(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **1-0026635**

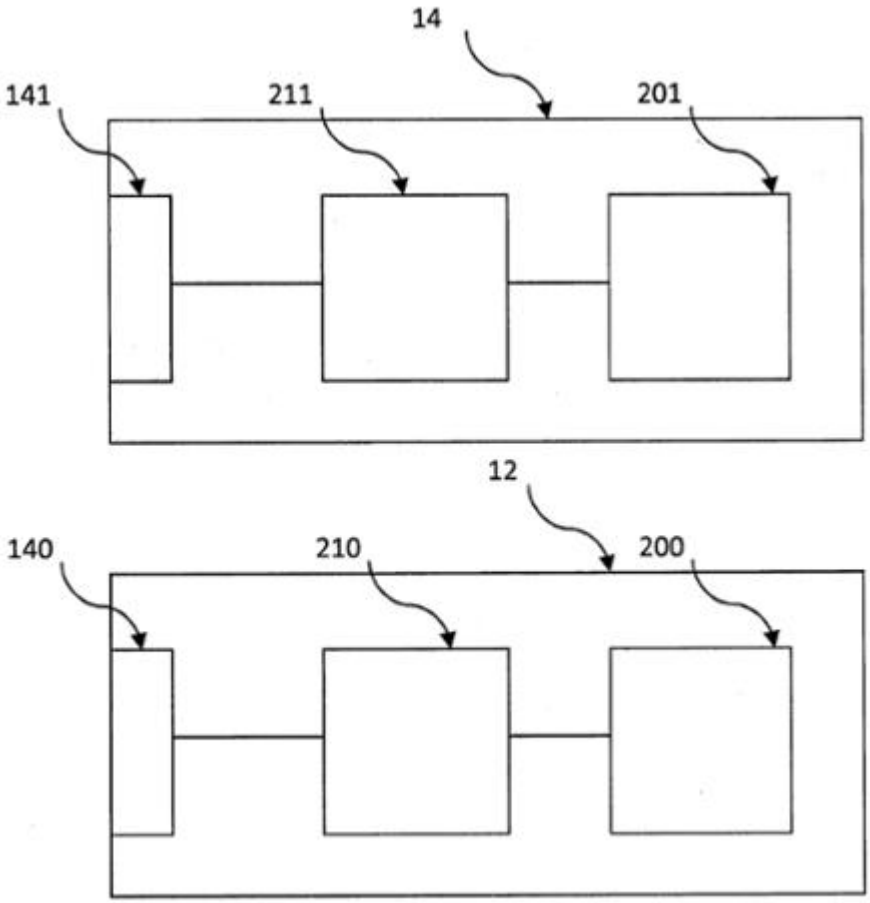
(51)[7] **H04L 29/06**; G06F 21/34; H04L 9/32; H04L 29/14; H04L 9/08; G06F 21/31

(13) **B**

(21) 1-2015-04750
(22) 16/05/2014
(86) PCT/SG2014/000215 16/05/2014
(87) WO 2014/185865 20/11/2014
(30) 201303827-8 16/05/2013 SG
(45) 25/12/2020 393
(43) 25/02/2016 335A
(73) FAST AND SAFE TECHNOLOGY PRIVATE LIMITED (SG)
9 Temasek Boulevard, #09-01, Suntec Tower Two, Singapore 038989, Singapore
(72) HSU, Hsiang Ke Desmond (SG).
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) THIẾT BỊ VÀ PHƯƠNG PHÁP TỰ XÁC THỰC

(57) Sáng chế đề cập đến thiết bị và phương pháp tự xác thực. Thiết bị tự xác thực này dùng cho người dùng hoặc chủ sở hữu của thiết bị bảo mật điện tử, trong đó thiết bị tự xác thực tách biệt khỏi thiết bị bảo mật và được cấu hình để nối với thiết bị tính toán qua liên kết truyền thông thứ nhất để xử lý tự xác thực, tốt hơn là để xử lý xác thực và phục hồi.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến hệ thống, thiết bị và phương pháp trong lĩnh vực bảo mật công nghệ thông tin (Information Technology - IT) và bảo mật điện tử.

Tình trạng kỹ thuật của sáng chế

Trong phạm vi bảo mật IT, nhiều thiết bị người dùng cuối, bao gồm máy tính để bàn, máy tính bảng, điện thoại thông minh, máy tính xách tay, ổ đĩa cứng di động, bộ nhớ chớp bus tuần tự đa năng (USB flash) và các thiết bị di động khác, cũng như các máy chủ, xử lý và trao đổi lượng thông tin lớn trong các môi trường có dây cũng như không dây. Một số thông tin này có độ nhạy cảm cao như thông tin cá nhân riêng tư và thông tin công ty gây hại. Thông tin có thể có lợi cho người dùng hoặc tổ chức cũng có thể được sử dụng để chống lại người dùng hoặc tổ chức này nếu thông tin này rơi vào tay của người không phải chủ sở hữu. Các nhân viên tình báo công nghiệp trong những ngành kinh doanh cạnh tranh cao đang sử dụng đến các thiết bị điện tử để lấy cắp thông tin tập thể.

Mã hóa là giải pháp thông dụng nhất để mang lại độ bảo mật của dữ liệu. Hầu hết các sản phẩm phần mềm mã hóa dữ liệu cài đặt và lưu khóa mã hóa được sử dụng để mã hóa, bảo vệ các dữ liệu bên trong chính thiết bị mà các dữ liệu được lưu. Nếu thiết bị bị mất hoặc bị bẻ khóa, thì cả các dữ liệu được mã hóa cũng như khóa mã hóa đều rơi vào tay cùng một người và do đó sự bảo mật của các dữ liệu bị ảnh hưởng.

Việc sử dụng thẻ di động ngoài được tách biệt về mặt cơ học với thiết bị lưu các dữ liệu, để lưu khóa mã hóa để mã hóa và truy cập các dữ liệu được bảo mật, chẳng hạn là từ đĩa bảo mật ảo, được gọi là biện pháp ưu tiên để bảo mật các dữ liệu nhạy cảm trên máy tính chủ khi nó có thể tách khóa mã hóa ra khỏi các dữ liệu được mã hóa. Liên kết truyền thông giữa thẻ và máy tính chủ có thể là qua mô đun hoặc phương tiện truyền thông bất kỳ như các kênh tần số vô tuyến (RF) (RF - Radio Frequency) hoặc các kết nối có dây. Thẻ di động ngoài có thể là thiết bị ngoại vi bất kỳ như là bộ nhớ USB flash, điện thoại di động hoặc thậm chí là một máy tính khác. Máy tính chủ có thể là máy tính bất kỳ như máy chủ, máy tính để bàn, máy tính di động hoặc các điện thoại thông minh.

Máy tính chủ có thể chứa trình quản lý bảo mật dữ liệu (DSM) (DSM - Data Security Manager).

Cơ chế bảo vệ mật khẩu được kết hợp cùng với thẻ để ngăn chặn việc sử dụng trái phép thẻ. Ví dụ, người dùng đòi hỏi truy cập các dữ liệu bảo mật được nhắc cắm thẻ của mình và đánh mật khẩu của mình vào. Mức độ chính xác của mật khẩu được kiểm tra. Nếu mật khẩu là chính xác, thẻ (và vì vậy là người dùng) được cho phép truy cập các dữ liệu bảo mật. Người dùng được cho phép truy cập vào các dữ liệu bảo mật chỉ khi thẻ được cắm vào và mật khẩu đăng nhập là chính xác. Các dữ liệu được mã hóa bằng cách sử dụng chẳng hạn là thuật toán mã hóa khóa đối xứng.

Trong khi biện pháp nêu trên có thể bảo mật dữ liệu nhạy cảm trên máy tính chủ, vấn đề tồn tại là người dùng bán lẻ trong môi trường tiêu dùng có thể quên mật khẩu được liên kết với thẻ di động của mình. Trong khi mật khẩu thường có thể được tái thiết lập bởi nhà sản xuất thẻ di động, biện pháp này không đưa ra giải pháp thỏa mãn vì bất kỳ lúc nào bên thứ hai tham gia quy trình bảo mật bất kỳ, thì khả năng dò rỉ bảo mật trở nên thực tế. Các vấn đề tương tự cũng tồn tại khi thẻ bị hư hại, bị mất hoặc bị đánh cắp.

Các phương án theo sáng chế nhằm đề xuất hệ thống, thiết bị và phương pháp tự xác thực, tốt hơn là hệ thống, thiết bị và phương pháp tự xác thực và phục hồi cho phép người dùng hoặc chủ sở hữu các dữ liệu tự giúp chính mình khi các vấn đề này xuất hiện mà không cần người khác tham gia.

Bản chất kỹ thuật của sáng chế

Theo khía cạnh thứ nhất, sáng chế đề xuất thiết bị tự xác thực dùng cho người dùng hoặc chủ sở hữu của thiết bị bảo mật điện tử, trong đó thiết bị tự xác thực được tách rời khỏi thiết bị bảo mật và được cấu hình để nối với thiết bị tính toán thông qua liên kết truyền thông thứ nhất để xử lý tự xác thực, tốt hơn là để xử lý tự xác thực và phục hồi.

Theo khía cạnh thứ hai, sáng chế đề xuất phương pháp tự xác thực đối với người dùng hoặc chủ sở hữu của thiết bị bảo mật điện tử, phương pháp này bao gồm bước nối thiết bị tự xác thực tách rời khỏi thiết bị bảo mật với thiết bị tính toán qua liên kết truyền

thông thứ nhất để xử lý tự xác thực, tốt hơn là để xử lý tự xác thực và quá trình phục hồi.

Mô tả vắn tắt các hình vẽ

Các phương án của sáng chế sẽ được hiểu rõ hơn và rõ ràng đối với người có hiểu biết trung bình trong lĩnh vực kỹ thuật tương ứng nhờ phần mô tả bằng văn bản dưới đây, chỉ bằng cách nêu ví dụ, và có dựa vào các hình vẽ kèm theo, trong đó:

Fig.1a) là hình vẽ sơ đồ giản lược thể hiện cụm thiết bị để tạo ra và truy cập đĩa ảo bảo mật theo một phương án thực hiện làm ví dụ;

Fig.1b) là hình vẽ sơ đồ giản lược thể hiện máy tính chủ giao tiếp với thẻ di động ngoài của cụm thiết bị được thể hiện trên Fig.1a theo một phương án thực hiện làm ví dụ;

Fig.2 là hình vẽ sơ đồ giản lược thể hiện cấu hình của thẻ di động ngoài của cụm thiết bị được thể hiện trên Fig.1a theo một phương án thực hiện làm ví dụ;

Fig.3a) là hình vẽ sơ đồ giản lược thể hiện việc xử lý xác thực để tái thiết lập mật khẩu thẻ theo một phương án thực hiện làm ví dụ;

Fig.3b) là hình vẽ lưu đồ thể hiện việc xử lý xác thực để tái thiết lập mật khẩu thẻ theo một phương án thực hiện làm ví dụ;

Fig.4a) là hình vẽ sơ đồ giản lược thể hiện việc xử lý xác thực để tạo ra thẻ phó bản để thay thế thẻ bị mất, bị hư hại hoặc bị đánh cắp theo một phương án thực hiện làm ví dụ;

Fig.4b) là hình vẽ lưu đồ thể hiện việc xử lý xác thực để tạo ra thẻ phó bản để thay thế thẻ bị mất, bị hư hại hoặc bị đánh cắp theo một phương án thực hiện làm ví dụ;

Fig.5a) là hình vẽ sơ đồ giản lược thể hiện sự truy cập tái mã hóa vào các tập tin dữ liệu bảo mật theo một phương án thực hiện làm ví dụ;

Fig.5b) là hình vẽ lưu đồ thể hiện sự truy cập tái mã hóa vào các tập tin dữ liệu bảo mật theo một phương án thực hiện làm ví dụ; và

Fig.6 là hình vẽ sơ đồ giản lược thể hiện sự truy cập chỉ đọc vào đĩa ảo bảo mật theo một phương án thực hiện làm ví dụ.

Mô tả chi tiết sáng chế

Một số phần của phần mô tả sau đây được thể hiện rõ ràng hoặc hoàn toàn dưới dạng các thuật toán và các phép biểu diễn dưới dạng hàm hoặc ký hiệu của các phép toán đối với các dữ liệu trong bộ nhớ máy tính. Các phần mô tả thuật toán và các phép biểu diễn dưới dạng hàm hoặc ký hiệu này là phương tiện được sử dụng bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật máy tính để truyền tải một cách hữu hiệu nhất bản chất công việc của mình cho người có hiểu biết trung bình trong lĩnh vực kỹ thuật tương ứng khác. Ở đây, thuật toán và thường được hiểu là thứ tự nhất quán của các bước dẫn đến kết quả mong muốn. Các bước này là các bước đòi hỏi các xử lý về mặt vật lý của các đại lượng vật lý như là các tín hiệu điện, từ trường hoặc quang học có khả năng được lưu, được truyền, được kết hợp, được so sánh và mặt khác, được xử lý.

Trừ khi được nêu một cách cụ thể khác đi và như rõ ràng từ phần sau đây, điều sẽ được hiểu là, trong toàn bộ bản mô tả này, các phần mô tả sử dụng các thuật ngữ như là "quét", "tính toán", "xác định", "thay thế", "tạo ra", "khởi tạo", "kết xuất" hoặc dạng tương tự, chỉ hoạt động và các quá trình của hệ thống máy tính hoặc thiết bị điện tử tương tự mà xử lý và biến đổi các dữ liệu được biểu diễn dưới dạng các đại lượng vật lý trong hệ thống máy tính thành các dữ liệu khác được biểu thị một cách tương tự như là các đại lượng vật lý trong hệ thống máy tính hoặc các thiết bị lưu, truyền hoặc hiển thị thông tin khác.

Bản mô tả này còn mô tả thiết bị thực hiện các hoạt động theo các phương pháp này. Thiết bị này có thể được cấu hình một cách cụ thể với các mục đích theo yêu cầu hoặc có thể bao gồm máy tính đa năng hoặc thiết bị khác được kích hoạt hoặc được tái cấu hình theo cách có lựa chọn nhờ chương trình máy tính được lưu trong máy tính. Các thuật toán và các phần hiển thị được thể hiện ở đây vốn không liên quan đến máy tính hoặc thiết bị cụ thể bất kỳ khác. Các máy đa năng khác nhau có thể được sử dụng với các chương trình theo các nội dung ở đây. Theo cách khác, cấu hình của thiết bị chuyên dụng hơn tiến hành các bước của phương pháp có thể là thích hợp. Cấu trúc máy tính đa năng thông thường sẽ xuất hiện từ phần mô tả dưới đây.

Hơn nữa, bản mô tả này còn bộc lộ một cách hoàn toàn thuật toán của chương trình máy tính, trong đó điều sẽ trở nên rõ ràng đối với người có hiểu biết trung bình trong lĩnh vực kỹ thuật tương ứng là các bước riêng lẻ của phương pháp được mô tả ở đây có thể được đưa vào áp dụng nhờ mã máy tính. Chương trình máy tính không nhằm bị hạn chế ở ngôn ngữ lập trình cụ thể bất kỳ và cách thực hiện chương trình này. Điều được hiểu là, các ngôn ngữ lập trình khác nhau và việc mã hóa của chúng có thể được sử dụng để thực hiện các nội dung của sáng chế được chứa đựng ở đây. Hơn nữa, chương trình máy tính không nhằm bị hạn chế ở dòng điều khiển cụ thể bất kỳ. Có nhiều biến thể khác của chương trình máy tính có thể sử dụng các dòng điều khiển khác nhau mà không nằm ngoài phạm vi bảo hộ của sáng chế.

Tiếp theo nữa, một hoặc nhiều bước của chương trình máy tính có thể được thực hiện song song hơn là tuần tự. Chương trình máy tính này có thể được lưu trên vật ghi đọc được bằng máy tính bất kỳ. Vật ghi đọc được bằng máy tính này có thể bao gồm các thiết bị lưu như các đĩa từ trường hoặc các đĩa quang, các chip nhớ các thiết bị lưu khác thích hợp để giao tiếp với máy tính đa năng. Vật ghi đọc được bằng máy tính này cũng có thể bao gồm phương tiện có dây vật lý như được nêu làm ví dụ trong hệ thống internet hoặc phương tiện không dây (chẳng hạn thiết bị wi-fi, thiết bị bluetooth và hệ thống điện thoại viễn thông di động). Chương trình máy tính khi được nạp và được thực hiện trên máy tính đa năng một cách hữu hiệu dẫn đến thiết bị thực hiện các bước của phương pháp được ưu tiên.

Sáng chế còn có thể được thực hiện dưới dạng các mô đun phần cứng. Cụ thể hơn, về mặt phần cứng, mô đun là khối phần cứng chức năng nhằm để sử dụng với các thành phần hoặc các mô đun khác. Chẳng hạn, mô đun có thể được thực hiện bằng cách sử dụng các thành phần điện tử rời rạc hoặc nó có thể tạo thành một phần của toàn bộ mạch điện tử như là mạch tích hợp chuyên dụng (ASIC - Application Specific Integrated Circuit). Nhiều khả năng khác có thể tồn tại. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật tương ứng sẽ hiểu là hệ thống cũng có thể được thực hiện dưới dạng kết hợp của các mô đun phần cứng và phần mềm.

Mô tả chung hệ thống mã hóa làm ví dụ với thẻ xác thực

Fig.1a) là hình vẽ thể hiện cụm 10 để sử dụng trong mã hóa và truy cập các dữ liệu bảo mật, chẳng hạn trên đĩa bảo mật ảo, theo một phương án thực hiện làm ví dụ. Cụm 10 bao gồm thẻ di động 12 để nối với máy tính chủ qua liên kết truyền thông thứ nhất để mã hóa và truy cập các dữ liệu bảo mật trên máy tính chủ, và thiết bị xác thực di động 14 được liên kết với thẻ 12. Thiết bị xác thực 14 được cấu hình để nối với thiết bị tính toán qua liên kết truyền thông thứ hai để xử lý tự xác thực và phục hồi.

Fig.1b) là hình vẽ thể hiện sơ đồ khối mức cao của máy tính chủ 100 được nối với thẻ di động 12 sử dụng liên kết truyền thông 120, theo một phương án thực hiện làm ví dụ. Liên kết truyền thông 120 thể hiện môi trường mà qua đó dữ liệu được truyền thông giữa thẻ di động 12 và máy tính chủ 100 qua giao diện của thẻ 140 và giao diện của máy tính 130. Liên kết truyền thông bao gồm, nhưng không giới hạn ở, mô đun hoặc phương tiện truyền thông bất kỳ như là các kênh tần số vô tuyến (RF) hoặc các kết nối có dây. Thẻ di động 12 có thể là thiết bị ngoại vi bất kỳ như là bộ nhớ USB flash, điện thoại di động hoặc thậm chí là một máy tính khác. Máy tính chủ 100 có thể là máy tính bất kỳ như là máy chủ, máy tính để bàn, điện thoại thông minh, máy tính cỡ sổ tay hoặc máy tính di động. Máy tính chủ chứa trình quản lý bảo mật dữ liệu (DSM) 150, có thể được cài đặt tách riêng, ví dụ từ CD-ROM hoặc có thể được cài đặt từ thẻ 12 hoặc qua internet.

Fig.2 là hình vẽ sơ đồ khối ở mức cao thể hiện một số thành phần quan trọng bên trong thẻ di động 12 và thiết bị xác thực 14 theo một phương án thực hiện làm ví dụ. Từng thành phần trong số thẻ 12 và thiết bị xác thực 14 lần lượt chứa bộ nhớ bất khả biến ghi lại được 200, 201, bộ điều khiển nhúng (EC) 210, 211 và giao diện 140, 141 với máy tính.

Bộ nhớ bất khả biến 200 chứa các mục dữ liệu như mật khẩu, trị số đếm và khóa thẻ và khóa nhóm thẻ. Mật khẩu được sử dụng để điều khiển truy cập của người dùng vào thẻ 12. Trị số đếm có thể là số nguyên dương nhỏ được sử dụng để kiểm soát số lần nhập lại mật khẩu thất bại liên tiếp. Theo một phương án, khóa thẻ là khóa bí mật ngẫu nhiên được sử dụng để mã hóa và giải mã tệp tin trong điều kiện thuật toán mã hóa khóa đối xứng. Khóa nhóm thẻ là khóa bí mật ngẫu nhiên được sử dụng cho khóa thẻ hoặc

mã hóa và giải mã khóa xác thực. Bộ nhớ bất khả biến 201 chứa các mục dữ liệu như là khóa xác thực.

Quay trở lại Fig.1b), trước khi thẻ được sử dụng trên hệ thống máy tính, DSM 150 cần phải được cài đặt và thẻ 12 cần được khởi tạo. Thẻ 12 được nối với máy tính 100 và mật khẩu người dùng dùng cho thẻ 12 được nhập vào. Khóa thẻ sau đó được tạo ra. Theo cách khác khóa thẻ có thể được cài đặt trước ở nhà máy.

Các khóa trùng khớp

Thiết bị xác thực 14 (Fig.1a)) có khóa xác thực trùng khớp đơn nhất với khóa thẻ. Theo một phương án, "trùng khớp" nghĩa là “bằng”, nhưng lưu ý rằng, trong các phương án khác nhau "trùng khớp" có thể bao gồm một khóa có thể được so khớp với khoá khác bằng cách sử dụng chẳng hạn thuật toán biến đổi khóa này thành khóa khác. Khóa xác thực đơn nhất đối với thiết bị xác thực 14 có thể được lưu trước trong thiết bị xác thực 14 trong quá trình sản xuất hoặc có thể được tạo ra và được lưu trong quá trình cài đặt bởi người sử dụng.

Ví dụ: So khớp sử dụng các bộ định danh đơn nhất riêng biệt.

Sự liên kết hoặc so cặp thẻ 12 và thiết bị xác thực kết hợp 14 có thể được thực hiện bằng cách sử dụng bộ định danh đơn nhất trong thẻ 12 và trong thiết bị xác thực 14 tương ứng. Cặp bộ định danh đơn nhất này có thể "bằng", nhưng theo cách khác, có thể được cấu hình sao cho bộ định danh đơn nhất này có thể được so khớp với bộ định danh đơn nhất khác bằng cách sử dụng thuật toán biến đổi bộ định danh đơn nhất này thành bộ định danh đơn nhất khác, chẳng hạn. Cặp bộ định danh đơn nhất có thể được lưu trước trong quá trình sản xuất hoặc có thể được tạo ra và được lưu trong quá trình cài đặt bởi người sử dụng.

Theo các phương án thực hiện làm ví dụ, liên kết giữa thẻ 12 và thiết bị xác thực 14 là đơn nhất, tức là chỉ liên kết một - một giữa một thẻ và một thiết bị xác thực 14 được tạo ra.

Ví dụ: So khớp sử dụng các bộ định danh quan hệ nhiều-một

Theo phương án thực hiện làm ví dụ khác, liên kết giữa thẻ 12 và thiết bị xác thực 14 là liên kết nhiều-một giữa nhiều thẻ 12 và một thiết bị xác thực 14.

Kiểm soát truy cập

DSM 150 tiến hành điều khiển truy cập đối với các dữ liệu bảo mật ví dụ là trên đĩa bảo mật ảo trên cơ sở bốn trường hợp sau đây: đưa thẻ vào, lấy thẻ ra, người sử dụng đăng nhập và người sử dụng đăng xuất. Người dùng được cho phép truy cập vào các dữ liệu bảo mật chỉ khi thẻ 12 được đưa vào và mật khẩu đăng nhập là chính xác. Nếu không thì, các dữ liệu bảo mật không truy cập được. Trong quá trình người sử dụng truy cập vào các dữ liệu bảo mật, DSM 150 luôn phát hiện liệu thẻ 12 có mặt hay không. Nếu DSM 150 phát hiện ra rằng, thẻ 12 được tháo ra khỏi máy tính chủ, thì người dùng lập tức bị từ chối truy cập vào các dữ liệu bảo mật. Khả năng truy cập chỉ được phục hồi khi cắm thẻ 12 vào và người sử dụng đăng nhập thành công.

Các dữ liệu được mã hóa sử dụng thuật toán mã hóa khóa đối xứng trong một phương án thực hiện làm ví dụ.

Tái thiết lập mật khẩu

Trong phần tiếp theo, sẽ mô tả cách thiết bị xác thực 14 có thể được sử dụng một cách có lợi để xử lý tự xác thực trước khi tái thiết lập mật khẩu đối với thẻ 12, chẳng hạn để lấy lại quyền truy cập hoàn toàn vào các dữ liệu bảo mật nếu người dùng quên mật khẩu ban đầu, trong kịch bản thứ nhất.

Fig.3a) là hình vẽ thể hiện việc xử lý xác thực sử dụng thẻ 12 và thiết bị xác thực 14. Theo một ví dụ, người dùng đưa thẻ 12 cùng với thiết bị xác thực 14 vào máy tính 300 ở chẳng hạn trung tâm dịch vụ, trạm sản xuất, giao diện trang internet của nhà sản xuất hoặc đại lý ủy quyền. Máy tính 300 này cũng có thể là máy tính chủ của người dùng. Thiết bị xác thực 14 và thẻ 12 được nối với máy tính 300 qua các liên kết truyền thông tương ứng 304, 302. Thẻ 12 và thiết bị xác thực 14 có thể được nối đồng thời với máy tính 300 hoặc có thể được nối tuần tự chẳng hạn khi chỉ một giao diện truyền thông để nối với máy tính 300 là có thể sử dụng được. Trình quản lý xác thực 306 (Authentication Manager- AM) đang chạy trên máy tính 300.

Ví dụ: Bước so khớp trước khi tái thiết lập mật khẩu

Như được thể hiện trên Fig.3b), người dùng yêu cầu "tái thiết lập mật khẩu" ở bước 350, chẳng hạn từ danh mục trình đơn được thể hiện trên màn hình máy tính dưới

sự điều khiển của AM 306 chạy trên máy tính 300, đáp lại việc cắm thẻ 12 và thiết bị xác thực 14 vào. Khi xác nhận yêu cầu, thiết bị xác thực 14 mã hóa khóa xác thực của nó ở bước 352 và gửi khóa xác thực được mã hóa vào thẻ 12, chẳng hạn qua AM 306 ở bước 354. Các phương pháp như là mật hóa khóa bí mật hoặc các phương pháp thích hợp khác có thể được sử dụng theo các phương án thực hiện làm ví dụ. Do đó, lưu ý rằng, theo cách có lợi, AM 306 theo phương án thực hiện làm ví dụ này không thể "thấy được" khóa xác thực thực tế.

Ở bước 356, thẻ 12 sau đó giải mã khóa xác thực được mã hóa được tiếp nhận từ thiết bị xác thực 14, kiểm tra khóa xác thực ở bước 358. Nếu khóa xác thực "trùng khớp" với khóa thẻ được lưu trong thẻ 12, thì sự trùng khớp giữa thiết bị xác thực 14 và thẻ 12 được xác lập một cách thành công theo phương án thực hiện làm ví dụ này. Sự xác lập thành công của sự trùng khớp được truyền thông đến AM 306. Theo một phương án khác, thẻ 12 có thể thực hiện mã hóa khóa thẻ của nó và gửi khóa thẻ được mã hóa đến thiết bị xác thực 14 để giải mã và kiểm tra sự trùng khớp. Như sẽ được hiểu bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật tương ứng, một cách có lợi, kết quả cuối cùng, tức là sự trùng khớp được kiểm tra, có thể là giống với phương án khác.

Sau đó AM 306 sẽ cho phép người dùng nhập lại mật khẩu mới đối với thẻ 12. AM 306 sẽ thay thế mật khẩu cũ của thẻ bằng mật khẩu mới, ở bước 360 hoặc sẽ tái thiết lập mật khẩu thành mật khẩu mặc định.

Do đó, chỉ khi người đưa ra thẻ "trùng khớp"và thiết bị xác thực 14, thì việc tái thiết lập mật khẩu được cho phép. Điều này có thể khắc phục một cách có lợi các vấn đề được liên kết với các giải pháp đã có được mô tả trong phần tình trạng kỹ thuật của sáng chế được nêu trên. Theo một phương án khác, AM 306 phân tích thiết bị xác thực 14 và thẻ 12 để xác nhận liên kết giữa chúng. Nói cách khác, AM 306 xác định một cách tự động liệu thẻ 12 và thiết bị xác thực 14 "có thuộc về nhau" hay không. Nếu chúng là thuộc về nhau, thì điều này đóng vai trò như là bằng chứng về việc người đưa ra thẻ là người được cấp quyền/chủ sở hữu của thẻ 12. Nếu không, việc tái thiết lập mật khẩu sẽ bị từ chối.

Theo một ví dụ, cả thẻ 12 và thiết bị xác thực 14, mà thuộc về nhau, đều chứa chuỗi dữ liệu đơn nhất giống nhau, như khóa thẻ và khóa xác thực trùng khớp tương

ứng. AM 306 sẽ so sánh các chuỗi dữ liệu trên thẻ 12 và trong thiết bị xác thực 14. Nếu hai chuỗi dữ liệu là giống nhau, thì sự trùng khớp được xác lập. Theo một ví dụ khác, các chuỗi dữ liệu trên thẻ 12 và thiết bị xác thực 14 thuộc về nhau có thể khác nhau. Trong trường hợp này, AM 306 sẽ sử dụng thuật toán xác thực để xử lý hai chuỗi dữ liệu để xác lập liệu chúng có trùng khớp với nhau hay không. Phương pháp như là mật hóa khóa bí mật hoặc các phương pháp thích hợp khác có thể được sử dụng theo các phương án thực hiện làm ví dụ.

Nếu sự xác thực liên kết giữa thẻ 12 và thiết bị xác thực 14 là thành công, AM 306, hoặc là tự động hoặc là được nhắc bởi thao tác nhập của người dùng, thực thi bước tái thiết lập mật khẩu.

Như nêu trên, bộ định danh đơn nhất được lưu trong thẻ 12 và thiết bị xác thực 14 tương ứng có thể được sử dụng trong việc kiểm tra sự trùng khớp giữa thẻ 12 và thiết bị xác thực 14, theo cùng phương thức như được mô tả đối với sự so khớp khóa nêu trên khi đề cập đến Fig.3.

Thẻ mã hóa phó bản

Sau đây, cách thiết bị xác thực 14 có thể sẽ được sử dụng một cách có lợi làm bằng chứng về việc người "được cấp quyền" trước khi tạo thẻ phó bản của thẻ 12 sẽ được mô tả.

Theo Fig.4a), theo một ví dụ, người dùng đưa ra thẻ “trống” 15 cùng với thiết bị xác thực 14 vào máy tính điện tử 400 chẳng hạn ở trung tâm dịch vụ, trạm sản xuất, giao diện trang mạng của nhà sản xuất hoặc đại lý ủy quyền. Thẻ “trống” 15 là thẻ không (chưa) được liên kết với thẻ bảo mật và chẳng hạn, không chứa khóa thẻ đơn nhất và cho phép khóa thẻ đơn nhất mới được đặt trong đó. Lưu ý rằng, thẻ thông thường cũng có thể được biến đổi thành thẻ “trống” bằng cách gỡ bỏ khóa thẻ. Chẳng hạn, người dùng đưa thẻ vào, nhập mật khẩu vào để thể hiện người dùng là chủ sở hữu và sau đó loại bỏ hoặc thay thế khóa thẻ. Do đó, thẻ thông thường có thể được sử dụng thay thế thẻ “trống” 15 theo một phương án khác.

Thiết bị xác thực 14 và thẻ 15 được nối với thiết bị tính toán 400 qua các liên kết truyền thông tương ứng 404, 402. Thẻ 15 và thiết bị xác thực 14 có thể được nối đồng

thời với máy tính 400 hoặc có thể được nối tuần tự, chẳng hạn khi chỉ một giao diện truyền thông để nối với máy tính 400 có thể sử dụng được.

Như được thể hiện trên Fig.4b), người dùng lựa chọn để tạo ra thẻ phó bản ở bước 450, chẳng hạn từ danh mục trình đơn được đưa ra trên màn hình máy tính dưới sự điều khiển của AM 406 chạy trên máy tính 800 đáp ứng lại việc cắm thẻ trống 15 và thiết bị xác thực 14 vào. Khi xác nhận yêu cầu, thiết bị xác thực 14 tạo ra khóa thẻ trùng khớp từ khóa xác thực của nó và mã hóa khóa thẻ ở bước 452. Các phương pháp như là mật hóa khóa bí mật hoặc các phương pháp thích hợp khác có thể được sử dụng theo các phương án thực hiện làm ví dụ.

Khóa thẻ được mã hóa được gửi đến thẻ "trống" 15, chẳng hạn qua AM 406, ở bước 454. Thẻ 15 giải mã khóa thẻ được tiếp nhận từ thiết bị xác thực 14 và cài đặt khóa thẻ được giải mã ở bước 456. Do đó, thẻ "trống" 15 bây giờ được biến đổi thành thẻ trùng khớp với, tức là được liên kết với thiết bị xác thực 14.

Theo một phương án khác, AM 406 trên máy tính 400 phân tích cú pháp thiết bị xác thực 14 và tạo ra khóa thẻ đối với thẻ 15. Khóa thẻ này được so khớp với khóa xác thực của thiết bị xác thực 14, sau đó được nhập vào thẻ 15 nhờ AM 406. Thẻ 15 và thiết bị xác thực 14 bây giờ "thuộc về nhau", tức là trở thành một cặp trùng khớp hoặc được liên kết. Theo ví dụ này, việc tạo thẻ phó bản là để thay thế thẻ bị hư hại. Điều này có thể được mong muốn trong trường hợp này để AM 406 trở thành máy chủ trong môi trường được cấp quyền.

Khi thiết bị xác thực 14 còn chứa bộ định danh đơn nhất để liên kết với thẻ, thiết bị xác thực 14, hoặc AM 406 theo một phương án khác, tạo ra bộ định danh đơn nhất trùng khớp để lưu trong thẻ 15 theo cùng phương thức như khóa thẻ.

Theo các ví dụ được mô tả trên đề cập đến Fig.3 và Fig.4, điều được giả thiết là thiết bị xác thực 14 được giữ an toàn bởi người dùng/chủ sở hữu của thẻ 12, do nó không cần cho sự sử dụng thông thường. Do đó, việc sở hữu thiết bị xác thực 14 có thể được xem là bằng chứng cho việc người này "được cấp quyền".

Tái mã hóa bằng khóa mới

Ví dụ: Thiết bị xác thực tái mã hóa dữ liệu

Trong các trường hợp khác, người dùng có thể mong muốn tái mã hóa các dữ liệu bảo mật của mình, mà dữ liệu này đã được mã hóa bởi thẻ đã bị mất. Trong ví dụ tiếp theo này, quá trình tái mã hóa các dữ liệu bảo mật sao cho thẻ bị mất không còn có khả năng truy cập đến các dữ liệu này được mô tả có dựa vào Fig.5a) và Fig.5b), theo một phương án.

Như được thể hiện trên Fig.5a), người dùng nối thiết bị xác thực 14 và thẻ 12 với máy tính chủ 500, qua các liên kết truyền thông tương ứng 504, 502. Thẻ này có thể là thẻ thay thế mới đối với thẻ bị mất. Như được thể hiện trên Fig.5b) người dùng nhập mật khẩu thẻ ở bước 550 và mật khẩu được kiểm tra và được xác minh là đúng ở bước 552.

Sau đó, AM 506 tiếp nhận lệnh của người dùng để thay đổi khóa xác thực và khóa thẻ và tái mã hóa tất cả các tệp tin bảo mật bằng khóa thẻ mới ở bước 554.

Ở bước 556, các dữ liệu bảo mật được giải mã bởi thiết bị xác thực 14 sử dụng khóa xác thực hiện thời. Thiết bị xác thực 14 sau đó tạo ra khóa thẻ mới và khóa xác thực trùng khớp ở bước 558. Thiết bị xác thực 14 tái mã hóa các dữ liệu bằng cách sử dụng khóa thẻ mới ở bước 560.

Thiết bị xác thực 14 thay thế khóa xác thực cũ của nó bằng khóa xác thực được tạo ra mới ở bước 562. Khóa thẻ mới được mã hóa bởi thiết bị xác thực và được chuyển đến thẻ 12, chẳng hạn qua AM 506, ở bước 564. Thẻ 12 giải mã khóa thẻ mới đã được tiếp nhận và thay thế khóa thẻ cũ bằng khóa thẻ mới ở bước 566.

Khóa thẻ và khóa xác thực bây giờ đã được thay thế bằng phiên bản mới hơn và các tệp tin bảo mật đã được tái mã hóa bằng khóa mới. Do đó, một cách có lợi, khóa bị mất hoặc bị đánh cắp, mà thẻ 12 là sự thay thế cho khóa này, sẽ không còn có khả năng mở các tệp tin bảo mật.

Ví dụ: Thẻ mới tái mã hóa dữ liệu

Theo một phương án khác, thẻ 12 có thể thực hiện các chức năng thay thế khóa và tái mã hóa của thiết bị xác thực 14. Sau khi các dữ liệu được giải mã bởi thiết bị xác thực 14, thì thẻ thay thế 12 tái mã hóa các dữ liệu bằng khóa thẻ mới. Sau đó, thẻ 12 sẽ mã hóa khóa thẻ mới của nó và gửi khóa thẻ này đến thiết bị xác thực 14. Thiết bị xác

thực 14 giải mã khóa thẻ này và tạo ra và cài đặt khóa xác thực mới là khóa trùng khớp với khóa thẻ mới. Như sẽ được hiểu bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật tương ứng, một cách có lợi, kết quả cuối cùng, tức là khóa thẻ và khóa xác thực đã được thay thế bằng phiên bản mới hơn và các tệp tin bảo mật đã được tái mã hóa bằng khóa mới, có thể giống như theo phương án khác.

Ví dụ: Tái mã hóa dữ liệu trình quản lý giấy phép

Theo một phương án khác, người dùng lệnh AM 506 tái mã hóa các tập tin dữ liệu bảo mật của mình, AM 506 sẽ tạo ra khóa xác thực mới đối với thiết bị xác thực 14 và khóa thẻ trùng khớp mới đối với thẻ trùng khớp 12 của nó, theo phương án thực hiện làm ví dụ này. Bằng cách sử dụng khóa xác thực cũ, AM 506 sẽ giải mã các dữ liệu bảo mật. Sau đó sẽ tái mã hóa dữ liệu được giải mã bằng cách sử dụng khóa thẻ mới. Do đó, thẻ bị mất hoặc bị đánh cắp bây giờ không thể truy cập các dữ liệu này với khóa thẻ cũ của nó. AM 506 sẽ ghi khóa xác thực mới vào thiết bị xác thực 14 để thay thế khóa xác thực cũ và khóa thẻ mới vào thẻ 12 để thay thế khóa thẻ cũ. Thẻ 12 bây giờ sẽ có khả năng truy cập các dữ liệu bảo mật, bằng cách sử dụng khóa thẻ mới.

Truy cập chỉ đọc

Sau đây sẽ mô tả cách thiết bị xác thực 14 có thể được sử dụng một cách có lợi để truy cập chỉ đọc các dữ liệu bảo mật có hoặc không có sự yêu cầu mật khẩu theo một phương án thực hiện làm ví dụ.

Theo Fig.6, nếu thiết bị xác thực 14 được nối với máy tính chủ 600 qua liên kết truyền thông 604, DSM 602 thực hiện việc điều khiển truy cập chỉ đọc đối với các dữ liệu bảo mật trên cơ sở sự kết nối thiết bị xác thực 14 và sự tháo bỏ thiết bị xác thực 14. Để cho phép truy cập, DSM 602 gửi các dữ liệu được mã hóa đến thiết bị xác thực 14 để giải mã các dữ liệu. Trong quá trình người dùng truy cập chỉ đọc đối với các dữ liệu bảo mật, DSM 602 luôn phát hiện liệu thiết bị xác thực 14 có mặt hay không. Nếu DSM 602 phát hiện ra rằng, thiết bị xác thực 14 được tháo ra khỏi máy tính chủ 600, thì người dùng lập tức bị từ chối truy cập vào các dữ liệu bảo mật.

Theo một phương án khác, DSM 602 đọc và phân tích khóa xác thực từ thiết bị xác thực 14. Với khóa xác thực, DSM 602 có thể nhận được khóa thẻ để giải mã các dữ

liệu bảo mật. Theo một phương án của sáng chế, khóa xác thực từ thiết bị xác thực 14 là bằng với khóa thẻ. Người dùng được cho phép truy cập chỉ đọc vào các dữ liệu bảo mật nếu thiết bị xác thực 14 được nối. Trong quá trình người dùng truy cập chỉ đọc vào các dữ liệu bảo mật, DSM 602 luôn phát hiện liệu thiết bị xác thực 14 có mặt hay không. Nếu DSM 602 phát hiện ra rằng, thiết bị xác thực 14 được tháo ra khỏi máy tính chủ 600, thì người dùng lập tức bị từ chối truy cập vào các dữ liệu bảo mật.

Theo cách đó, một cách có lợi, các phương án thực hiện làm ví dụ cho phép nếu người dùng quên mật khẩu hoặc làm mất thẻ, người dùng vẫn có khả năng đọc các dữ liệu bằng cách sử dụng thiết bị xác thực 14.

Các phương án thực hiện làm ví dụ và các phương án biến thể

Theo một phương án của sáng chế, thiết bị tự xác thực để xác thực người dùng hoặc chủ sở hữu của thiết bị bảo mật điện tử được đề xuất, trong đó thiết bị phục hồi tự xác thực tách biệt khỏi thiết bị bảo mật và được cấu hình để nối với thiết bị tính toán qua liên kết truyền thông thứ nhất để xử lý tự xác thực, tốt hơn là để xử lý xác thực và phục hồi. Việc xử lý xác thực có thể bao gồm việc xác thực liên kết giữa thiết bị bảo mật và thiết bị phục hồi tự xác thực. Việc xử lý xác thực có thể bao gồm sự so khớp khóa thứ nhất và/hoặc bộ định danh đơn nhất thứ nhất được lưu trong thiết bị tự xác thực với khóa thứ hai và/hoặc bộ định danh đơn nhất thứ hai được lưu trong thiết bị bảo mật.

Theo một phương án của sáng chế, thiết bị tự xác thực được cấu hình để tạo ra khóa thứ ba và/hoặc bộ định danh đơn nhất thứ ba để cấu hình thiết bị bảo mật khác thành được liên kết với thiết bị tự xác thực.

Thiết bị tự xác thực có thể được cấu hình để cho phép tái thiết lập mật khẩu được lưu trong thiết bị bảo mật khi sự xác thực thành công.

Thiết bị tự xác thực có thể còn có cấu hình để nối với máy tính chủ qua liên kết truyền thông thứ hai, để đọc dữ liệu được lưu chẳng hạn trên đĩa bảo mật ảo trên máy tính chủ. Thiết bị tự xác thực có thể còn được cấu hình để nối với máy tính chủ qua liên kết truyền thông thứ hai, để đọc dữ liệu được lưu chẳng hạn trên đĩa bảo mật ảo trên máy tính chủ có yêu cầu hoặc không yêu cầu mật khẩu.

Theo một phương án thiết bị tự xác thực được cấu hình để giải mã dữ liệu được lưu chẳng hạn trên đĩa bảo mật ảo trên máy tính chủ, tạo ra khóa thứ tư và mã hóa các dữ liệu bằng cách sử dụng khóa thứ tư.

Thiết bị tính toán có thể là máy tính chủ đối với thiết bị bảo mật hoặc thiết bị tính toán nằm trong một hoặc nhiều thiết bị trong nhóm bao gồm trung tâm dịch vụ, trạm sản xuất, giao diện trang mạng của nhà sản xuất hoặc đại lý ủy quyền. Thiết bị bảo mật có thể là thẻ mã hóa dữ liệu.

Theo một phương án của sáng chế, phương pháp tự xác thực để xác thực người dùng hoặc chủ sở hữu của thiết bị bảo mật điện tử được đề xuất, phương pháp này bao gồm bước nối thiết bị tự xác thực tách biệt khỏi thiết bị bảo mật với thiết bị tính toán qua liên kết truyền thông thứ nhất để xử lý tự xác thực, tốt hơn là để xử lý xác thực và phục hồi. Phương pháp có thể còn bao gồm bước nối thiết bị bảo mật với thiết bị tính toán qua liên kết truyền thông thứ hai, để xử lý tự xác thực. Bước xử lý xác thực có thể bao gồm việc xác thực liên kết giữa thiết bị bảo mật và thiết bị tự xác thực. Việc xử lý xác thực có thể bao gồm sự so khớp khóa thứ nhất và/hoặc bộ định danh đơn nhất thứ nhất được lưu trong thiết bị tự xác thực với khóa thứ hai và/hoặc bộ định danh đơn nhất thứ hai được lưu trong thiết bị bảo mật.

Theo một phương án của sáng chế, phương pháp có thể còn bao gồm bước tái thiết lập mật khẩu người dùng được lưu trong thiết bị bảo mật khi xác thực thành công liên kết giữa thiết bị tự xác thực và thiết bị bảo mật.

Việc xử lý xác thực có thể bao gồm việc thu được khóa thứ ba và/hoặc bộ định danh đơn nhất thứ ba từ thiết bị tự xác thực để tạo cấu hình thiết bị bảo mật chưa được liên kết thành được liên kết với thiết bị tự xác thực.

Phương pháp có thể còn bao gồm bước nối thiết bị tự xác thực với máy tính chủ qua liên kết truyền thông thứ ba để đọc dữ liệu được lưu chẳng hạn trên đĩa bảo mật ảo trên máy tính chủ. Bước đọc các dữ liệu được lưu chẳng hạn trên đĩa bảo mật ảo trên máy tính chủ là có yêu cầu hoặc không yêu cầu mật khẩu.

Theo một phương án của sáng chế, phương pháp còn bao gồm bước giải mã dữ liệu được lưu chẳng hạn trên đĩa bảo mật ảo của máy tính chủ; mã hóa dữ liệu được giải

mã bằng cách sử dụng khóa mới; và lưu khóa mới trong thẻ và khóa xác thực trùng khớp trong thiết bị tự xác thực.

Thiết bị bảo mật có thể là thẻ mã hóa dữ liệu.

Sẽ được hiểu bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật tương ứng là một số phương án biến thể và/hoặc các phương án cải biến có thể được thực hiện đối với sáng chế như được thể hiện theo các phương án cụ thể mà không tách rời phạm vi của sáng chế như được mô tả một cách tổng quát. Do đó, các phương án này cần được xem xét ở tất cả các khía cạnh là để minh họa và không nhằm hạn chế. Đồng thời, sáng chế bao gồm sự kết hợp bất kỳ của các dấu hiệu, cụ thể là, sự kết hợp bất kỳ của các dấu hiệu theo các điểm của yêu cầu bảo hộ, ngay cả khi nếu dấu hiệu hoặc sự kết hợp của các dấu hiệu không được nêu một cách rõ ràng trong các điểm của yêu cầu bảo hộ hoặc các phương án này.

Chẳng hạn, chức năng của DSM và AM được mô tả theo các phương án thực hiện làm ví dụ có thể được thực hiện trong một trình quản lý điều khiển bảo mật (Security Control Manager - SCM) theo các phương án khác nhau.

Đồng thời, trong khi các phương án của sáng chế đã được mô tả trong phạm vi của thẻ bảo mật để mã hóa dữ liệu, nên hiểu rằng, sáng chế có thể được áp dụng đối với các thiết bị bảo mật điện tử khác nhau như là các thẻ truy cập bảo mật điện tử đối với các công trình hoặc các khu vực an ninh.

Dưới dạng một ví dụ khác, mặc dù theo các phương án được mô tả, thẻ bảo mật được thực hiện dưới dạng một thiết bị di động, cần lưu ý rằng sáng chế có thể được sử dụng kết hợp với các phương án thực hiện khác nhau của thẻ bảo mật. Chẳng hạn, thẻ bảo mật có thể được thực hiện bằng cách sử dụng một hoặc nhiều thiết bị tương tác mà có thể tương tác không dây và/hoặc có dây để thực hiện chức năng bảo mật cần thiết. Các thiết bị có thể bao gồm một hoặc nhiều thiết bị ngoại vi như là bộ nhớ USB flash, điện thoại di động hoặc máy tính /thiết bị khác bất kỳ.

Ngoài ra, mặc dù trong các phương án được mô tả, thẻ bảo mật được thực hiện để mã hóa dữ liệu bằng cách sử dụng ổ đĩa ảo, nhưng nên hiểu rằng rằng, theo các

phương án khác, sự mã hóa tệp tin, sự mã hóa thư mục hoặc sự mã hóa toàn bộ đĩa v.v.. có thể được thực hiện.

YÊU CẦU BẢO HỘ

1. Thiết bị tự xác thực (14) dùng cho người dùng hoặc chủ sở hữu của thiết bị bảo mật điện tử (12), trong đó thiết bị tự xác thực (14) tách biệt khỏi thiết bị bảo mật (12) và được cấu hình để nối với thiết bị tính toán (300, 400, 500, 600) thông qua liên kết truyền thông thứ nhất để xử lý tự xác thực và trong đó thiết bị tự xác thực (14) được cấu hình để cho phép tái thiết lập mật khẩu người dùng được lưu trong thiết bị bảo mật (12) khi việc tự xác thực thành công mà không yêu cầu người dùng nhập mật khẩu xác thực.

2. Thiết bị tự xác thực (14) theo điểm 1, trong đó việc xử lý tự xác thực bao gồm việc so khớp khóa thứ nhất và/hoặc bộ định danh đơn nhất thứ nhất được lưu trong thiết bị tự xác thực (14) với khóa thứ hai và/hoặc bộ định danh đơn nhất thứ hai được lưu trong thiết bị bảo mật (12).

3. Thiết bị tự xác thực (14) theo điểm bất kỳ trong số các điểm từ 1 đến 2, trong đó thiết bị tự xác thực (14) được cấu hình để tạo ra khóa thứ ba và/hoặc bộ định danh đơn nhất thứ ba để tạo cấu hình thiết bị bảo mật khác (15) thành được liên kết với thiết bị tự xác thực (14).

4. Thiết bị tự xác thực (14) theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó thiết bị tự xác thực (14) còn được cấu hình để nối với máy tính chủ (300, 400, 500, 600) thông qua liên kết truyền thông thứ hai, để đọc dữ liệu được lưu, chẳng hạn trên đĩa bảo mật ảo trên máy tính chủ (300, 400, 500, 600).

5. Thiết bị tự xác thực (14) theo điểm 4, trong đó thiết bị tự xác thực (14) còn được cấu hình để nối với máy tính chủ (300, 400, 500, 600) thông qua liên kết truyền thông thứ hai, để đọc dữ liệu được lưu, chẳng hạn trên đĩa bảo mật ảo trên máy tính chủ (300, 400, 500, 600) mà không yêu cầu mật khẩu.

6. Thiết bị tự xác thực (14) theo điểm bất kỳ trong số các điểm từ 1 đến 5, trong đó thiết bị tự xác thực (14) được cấu hình để giải mã dữ liệu được lưu chẳng hạn trên đĩa bảo mật ảo trên máy tính chủ (300, 400, 500, 600), tạo ra khóa thứ tư và mã hóa các dữ liệu bằng cách sử dụng khóa thứ tư.

7. Thiết bị tự xác thực (14) theo điểm bất kỳ trong số các điểm từ 1 đến 6, trong đó thiết bị bảo mật (12) là thẻ mã hóa dữ liệu.

8. Phương pháp tự xác thực dùng cho người dùng hoặc chủ sở hữu của thiết bị bảo mật điện tử (12), phương pháp này bao gồm bước nối thiết bị tự xác thực (14) tách biệt khỏi thiết bị bảo mật (12) với thiết bị tính toán (300, 400, 500, 600) thông qua liên kết truyền thông thứ nhất để xử lý tự xác thực và tái thiết lập mật khẩu người dùng được lưu trong thiết bị bảo mật (12) khi xác thực thành công liên kết giữa thiết bị tự xác thực (14) và thiết bị bảo mật (12) mà không yêu cầu người dùng nhập mật khẩu xác thực.

9. Phương pháp theo điểm 8, trong đó bước xử lý tự xác thực bao gồm việc xác thực liên kết giữa thiết bị bảo mật (12) và thiết bị tự xác thực (14).

10. Phương pháp theo điểm 9, trong đó bước xử lý tự xác thực bao gồm việc so khớp khóa thứ nhất và/hoặc bộ định danh đơn nhất thứ nhất được lưu trong thiết bị tự xác thực (14) với khóa thứ hai và/hoặc bộ định danh đơn nhất thứ hai được lưu trong thiết bị bảo mật (12).

11. Phương pháp theo điểm bất kỳ trong số các điểm từ 8 đến 10, trong đó bước xử lý tự xác thực bao gồm việc thu được khóa thứ ba và/hoặc bộ định danh đơn nhất thứ ba từ thiết bị tự xác thực (14) để tạo cấu hình thiết bị bảo mật chưa được liên kết (15) thành được liên kết với thiết bị tự xác thực (14).

12. Phương pháp theo điểm bất kỳ trong số các điểm từ 8 đến 11, trong đó phương pháp này còn bao gồm bước nối thiết bị tự xác thực (14) với máy tính chủ (300, 400, 500, 600) thông qua liên kết truyền thông thứ ba để đọc dữ liệu được lưu, chẳng hạn trên đĩa bảo mật ảo trên máy tính chủ (300, 400, 500, 600).

13. Phương pháp theo điểm 12, trong đó bước đọc các dữ liệu được lưu, chẳng hạn trên đĩa bảo mật ảo trên máy tính chủ (300, 400, 500, 600) không yêu cầu mật khẩu.

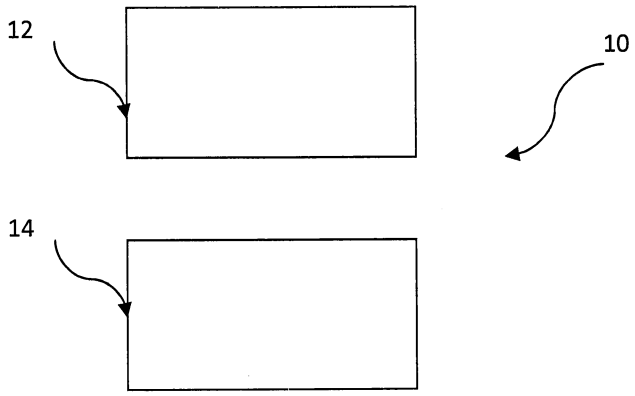
14. Phương pháp theo điểm bất kỳ trong số các điểm từ 8 đến 13, trong đó phương pháp này còn bao gồm bước:

giải mã dữ liệu được lưu chẳng hạn trên đĩa bảo mật ảo của máy tính chủ (300, 400, 500, 600);

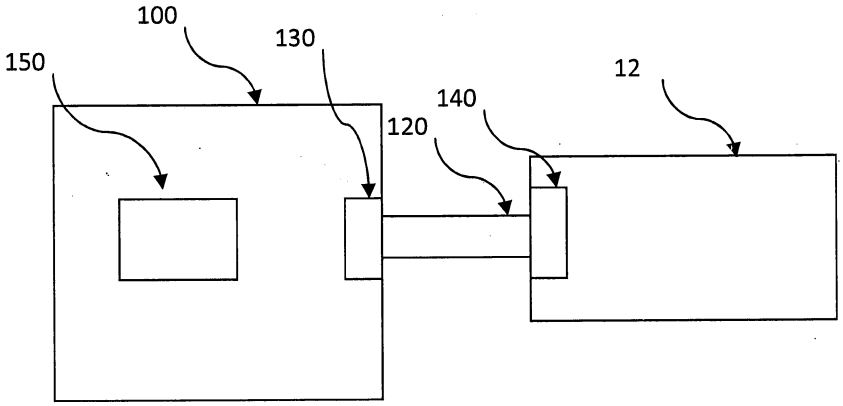
mã hóa dữ liệu được giải mã bằng cách sử dụng khóa mới; và

lưu khóa mới trong thiết bị bảo mật (12) và khóa xác thực trùng khớp trong thiết bị tự xác thực (14).

15. Phương pháp theo điểm bất kỳ trong số các điểm từ 8 đến 14, trong đó thiết bị bảo mật (12) là thẻ mã hóa dữ liệu.



a)



b)

Fig.1

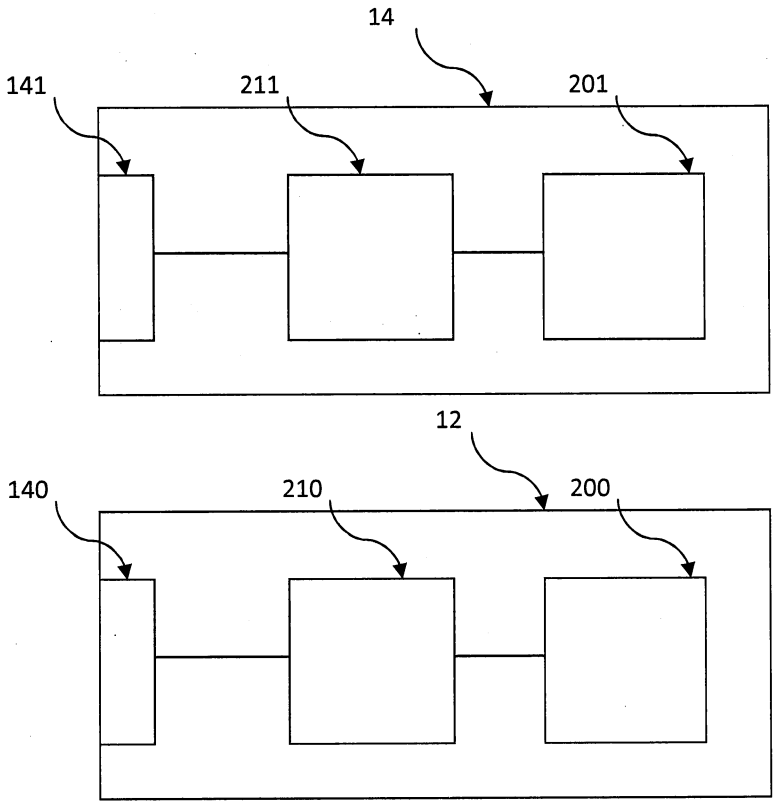
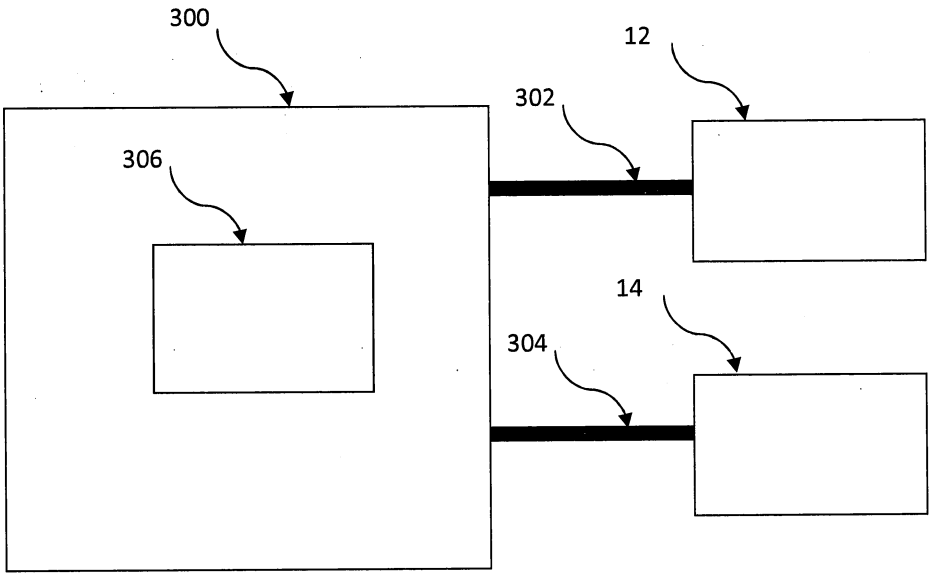
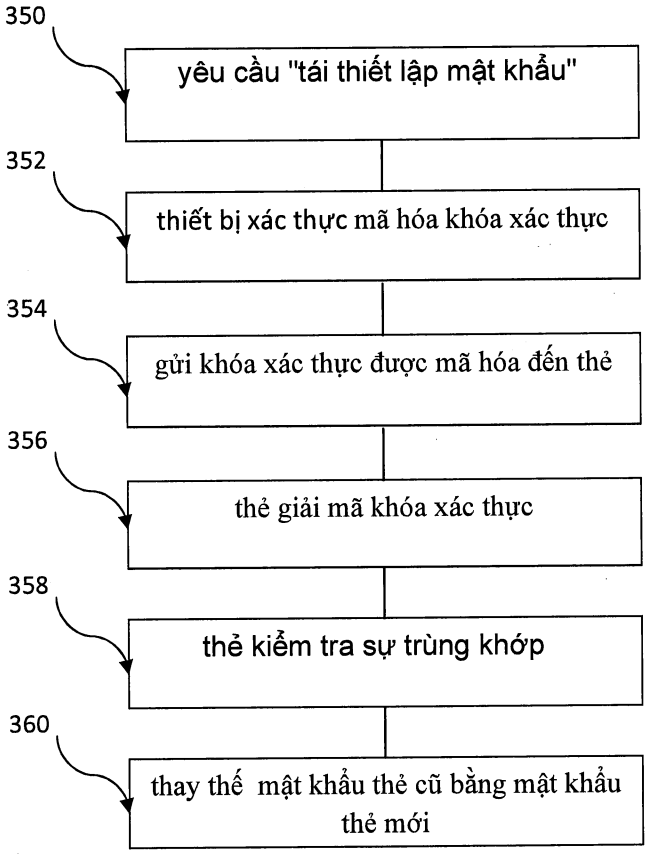


Fig.2

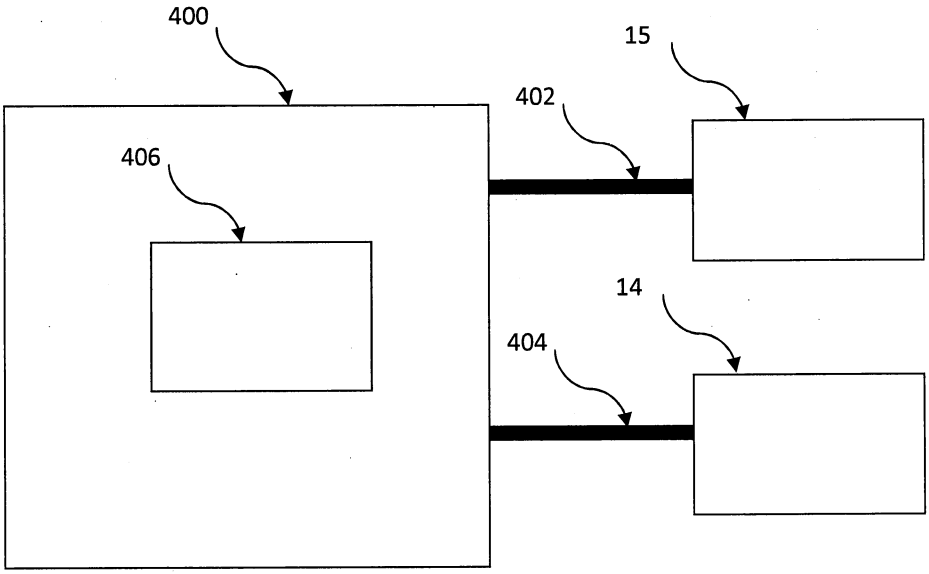

300
12
302
306
14
304

a)

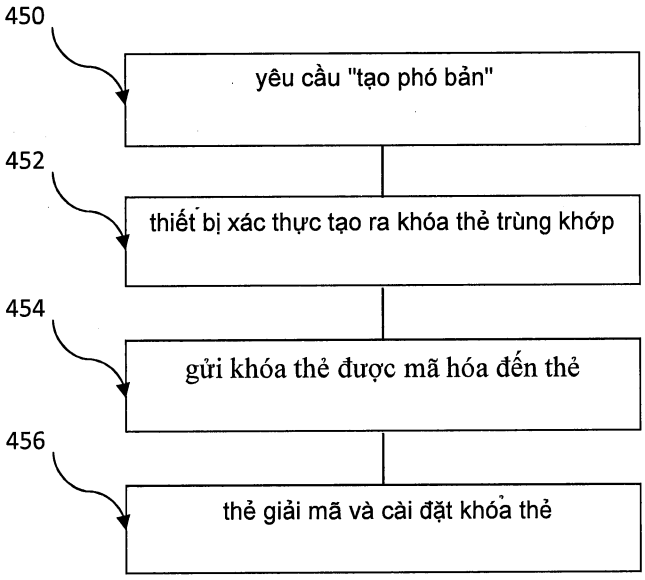

350
yêu cầu "tái thiết lập mật khẩu"
352
thiết bị xác thực mã hóa khóa xác thực
354
gửi khóa xác thực được mã hóa đến thẻ
356
thẻ giải mã khóa xác thực
358
thẻ kiểm tra sự trùng khớp
360
thay thế mật khẩu thẻ cũ bằng mật khẩu thẻ mới

b)

Fig.3

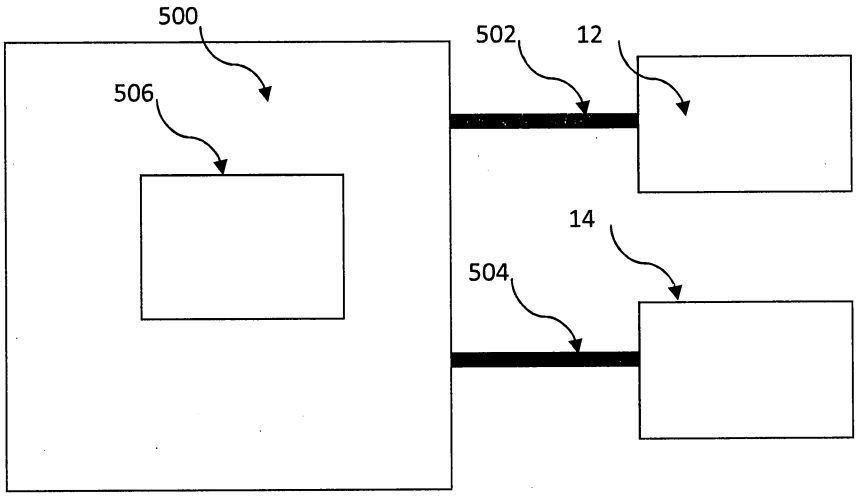

400
15
402
406
14
404

a)

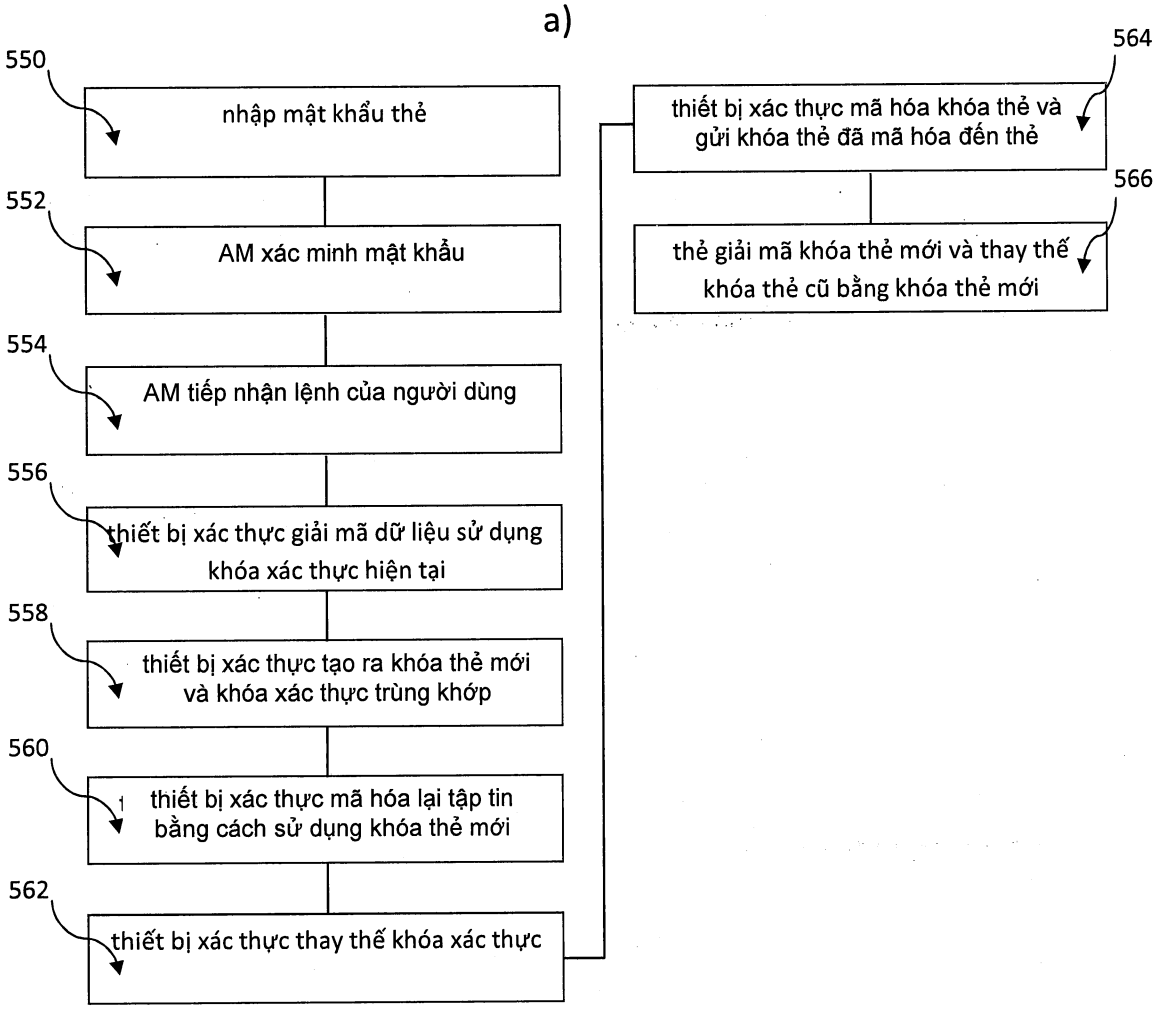

450
yêu cầu "tạo phó bản"
452
thiết bị xác thực tạo ra khóa thẻ trùng khớp
454
gửi khóa thẻ được mã hóa đến thẻ
456
thẻ giải mã và cài đặt khóa thẻ

b)

Fig.4


500
506
502
12
14
504

a)


550
nhập mật khẩu thẻ
552
AM xác minh mật khẩu
554
AM tiếp nhận lệnh của người dùng
556
thiết bị xác thực giải mã dữ liệu sử dụng khóa xác thực hiện tại
558
thiết bị xác thực tạo ra khóa thẻ mới và khóa xác thực trùng khớp
560
thiết bị xác thực mã hóa lại tập tin bằng cách sử dụng khóa thẻ mới
562
thiết bị xác thực thay thế khóa xác thực
564
thiết bị xác thực mã hóa khóa thẻ và gửi khóa thẻ đã mã hóa đến thẻ
566
thẻ giải mã khóa thẻ mới và thay thế khóa thẻ cũ bằng khóa thẻ mới

b)

Fig.5

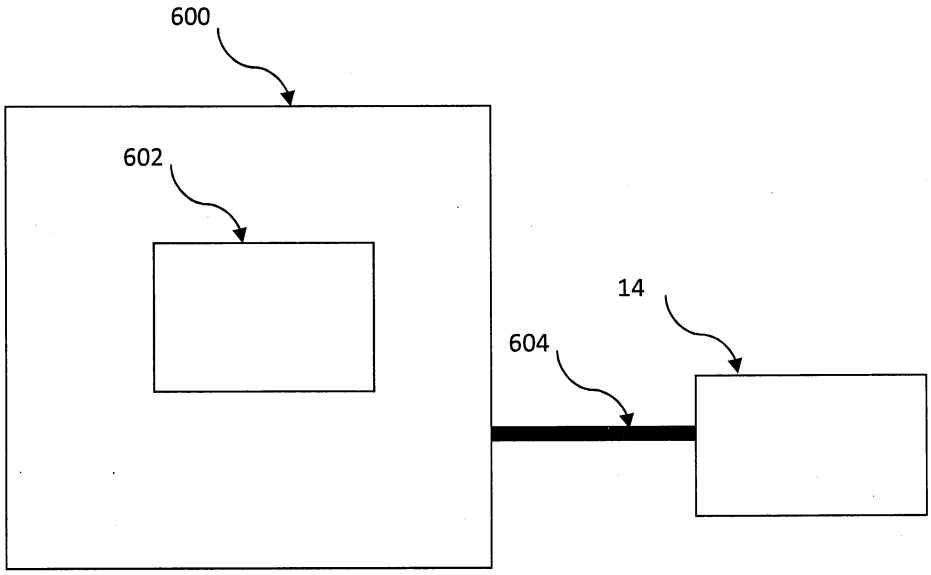


Fig.6