030111.pdf>

Terry, Lisa (2002), *Smart Money: Biometric Cards Promise Speedy E-commerce and Secure Identiffication,* Supply Chain Systems Magazine, May 2002, <http://www.scs-mag.com/reader/2002/2002_05/>.

Yau Wei Yun và Chen Tai Pang, Lawrence (không năm xuất bản), *Section Three: An Introduction to Biometric Match – On- Card*, truy cập ngày 29 tháng 8 năm 2014, từ <http://www.e-xpertsolutions.com/images/pdf/moc/3_BiometricMOC.pdf>.

Thông tin tác giả:

**** Trần Thị Thu Hà,** Tiến sỹ*

- Tổ chức tác giả công tác: Khoa Tin học Kinh tế, trường Đại học Kinh tế quốc dân

- Lĩnh vực nghiên cứu chính: Tin học Kinh tế, Hệ thống thông tin quản lý

- Tạp chí đã từng đăng tải các nghiên cứu: Tạp chí Kinh tế và phát triển

- Địa chỉ liên hệ: Địa chỉ Email hatt@neu.edu.vn,