(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) **1-0025327**

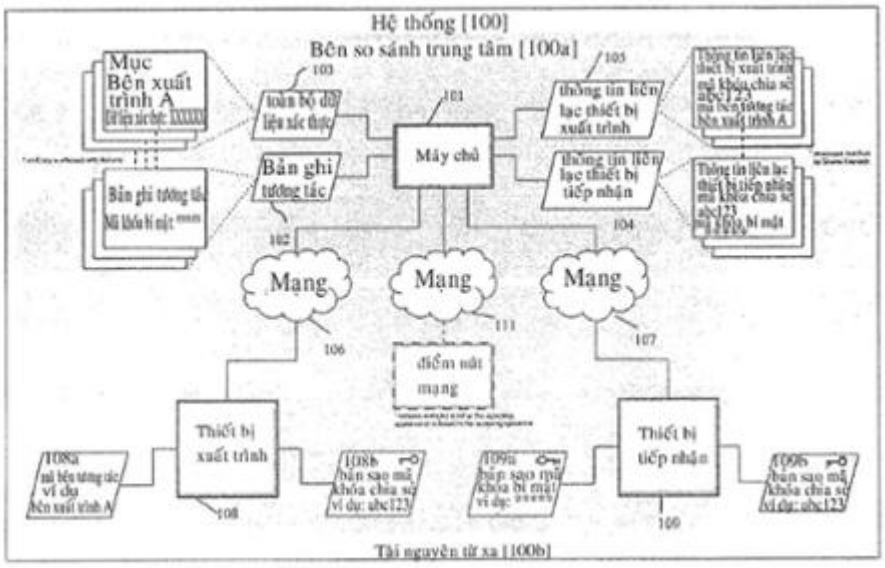
(51)[7] **H04L 29/06**; G06Q 20/20; G06Q 20/40; G06F 21/62; G06Q 20/32

(13) **B**

(21) 1-2016-02853
(22) 09/01/2015
(86) PCT/EP2015/050354 09/01/2015
(87) WO2015/104387 16/07/2015
(30) 14150856.4 10/01/2014 EP
(45) 25/09/2020 390
(43) 27/02/2017 347A
(73) PRIVITI PTE. LTD. (SG)
Level 24, Suite 03-36 31 Rochester Drive Singapore 138637
(72) Gerard BARRY (IE); Declan BARRY (IE).
(74) Văn phòng Luật sư Ân Nam (ANNAM IP & LAW)

(54) HỆ THỐNG VÀ PHƯƠNG PHÁP DÙNG ĐỂ TRUYỀN THÔNG DỮ LIỆU XÁC THỰC

(57) Sáng chế đề xuất hệ thống và phương pháp thực hiện các giao dịch liên quan đến sự truyền thông các dữ liệu xác thực được kết nối với một tổ chức hoặc cá nhân, được biết đến là bên xuất trình đến đích đến được cấp phép, được biết đến là điểm nút mạng (110) theo yêu cầu từ bên tiếp nhận trong khi vẫn duy trì tính riêng tư thường thấy trong các dữ liệu xác thực. Hệ thống bao gồm các thiết bị xuất trình (108) và các thiết bị tiếp nhận (109) truyền thông với máy chủ điều khiển (101). Máy chủ điều khiển nhận thông tin truyền thông từ các thiết bị tiếp nhận và xuất trình chứa mã khóa bí mật dành riêng cho cá nhân hoặc bên xuất trình, các mã nhận biết bên xuất trình và mã khóa chia sẻ và nếu các thông tin truyền thông này là phù hợp với nhau, các dữ liệu xác thực đặc trưng cho mã nhận biết bên xuất trình được cho phép được phát hành cho điểm nút mạng đã biết.



Lĩnh vực kỹ thuật được đề cập

Sáng chế thuộc lĩnh vực kỹ thuật thông tin và truyền thông, tính riêng tư của sự trao đổi dữ liệu được thực hiện bởi kỹ thuật thông tin và truyền thông, cũng như việc sử dụng và bảo vệ tính riêng tư thường thấy của các dữ liệu xác thực được truyền thông với kỹ thuật thông tin và truyền thông. Tính riêng tư là quyền sở hữu của thực thể hoặc sự tham gia vào thông tin bất kỳ của thực thể, hoặc bộ dữ liệu xác thực bất kỳ liên quan đến thực thể và cá nhân cụ thể. Cụ thể, sáng chế liên quan đến, nhưng không bị giới hạn ở việc được phép phát hành dữ liệu bao gồm bộ thông tin cá nhân riêng tư và dữ liệu xác thực đã được kiểm soát mà người thiết lập dữ liệu xác thực có thể muốn chấp nhận và cho phép để được kín đáo phát hành theo cách được bảo vệ và an toàn trong khi đảm bảo được sự bảo toàn và duy trì liên tục tính bảo mật và riêng tư về các thông tin cá nhân và các dữ liệu xác thực đã được kiểm soát cho nhiều mục đích. Các dữ liệu xác thực đã được kiểm soát là thông tin liên quan đến người sở hữu/người phát hành các dữ liệu xác thực đã được kiểm soát và người nắm giữ/sở hữu các dữ liệu xác thực đã được kiểm soát.

Tình trạng kỹ thuật của sáng chế

Trong xã hội hiện đại, các cá nhân được gắn liền với một loạt các dữ liệu cá nhân. Một số ví dụ về dữ liệu cá nhân đó bao gồm, nhưng không giới hạn ở tên, địa chỉ, ngày sinh, quốc tịch, số an sinh xã hội, số hộ chiếu, số giấy phép lái xe, mã số thành viên (trong tổ chức nhất định), tên thời con gái (nếu có), tên thời con gái của mẹ, thông tin nơi làm việc, số tài khoản ngân hàng, số thẻ tín dụng, v.v.. Dữ liệu cá nhân này được sử dụng theo vô số cách như/và khi các cá nhân tương tác với cá nhân hoặc tổ chức khác. Nhiều loại tương tác phụ thuộc rất nhiều vào độ chính xác của bộ dữ liệu vừa đặc thù cho mỗi cá nhân vừa cần thiết cho sự tương tác. Theo đó, vì mỗi bộ dữ liệu như thế (sau đây được gọi là "bộ dữ liệu xác thực") vừa đặc thù cho mỗi cá nhân vừa cần thiết cho sự tương tác, nên đó là thông tin nhạy cảm cần được giữ ở trạng thái riêng tư. Thông tin này là dữ liệu liên quan bổ sung nhạy cảm (và cần được giữ ở trạng thái riêng tư), ví dụ như dữ liệu liên quan đến các đặc trưng bảo mật bổ sung, ví dụ, mã khóa bí mật được kết hợp với công cụ nhất định. Điều này cũng sẽ được hiểu rằng

ngay cả khi có dự định lấy bộ dữ liệu xác thực từ bản ghi, có thể cần đảm bảo rằng dữ liệu kết hợp sẽ không bao giờ bị lộ ra, đặc biệt là khi dữ liệu đó liên quan đến các đặc trưng bảo mật bổ sung.

Các vị trí đăng ký bản ghi như thế thường được đặt theo cách như sau. Bộ dữ liệu xác thực liên quan đến một người được cung cấp cho bộ điều khiển và bộ dữ liệu xác thực được xác minh và công nhận. Ngay khi bộ dữ liệu xác thực được xác minh và công nhận, công cụ được tạo ra mang bộ dữ liệu xác thực, và bộ dữ liệu xác thực này được cung cấp cho người đó. Bộ dữ liệu xác thực cũng được nhập vào bản ghi mới trong vị trí đăng ký bản ghi và thường được bổ sung với dữ liệu bất kỳ liên quan đến công cụ tương ứng (ví dụ như số seri, v.v.) và dữ liệu liên quan khác (ví dụ dữ liệu đặc trưng bảo mật bổ sung bao gồm, nhưng không giới hạn ở sinh trắc học, v.v.).

Các phương pháp đã được phát triển để đưa ra các bộ dữ liệu xác thực trên các công cụ chuyên biệt như thế. Trong lịch sử, dữ liệu như thế có thể đã được đánh dấu, làm nổi bật hoặc dán nhãn trên công cụ được phát hành. Sau này, dữ liệu kiểu này có thể được dập nổi hoặc khắc hoặc mã hóa hoặc gắn chìm trên công cụ được phát hành. Gần đây hơn, phương tiện ghi có thể đọc được bằng máy (ví dụ băng từ hoặc các con chip) đã được sử dụng làm công cụ, trong đó các bộ dữ liệu xác thực liên quan được lưu trên phương tiện ghi đó. Dạng thức của nhiều công cụ (và dạng thức trong đó các bộ dữ liệu xác thực được lưu trên đó) được quản lý bởi Tổ chức tiêu chuẩn quốc tế (International Organization for Standardization – ISO). Ví dụ, ISO 7501 quản lý dạng thức của các tài liệu du lịch có thể đọc bằng máy; ISO 7810 và ISO 7811 quản lý dạng thức của thẻ nhận dạng; và ISO 7812 và ISO 7816 quản lý cách thức trong đó các thẻ có thể được cung cấp từ các nhà phát hành khác nhau.

Ngay cả đã đạt được các tiến bộ trong việc cung cấp các công cụ mang các bộ dữ liệu xác thực, vẫn còn tồn tại nguy cơ gian lận. Vẫn cần thiết để có thể vừa xác minh rằng bên xuất trình mang công cụ bao gồm bộ dữ liệu xác thực là đúng là người chủ/hợp lệ (tức là, công cụ không bị đánh cắp hoặc làm giả và do đó không bị sử dụng gian lận), và vừa xác minh rằng công cụ được tặng chứa bộ dữ liệu xác thực là thực sự chính xác (tức là, dữ liệu xác thực là chính xác và công cụ không phải là sản phẩm giả mạo hoàn toàn). Đây là một vấn đề đang ngày càng được quan tâm do người mang các công cụ này trình ra các bộ dữ liệu xác thực của họ trên cơ sở ngày càng thường xuyên. Trong khi các bộ dữ liệu xác thực ban đầu được giữ trong môi trường bí

mật/riêng tư, tồn tại giữa người có các bộ dữ liệu xác thực và các nhà điều khiển, môi trường bí mật/riêng tư này bị nguy hại bất kỳ khi nào khi bộ dữ liệu xác thực được trình ra trong khi trao đổi với bên thứ ba. Trong khi các cải thiện trong việc bảo mật bằng các phương tiện nhờ đó các bộ dữ liệu xác thực được trình ra được phát hành để hỗ trợ cho việc môi trường bí mật/riêng tư này vẫn được giữ.

Ví dụ, với trường hợp với sự ra đời của các hệ thống đọc các công cụ hộ chiếu tự động, khi hành khách xuất trình hộ chiếu của họ cho nhân viên kiểm tra hoặc cơ quan kiểm soát biên giới bất kỳ ("người chấp nhận"), các dữ liệu xác thực đã được điều chỉnh trên công cụ được phát hành cấp có thể xác định được và được xử lý bởi người chấp nhận trước và sau khi chụp các dữ liệu xác thực đã được điều chỉnh trong thiết bị đọc. Nếu vi phạm chính sách bảo mật, dữ liệu xác thực được xem được sao chép và chia sẻ bởi người chấp nhận, không chỉ được chụp và xử lý, trạng thái riêng tư trong đó các dữ liệu xác thực ban đầu có trong công cụ hộ chiếu có thể được chấp nhận. Các thiếu sót tương tự tồn tại đối với các dụng cụ khác mà hệ thống chụp dữ liệu xác thực tự động đã được phát triển, chẳng hạn như giấy phép lái xe, thẻ khách hàng thân thiết/thẻ hội viên, và các loại thẻ thanh toán.

Cần có các phương pháp và hệ thống cải tiến để nhờ đó bên xuất trình có thể trao đổi các bộ dữ liệu xác thực trong quá trình trao đổi với các cá nhân hoặc tổ chức khác theo cách thức đảm bảo cả tính xác thực của bộ dữ liệu xác thực, và tính xác thực của các bên xuất trình mang bộ dữ liệu xác thực. Cũng rất cần có phương pháp và hệ thống để đảm bảo môi trường hoàn toàn bí mật/riêng tư cho các bộ dữ liệu xác thực khi chúng được bộc lộ. Đối với các phương pháp và hệ thống cải tiến bất kỳ như thế để có thể tương thích ngược với các phương pháp và các hệ thống hiện có, tốt nhất là ứng dụng thông thường sao cho các phương pháp và hệ thống cải tiến có thể được thực hiện theo từng giai đoạn một cách trôi chảy và từ từ. Đây sẽ là thuận lợi rất lớn vì sẽ không cần quá trình chuyển đổi tốn kém và mất thời gian sang hệ thống và phương pháp mới. Tốt hơn là các phương pháp và hệ thống cải tiến mới bất kỳ có thể mở rộng sao cho chúng có thể dùng cho nhiều bộ dữ liệu xác thực khác nhau thông qua một hệ thống và phương pháp duy nhất.

US-A-201 310246203 bộc lộ cách thực hiện các giao dịch thanh toán trong đó sự gian lận đã được giảm xuống. Các dữ liệu xác thực cho việc thanh toán của khách hàng không bao giờ được cung cấp cho người bán và không thể truy cập được để sử

dụng trong giao dịch thanh toán trừ khi có yêu cầu truy cập được cung cấp từ thiết bị đã được cấp quyền do khách hàng chỉ định. Theo một phương án, thiết bị đã được cấp quyền bao gồm điện thoại di động.

Tài liệu WO-A-20041049621 bộc lộ hệ thống xác nhận trong đó thiết bị đầu cuối thứ nhất truyền thông với bên hỗ trợ qua kênh viễn thông thứ nhất và thiết bị đầu cuối thứ hai truyền thông với bên điều hành qua kênh viễn thông thứ hai, bên hỗ trợ và bên điều hành có thể truyền thông với nhau. Không có dữ liệu nhận dạng được cung cấp cho thiết bị đầu cuối thứ nhất bởi bên điều hành, bên hỗ trợ hoặc thiết bị đầu cuối thứ hai, và không có dữ liệu nhận dạng của thiết bị đầu cuối thứ nhất được cung cấp cho thiết bị đầu cuối thứ hai bởi bên điều hành, bên hỗ trợ hoặc thiết bị đầu cuối thứ nhất, và sự truyền thông giữa thiết bị đầu cuối thứ nhất và bên hỗ trợ, và giữa thiết bị đầu cuối thứ hai và bên điều hành không chứa dữ liệu liên quan đến các chi tiết nhận dạng của người dùng.

Tài liệu WO-A-20131034192 bộc lộ phương pháp để xác nhận giao dịch điện tử trong đó dữ liệu nhận dạng được chuyển từ điện thoại di động đến thiết bị đầu cuối điểm bán và cần được xác nhận bởi một mã PIN được cung cấp cho máy chủ bằng cuộc gọi qua điện thoại.

Bản chất kỹ thuật của sáng chế

Một khía cạnh của sáng chế bao gồm hệ thống cho phép sự truyền thông của ít nhất một bộ dữ liệu xác thực đã được kiểm soát kết nối với bên xuất trình, đến điểm nút mạng, đồng thời duy trì tính riêng tư thường thấy trong các dữ liệu xác thực đã được kiểm soát nêu trên được kết nói với bên xuất trình, trong đó hệ thống bao gồm ít nhất một thiết bị tiếp nhận, ít nhất một thiết bị xuất trình, ít nhất một điểm nút mạng và ít nhất một máy chủ, và trong đó một trong các máy chủ nêu trên bao gồm một hoặc nhiều bản ghi. Mỗi bản ghi liên quan đến bên xuất trình đã cho, bao gồm mã nhận biết bên xuất trình, và mã khóa bí mật được liên kết với mỗi mã nhận biết bên xuất trình, và được liên kết với ít nhất một mục phù hợp với bộ các dữ liệu xác thực đã được kiểm soát kết nối với bên xuất trình. Mỗi mục liên quan đến ít nhất một bộ các dữ liệu xác thực liên quan đến bên xuất trình đã cho. Mỗi mục cũng có thể liên quan đến ít nhất một tên hiệu, mỗi tên hiệu được kết nối với một trong các bộ các dữ liệu xác thực nêu trên. Mỗi điểm nút mạng là một nơi tiếp nhận được chỉ định của loại dữ liệu xác thực

đã được kiểm soát được kết đối với các bên xuất trình, mỗi điểm nút hoặc là bên tiếp nhận hoặc là điểm nút do bên thứ ba chỉ định được liên kết với bên tiếp nhận; trong đó việc cho phép truyền thông của ít nhất một bộ các dữ liệu xác thực đã được kiểm soát kết nối với bên xuất trình được thực hiện trong bối cảnh tương tác giữa dụng cụ tương tác xuất trình và dụng cụ tương tác tiếp nhận; và trong đó bộ dữ liệu xác thực có sự cho phép được kết hợp với dụng cụ tương tác xuất trình. Một trong các máy chủ nêu trên có chức năng là máy chủ điều khiển còn được tạo cấu hình để (a) tiếp nhận thông tin truyền thông từ dụng cụ tiếp nhận mà sau đây được gọi là thông tin truyền thông bên tiếp nhận, thông tin truyền thông này chứa mã khóa bí mật liên quan đến bên xuất trình và mã khóa chia sẻ một lần; (b) nhận thông tin truyền thông từ bên xuất trình mà sau đây được gọi là thông tin truyền thông bên xuất trình, thông tin truyền thông này chứa mã nhận biết bên xuất trình liên quan đến bên xuất trình và mã khóa chia sẻ một lần; (c) tìm để phối chọn mã khóa chia sẻ một lần có trong thông tin truyền thông bên tiếp nhận và mã khóa chia sẻ một lần tương ứng có trong thông tin truyền thông bên xuất trình; (d) khởi tạo tìm kiến đối với bản ghi mục tiêu bằng cách liên kết mã khóa bí mật có trong thông tin truyền thông bên tiếp nhận nêu trên và mã nhận dạng mã nhận biết bên xuất trình có trong thông tin truyền thông bên xuất trình đó, trong đó cả hai thông tin truyền thông này đều chứa cùng một mã khóa chia sẻ; (e) tiến hành tìm kiến đối với bản ghi đích nêu trên sao cho bao gồm cả mã khóa bí mật nêu trên và mã nhận biết bên xuất trình nêu trên; (f) nhận biết mục được liên kết với bản ghi đích nêu trên, mục này liên quan đến bộ các dữ liệu xác thực đã được kiểm soát kết nối với bên xuất trình; (g) cho phép thu hồi bộ dữ liệu xác thực liên quan đến mục nêu trên và cho phép phát hành bộ dữ liệu xác thực nêu trên đến điểm nút mạng nêu trên, điểm nút nêu trên là bên tiếp nhận được cấp phép của bộ các dữ liệu xác thực đã được kiểm soát kết nối với bên xuất trình nêu trên, và điểm nút là bên tiếp nhận hoặc là điểm được bên thứ ba chỉ định được liên kết với bên tiếp nhận.

Khía cạnh khác của sáng chế bao gồm phương pháp cho phép sự truyền thông của ít nhất một bộ các dữ liệu xác thực đã được kiểm soát kết nối với bên xuất trình, từ máy chủ đến điểm nút mạng, trong khi vẫn duy trì tính riêng tư thường thấy trong các dữ liệu xác thực đã được kiểm soát kết nối với bên xuất trình; và trong đó máy chủ bao gồm một hoặc nhiều bản ghi, mỗi bản ghi liên quan đến một bên xuất trình (bên được đăng ký với máy chủ dưới dạng bên xuất trình và/hoặc dưới dạng bên tiếp nhận), và

mỗi bản ghi có chứa mã nhận biết bên xuất trình (và/hoặc mã nhận biết bên tiếp nhận) và mã khóa bí mật (của bên xuất trình và/hoặc bên tiếp nhận) liên kết với mã nhận biết bên xuất trình, và mỗi bản ghi được liên kết với mục liên quan đến bộ các dữ liệu xác thực đã được kiểm soát (được kết hợp với bên nêu trên) được kết nối với bên xuất trình nêu trên; phương pháp bao gồm các bước: (a) tại bên tiếp nhận, làm cho mã khóa chia sẻ một lần sẵn sàng đối với dụng cụ tương tác xuất trình; (b) tại bên tiếp nhận, nhận mã khóa bí mật (bên xuất trình) liên quan đến dụng cụ tương tác xuất trình trong đó mã khóa bí mật (bên xuất trình) nêu trên được nhập vào bên tiếp nhận nhờ dụng cụ tương tác xuất trình; (c) tại bên tiếp nhận, truyền thông thông tin truyền thông bên tiếp nhận đến ít nhất một trong số các máy chủ, thông tin truyền thông bên tiếp nhận này chứa mã khóa chia sẻ một lần và mã khóa bí mật (bên xuất trình); (d) tại bên xuất trình có dụng cụ tương tác xuất trình, nhận mã phín chia sẻ một lần; (e) tại bên xuất trình, lấy lại mã nhận biết bên xuất trình liên quan đến dụng cụ tương tác xuất trình từ ví trí lưu trữ trên bên xuất trình; và (f) tại bên xuất trình, truyền thông thông tin truyền thông bên xuất trình tới máy chủ, thông tin truyền thông bên xuất trình này chứa mã khóa chia sẻ một lần và mã nhận biết bên xuất trình, trong đó (g) ngay khi nhận thông tin truyền thông bên tiếp nhận và thông tin truyền thông bên xuất trình nêu trên, tại máy chủ, xử lý các thông tin truyền thông để xác định chắc chắn nếu nó được cấp phép để truyền thông bộ các dữ liệu xác thực đã được kiểm soát kết nối với bên xuất trình, nhờ đó cho phép lấy lại tại máy chủ và nhờ đó cho phép phát hành tới điểm nút mạng, điểm nút mạng này được phép tiếp nhận, và điểm nút này là bên tiếp nhận hoặc bên thứ ba được chỉ định liên kết với bên tiếp nhận.

Theo một khía cạnh của sáng chế, tất cả các bộ dữ liệu xác thực được kết nối với bên xuất trình (hoặc các tên hiệu liên kết với các bộ dữ liệu xác thực) có thể được bao gồm toàn bộ trong bản ghi nêu trên.

Theo khía cạnh khác của sáng chế, tất các bộ dữ liệu xác thực được kết nối với bên xuất trình (và các tên hiệu được liên kết) có thể được bao gồm dưới dạng các mục riêng biệt trên một máy chủ riêng biệt có khả năng truyền thông với máy chủ điều khiển. Ngoài ra, một số bộ dữ liệu xác thực được kết nối với bên xuất trình và các tên hiệu được liên kết có thể được bao gồm toàn bộ trong bản ghi nêu trên, trong khi các bộ dữ liệu xác thực còn lại có thể được bao gồm dưới dạng các mục riêng biệt trên máy chủ đó hoặc dưới dạng các mục riêng biệt trên các máy chủ khác nhau.

Thông tin truyền thông thiết bị tiếp nhận có thể được truyền thông với máy chủ nêu trên qua kênh truyền thông thứ nhất và thông tin truyền thông thiết bị xuất trình có thể được truyền thông với máy chủ trên qua kênh truyền thông thứ hai.

Theo một khía cạnh của sáng chế, mã khóa chia sẻ một lần có thể được tạo ra tại máy chủ và được truyền thông tới thiết bị tiếp nhận trước khi mã khóa chia sẻ một lần này được đưa sẵn sàng cho bên tương tác xuất trình hoặc/và thiết bị xuất trình.

Theo khía cạnh khác của sáng chế, mã khóa chia sẻ một lần có thể được tạo ra tại thiết bị tiếp nhận trước khi mã khóa chia sẻ một lần được tạo ra sẵn sàng cho bên tương tác xuất trình hoặc/và thiết bị xuất trình.

Bản sao của mã khóa chia sẻ một lần có thể được truyền thông từ thiết bị tiếp nhận tới thiết bị xuất trình thông qua công nghệ vô tuyến, công nghệ vô tuyến được tùy chọn từ nhóm gồm có Wifi, bluetooth, NFC hoặc RFID.

Theo một khía cạnh của sáng chế, thời hạn hiệu lực có thể được ấn định cho thông tin truyền thông thiết bị tiếp nhận và thông tin truyền thông thiết bị xuất trình và/hoặc mã khóa chia sẻ. Điều này đảm bảo rằng nếu thông tin truyền thông thiết bị tiếp nhận không phù hợp với thông tin truyền thông thiết bị xuất trình như sẽ được đề cập dưới đây là trong khoảng thời gian nhất định (thời hạn hiệu lực), sau đó thông tin truyền thông này trôi qua và từ đó trở nên mất giá trị để thực hiện các quy trình sau đó. Khi các thông tin truyền thông này trôi qua và từ đó trở nên mất giá trị để thực hiện các quy trình sau đó, dữ liệu liên quan đến thông tin truyền thông có thể được loại bỏ, mở thông các tài nguyên để xử lý các thông tin truyền thông khác. Khi các thông tin truyền thông được tạo ra, phát hoặc thu, chứa các mã khóa chia sẻ mang thời hạn hiệu lực, thời hạn hiệu lực có thể đảm bảo là các mã khóa chia sẻ ngắn và ít phức tạp có thể được sử dụng vì nhờ đó việc tái sử dụng các mã khóa chia sẻ có thể xảy ra. Khi hết thời gian thời hạn hiệu lực của mã khóa chia sẻ, cùng một mã khóa chia sẻ có thể được tái sử dụng lặp lại sau đó theo phương pháp.

Theo một khía cạnh của sáng chế, bản sao của mã khóa chia sẻ một lần có thể sẵn sàng cho bên tương tác xuất trình hoặc/và thiết bị xuất trình thông qua màn hình có trong thiết bị tiếp nhận hoặc trên bản in từ thiết bị tiếp nhận, trong đó hoặc là: (a) bản sao của mã khóa chia sẻ một lần được tạo sẵn sàng ở định dạng ký tự có thể đọc được bằng máy, ví dụ UTF-8, và bản sao của mã khóa chia sẻ một lần được nhận ở thiết bị

ngoại vi xuất trình thông qua việc nhập từ bên tương tác xuất trình hoặc/và bên tương tác tiếp nhận hoặc/và thiết bị tiếp nhận; hoặc là (b) bản sao của mã khóa chia sẻ một lần được bao gồm trong mã QR, và bản sao của mã khóa chia sẻ một lần được nhận ở thiết bị xuất trình thông qua chức năng camera có trong thiết bị xuất trình được sử dụng để chụp mã phản ứng nhanh và xuất bản sao của mã khóa chia sẻ một lần.

Thông tin truyền thông thiết bị tiếp nhận có thể còn chứa một hoặc nhiều tham số phụ định trước, và thông tin truyền thông thiết bị xuất trình cũng có thể còn chứa một hoặc nhiều tham số phụ định trước nêu trên. Các tham số phụ này có thể tùy chọn cũng phải phù hợp như sẽ được mô tả dưới đây trước khi sự chứng thực thành công để khởi tạo và tiến hành tìm kiếm các bản ghi đích bất kỳ. Điều kiện phù hợp thêm này trong quá trình chứng thực, khi được đặt quanh và trên mã khóa chia sẻ, còn nâng cao phương pháp do nó đưa ra các điều kiện bổ sung vào quy trình tìm để phối chọn thông tin truyền thông thiết bị tiếp nhận và thông tin truyền thông thiết bị xuất trình. Tham số phụ định trước có thể là mã đã được thỏa thuận giữa bên tương tác tiếp nhận và bên tương tác xuất trình, hoặc có thể là giá trị thích hợp với sự tương tác giữa bên tương tác xuất trình và bên tương tác tiếp nhận, ví dụ như giá trị giao dịch dự tính.

Nếu thời hạn hiệu lực được ấn định cho mã khóa chia sẻ một lần, mã khóa chia sẻ đó có thể là duy nhất trong suốt thời hạn hiệu lực của nó.

Khía cạnh khác của sáng chế đề xuất phương pháp cho phép truyền thông ít nhất một bộ dữ liệu xác thực kiểm soát được kết nối với bên xuất trình, ở máy chủ tới điểm nút mạng, trong khi vẫn duy trì tính riêng tư chung trong bộ dữ liệu xác thực đã được kiểm soát được kết nối với bên xuất trình trong đó sự cấp phép có chứa thông tin truyền thông thiết bị tiếp nhận chứa mã khóa chia sẻ và mã khóa bí mật của bên xuất trình, và thông tin truyền thông thiết bị xuất trình chứa mã khóa chia sẻ và mã nhận biết bên xuất trình, phương pháp bao gồm: (a) ở máy chủ nhận thông tin truyền thông thiết bị tiếp nhận; (b) tại máy chủ nhận thông tin truyền thông thiết bị xuất trình; (c) tại máy chủ tìm để phối chọn mã khóa chia sẻ một lần có trong thông tin truyền thông thiết bị tiếp nhận với mã khóa chia sẻ một lần tương ứng có trong thông tin truyền thông thiết bị xuất trình, (d) ở máy chủ, khởi tạo tìm kiếm đối với bản ghi đích bằng cách liên kết mã khóa bí mật (bên xuất trình) có trong thông tin truyền thông thiết bị tiếp nhận và mã nhận biết bên xuất trình có trong thông tin truyền thông thiết bị xuất trình, trong đó cả hai thông tin truyền thông này đều chứa cùng một mã khóa chia sẻ;

(e) ở máy chủ, tiến hành tìm kiếm đối với bản ghi đích bao gồm cả hai mã khóa bí mật (bên xuất trình) nêu trên và mã nhận biết bên xuất trình nêu trên; (f) nếu bản ghi đích được xác định, tại máy chủ, xác định mục được liên kết với bản ghi đích nêu trên, mục này liên quan đến các dữ liệu xác thực đã được kiểm soát được kết nối với bên xuất trình; (g) tại máy chủ, cho phép lấy lại bộ dữ liệu xác thực được xác định bởi mục liên kết với bản ghi đích, và cho phép phát hành bộ dữ liệu xác thực đó đến điểm nút mạng, điểm nút này là bên tiếp nhận được cấp phép đối với bộ dữ liệu xác thực đã được kiểm soát được kết nối với bên xuất trình, và điểm nút này là thiết bị tiếp nhận hoặc là bên thứ ba được chỉ định được liên kết với thiết bị tiếp nhận.

Bản ghi đích ở máy chủ nêu trên cũng có thể còn có chứa tên hiệu được kết hợp với mục liên quan đến mỗi bộ dữ liệu xác thực được kết nối với bên xuất trình, và thông tin truyền thông thiết bị xuất trình có thể còn chứa bản sao của tên hiệu được lựa chọn từ danh sách các tên hiệu được phân loại tại thiết bị xuất trình, trong đó bước tiến hành tìm kiếm đối với bản ghi đích bao gồm cùng một mã nhận biết bên xuất trình và mã khóa bí mật cũng sử dụng bản sao của tên hiệu có trong thông tin truyền thông thiết bị xuất trình để tìm kiếm đối với bản ghi đích có chứa tên hiệu tương tự bên cạnh mã nhận biết bên xuất trình và mã khóa bí mật giống nhau.

Mục liên quan đến bộ dữ liệu xác thực được kết nối với bên xuất trình có thể được bao gồm trong bản ghi đích trên máy chủ điều khiển được tạo cấu hình cho phép lấy lại và phát hành bộ dữ liệu xác thực được kết nối với bên xuất trình, và các bước lấy lại bộ dữ liệu xác thực được kết nối với bên xuất trình và phát hành bộ dữ liệu xác thực được kết nối với bên xuất trình được thực hiện ở máy chủ điều khiển được tạo cấu hình cho phép lấy lại và phát hành bộ dữ liệu xác thực được kết nối với bên xuất trình.

Bộ dữ liệu xác thực được kết nối với bên xuất trình có thể được bao gồm trong các mục riêng biệt trên máy chủ khác tách biệt với máy chủ điều khiển được tạo cấu hình cho phép lấy lại và phát hành bộ dữ liệu xác thực được kết nối với bên xuất trình, các mục riêng biệt được liên kết với bản ghi đích, trong đó các bước lấy lại và phát hành bộ dữ liệu xác thực được thực hiện ở máy chủ điều khiển được tạo cấu hình cho phép lấy lại và phát hành bộ dữ liệu xác thực được kết nối với bên xuất trình hoặc máy chủ khác tách biệt với máy chủ điều khiển được tạo cấu hình cho phép lấy lại và phát hành bộ dữ liệu xác thực được kết nối với bên xuất trình.

Thời hạn hiệu lực có thể được ấn định cho thông tin truyền thông thiết bị tiếp nhận và/hoặc thông tin truyền thông thiết bị xuất trình và/hoặc mã khóa chia sẻ có trong thông tin truyền thông thiết bị tiếp nhận hoặc/và trong thông tin truyền thông thiết bị xuất trình, trong đó bước tìm để phối chọn mã khóa chia sẻ có trong thông tin truyền thông thiết bị tiếp nhận và mã khóa chia sẻ có trong thông tin truyền thông thiết bị xuất trình còn bao gồm thiết lập thời điểm mà thời hạn hiệu lực hết hạn. Điều này đảm bảo rằng nếu thông tin truyền thông thiết bị tiếp nhận không phù hợp với thông tin truyền thông thiết bị xuất trình như được đề cập dưới đây trong khoảng thời gian nhất định (thời hạn hiệu lực), sau đó tương tác/thông báo/ truyền thông như thế trôi qua và từ đó trở nên mất giá trị để thực hiện các quy trình sau đó. Khi thời hạn hiệu lực bất kỳ trôi qua và trở nên vô giá trị để thực hiện các quy trình sau đó, dữ liệu liên quan đến thông tin truyền thông có thể được loại bỏ, mở thông các tài nguyên để xử lý các thông tin truyền thông khác. Khi các thông tin truyền thông được tạo ra/phát/ thu và chứa các mã khóa chia sẻ mang thời hạn hiệu lực, thời hạn hiệu lực có thể đảm bảo là các mã khóa chia sẻ ngắn và ít phức tạp có thể được sử dụng vì nhờ đó việc tái sử dụng các mã khóa chia sẻ có thể xảy ra. Khi hết thời gian thời hạn hiệu lực của mã khóa chia sẻ, cùng một mã khóa chia sẻ có thể được tái sử dụng lặp lại sau đó theo phương pháp.

Nếu thời hạn hiệu lực được ấn định cho mã khóa chia sẻ, mã khóa chia sẻ đó có thể là duy nhất trong suốt thời hạn hiệu lực của nó.

Thông tin truyền thông thiết bị tiếp nhận có thể còn chứa một hoặc nhiều các tham số phụ định trước, và thông tin truyền thông thiết bị xuất trình cũng có thể còn chứa một hoặc nhiều tham số phụ định trước, trong đó bước tìm để phối chọn các mã khóa chia sẻ còn bao gồm bước tìm để chứng thực tham số phụ định trước có trong thông tin truyền thông thiết bị tiếp nhận và tham số phụ định trước có trong thông tin truyền thông thiết bị xuất trình.

Khía cạnh khác nữa của sáng chế đề xuất phương pháp cho phép truyền thông bộ dữ liệu xác thực đã được kiểm soát được kết nối với bên xuất trình, tại máy chủ tới điểm nút mạng, trong khi vẫn duy trình tính riêng tư thường thấy trong các dữ liệu xác thực được kết nối với bên xuất trình, sự cấp phép được tạo ra/cấp theo khía cạnh bất kỳ của sáng chế được mô tả ở trên, phương pháp bao gồm: (a) tại máy chủ, nhận thông tin truyền thông thiết bị tiếp nhận; (b) tại máy chủ, nhận thông tin truyền thông thiết bị

xuất trình; (c) tại máy chủ, tìm để phối chọn mã khóa chia sẻ một lần có trong thông tin truyền thông thiết bị tiếp nhận và mã khóa chia sẻ một lần tương ứng có trong thông tin truyền thông thiết bị xuất trình, (và nhờ đó phối chọn thông tin truyền thông thiết bị tiếp nhận với thông tin truyền thông thiết bị xuất trình); (d) tại máy chủ, khởi tạo tìm kiếm đối với bản ghi đích bằng cách liên kết mã khóa bí mật có trong thông tin truyền thông thiết bị tiếp nhận và mã nhận biết bên xuất trình có trong thông tin truyền thông thiết bị xuất trình; (e) tại máy chủ, tiến hành tìm kiếm bản ghi đích có chứa cả hai mã khóa bí mật và mã nhận biết bên xuất trình; (f) nếu xác định được bản ghi đích, xác định mục liên quan đến bộ dữ liệu xác thực được kết nối với bên xuất trình và được kết hợp; (g) nếu bộ dữ liệu xác thực được kết nối với bên xuất trình được xác định, tại máy chủ, cho phép lấy lại bộ dữ liệu xác thực được kết nối với bên xuất trình, và cho phép phát hành bộ dữ liệu xác thực được kết nối với bên xuất trình tới điểm nút mạng, điểm nút này là bên tiếp nhận được cấp phép đối với bộ dữ liệu xác thực được kết nối với bên xuất trình, và điểm nút này là thiết bị tiếp nhận hoặc là bên thứ ba được chỉ định liên kết với thiết bị tiếp nhận.

Nếu các bộ dữ liệu xác thực được kết nối với bên xuất trình được chứa trong các bản ghi trên máy chủ điều khiển được tạo cấu hình cho phép lấy lại và phát hành các dữ liệu xác thực đã được kiểm soát, các bước lấy lại bộ dữ liệu xác thực của bên xuất trình được kết nối và truyền thông bộ dữ liệu xác thực của bên xuất trình được kết nối có thể được thực hiện tại máy chủ điều khiển được tạo cấu hình cho phép lấy lại và phát hành các dữ liệu xác thực đã được kiểm soát.

Nếu các bộ dữ liệu xác thực được kết nối với bên xuất trình được chứa trong các mục riêng biệt trên máy chủ khác tách biệt với máy chủ điều khiển được tạo cấu hình cho phép lấy lại và phát hành các dữ liệu xác thực đã được kiểm soát, (bước xác định mục liên quan đến bộ dữ liệu xác thực của bên xuất trình được kết nối có thể được thực hiện ở máy chủ khác tách biệt với máy chủ điều khiển được tạo cấu hình cho phép lấy lại và phát hành các dữ liệu xác thực đã được kiểm soát), các bước lấy lại bộ dữ liệu xác thực được kết nối và phát hành bộ dữ liệu xác thực được kết nối có thể được thực hiện tại máy chủ điều khiển được tạo cấu hình cho phép lấy lại và phát hành bộ dữ liệu xác thực được kết nối với bên xuất trình hoặc máy chủ khác tách biệt với máy chủ điều khiển được tạo cấu hình cho phép lấy lại và phát hành bộ dữ liệu xác thực được kết nối với bên xuất trình.

Bước tìm để phối chọn các mã khóa chia sẻ có thể còn bao gồm thiết lập thời điểm mà thời hạn hiệu lực hết hạn.

Bước tìm để phối chọn các mã khóa chia sẻ có thể còn bao gồm tìm để phối chọn tham số phụ định trước có trong thông tin truyền thông thiết bị tiếp nhận với tham số phụ định trước tương ứng có trong thông tin truyền thông thiết bị xuất trình.

Nếu thời hạn hiệu lực được ấn định cho mã khóa chia sẻ một lần, mã khóa chia sẻ đó có thể là duy nhất trong suốt thời hạn hiệu lực của nó.

Theo khía cạnh khác của sáng chế, phương pháp bao gồm các bước: (a) thiết bị tiếp nhận làm cho mã khóa chia sẻ một lần sẵn sàng với bên tương tác xuất trình; (b) nhận mã khóa bí mật của bên xuất trình đang thuộc về bên tương tác xuất trình tại thiết bị tiếp nhận trong đó mã khóa bí mật của bên xuất trình được nhập vào ở thiết bị đầu cuối nhờ bên tương tác xuất trình; (c) truyền thông thông tin truyền thông thiết bị tiếp nhận từ thiết bị tiếp nhận tới máy chủ, thông tin truyền thông thiết bị tiếp nhận bao gồm mã khóa chia sẻ một lần và mã khóa bí mật của bên xuất trình; (d) thiết bị xuất trình nhận mã khóa chia sẻ một lần; (e) thiết bị xuất trình lấy lại mã nhận biết bên xuất trình đang thuộc về bên tương tác xuất trình từ vị trí lưu trữ trên thiết bị xuất trình; và (f) thiết bị xuất trình truyền thông thông tin truyền thông thiết bị xuất trình tới máy chủ điều khiển, thông tin truyền thông thiết bị xuất trình bao gồm mã khóa chia sẻ một lần, và mã nhận biết bên xuất trình.

Bản ghi đích tại máy chủ cũng có thể còn có chứa tên hiệu được kết hợp với mục liên quan đến mỗi bộ dữ liệu xác thực được kết nối với bên xuất trình, và thông tin truyền thông thiết bị xuất trình còn có thể chứa bản sao của tên hiệu được chọn từ danh sách các tên hiệu được phân loại tại thiết bị xuất trình, và trong đó bước tiến hành tìm kiếm bản ghi đích có chứa mã nhận biết bên xuất trình và mã khóa bí mật giống nhau cũng sử dụng tên hiệu có trong thông tin truyền thông thiết bị xuất trình để tìm kiếm đối với bản ghi đích có cùng tên hiệu bên cạnh mã nhận biết bên xuất trình và mã khóa bí mật giống nhau.

Bộ dữ liệu xác thực có thể được chứa dưới dạng một mục trong bản ghi đích trên máy chủ điều khiển được tạo cấu hình cho phép lấy lại và phát hành các dữ liệu xác thực đã được kiểm soát, và các bước lấy lại bộ dữ liệu xác thực và phát hành bộ dữ liệu xác thực được thực hiện ở máy chủ điều khiển được tạo cấu hình cho phép lấy lại

và phát hành các dữ liệu xác thực đã được kiểm soát.

Bộ dữ liệu xác thực có thể được chứa dưới dạng một mục trên máy chủ khác tách biệt với máy chủ điều khiển được tạo cấu hình cho phép lấy lại và phát hành các dữ liệu xác thực đã được kiểm soát, mục riêng biệt được liên kết với bản ghi đích, và trong đó các bước lấy lại và phát hành bộ dữ liệu xác thực có thể được thực hiện tại hoặc là máy chủ điều khiển được tạo cấu hình cho phép lấy lại và phát hành các dữ liệu xác thực đã được kiểm soát hoặc là máy chủ khác tách biệt với máy chủ điều khiển được tạo cấu hình cho phép lấy lại và phát hành các dữ liệu xác thực đã được kiểm soát.

Khía cạnh khác nữa của sáng chế bao gồm thiết bị xuất trình được tạo cấu hình để thực hiện một hoặc nhiều bước của thiết bị xuất trình được mô tả ở trên.

Khía cạnh khác nữa của sáng chế bao gồm thiết bị tiếp nhận được tạo cấu hình để thực hiện một hoặc nhiều bước của thiết bị tiếp nhận được mô tả ở trên.

Khía cạnh bổ sung của sáng chế bao gồm máy chủ được tạo cấu hình để thực hiện một hoặc nhiều bước của máy chủ được mô tả ở trên.

Khía cạnh khác nữa của sáng chế bao gồm hệ thống bao gồm hai hoặc nhiều thiết bị xuất trình, hai hoặc nhiều thiết bị tiếp nhận, và máy chủ điều khiển được tạo cấu hình để thực hiện một hoặc nhiều phương án như được mô tả ở trên.

Khía cạnh bổ sung của sáng chế bao gồm môi trường bộ nhớ có thể đọc được bằng máy tính mang chương trình máy tính được lưu trên đó, chương trình bao gồm các chỉ lệnh có thể thực hiện được bằng máy tính để thực hiện một hoặc nhiều bước thuộc phương pháp được mô tả ở trên khi được thực hiện bởi một hoặc nhiều mô-đun xử lý.

Mô tả vắn tắt các hình vẽ

Fig.1 là biểu đồ minh họa hệ thống trung tâm để bảo vệ tính riêng tư, theo cách thức mà cũng tạo điều kiện cho phép phát hành bộ dữ liệu xác thực được lưu trữ tới nơi tiếp nhận được do bên sở hữu bộ dữ liệu xác thực chấp thuận;

Fig.2 là lưu đồ minh họa cách để một bên yêu cầu tiềm năng mới đăng ký với máy chủ 101 là bên xuất trình theo phương án của sáng chế;

Fig.3 là lưu đồ tương tự với lưu đồ trên Fig.2 mô tả các bước thông qua đó một

bên có thể đăng ký là bên tiếp nhận với máy chủ 101 theo phương án của sáng chế;

Fig.4 là lưu đồ minh họa phương pháp cho phép phát hành ít nhất một bộ dữ liệu xác thực đã được kiểm soát kết nối với bên xuất trình trong khi vẫn duy trì tính riêng tư liên quan trong các dữ liệu xác thực nêu trên theo phương án của sáng chế;

Fig.5A và Fig.5B minh họa quy trình được thực hiện ở thiết bị tiếp nhận;

Fig.6A và Fig.6B minh họa quy trình được thực hiện ở thiết bị xuất trình;

Fig.7 và Fig.8 là các hình vẽ đại diện cho các mục liên quan đến các dữ liệu xác thực được điều khiển kết nối với bên xuất trình;

Fig.7A đến Fig.7E thể hiện các phương án khác nhau để lưu các bản ghi trên máy chủ điều khiển hoặc máy chủ dữ liệu xác thực 101;

Fig.9A và Fig.9B bộc lộ các hình vẽ đại diện bằng đồ thị liên quan đến quy trình truyền thông các tin nhắn ở máy chủ điều khiển từ các bên tương tác hiện tại và các bên tương tác tiếp nhận và quá trình gửi các dữ liệu xác thực được điều khiển đến các đích đến được cấp phép;

Fig.10 là sơ đồ chuỗi minh họa quy trình nhờ đó sự cấp phép có thể được cấp theo phương án của sáng chế liên quan đến máy chủ 1001, bên tương tác xuất trình 1002, thiết bị xuất trình 1003, điểm nút mạng 1004, và thiết bị tiếp nhận 1005, để lấy lại bộ dữ liệu xác thực lưu tại vị trí được xác định bởi bên tương tác xuất trình 1002 và phát hành bộ dữ liệu xác thực tới dụng cụ của bên tiếp nhận được cho phép bởi bên tương tác xuất trình 1002.

Mô tả chi tiết sáng chế

Fig.1 là biểu đồ minh họa hệ thống trung tâm để bảo vệ tính riêng tư, theo cách thức mà cũng tạo điều kiện cho phép phát hành bộ dữ liệu xác thực được lưu trữ tới nơi tiếp nhận được do bên sở hữu bộ dữ liệu xác thực chấp thuận, hệ thống 100 đảm bảo cho các bộ dữ liệu xác thực được bảo vệ trong đó mà không bị truy cập trái phép từ các nơi tiếp nhận không được cấp phép, và cũng tránh cho các bộ dữ liệu xác thực không bị sử dụng bởi những người có thể xuất trình bộ dữ liệu xác thực một cách gian lận như là của riêng họ. Các bên đã đăng ký với hệ thống được gọi là "bên xuất trình" và "bên tiếp nhận" phù hợp với vai trò của chúng theo phương pháp của sáng chế và cách thức mà chúng tương tác với hệ thống theo sáng chế. Trong quá trình tương tác

giữa bên xuất trình và bên tiếp nhận, có thể là cần thiết để bên xuất trình đưa ra bộ dữ liệu xác thực mà chúng có liên quan. Các bên xuất trình và các bên tiếp nhận tích cực tham gia vào các tương tác lần lượt được gọi là "các bên tương tác xuất trình" và "các bên tương tác tiếp nhận". Có thể đánh giá rằng trong nhiều phương án của sáng chế, các bên xuất trình với mỗi bên được kết hợp với các bộ dữ liệu xác thực duy nhất đối với chúng sao cho các bên xuất trình được liên kết với các bộ dữ liệu xác thực theo cách thức "một-một". Tuy nhiên, sáng chế cũng dự trù các tình huống có mối liên hệ "nhiều-một" giữa các bên xuất trình và các bộ dữ liệu xác thực, với nhiều bên xuất trình được kết hợp với một bộ dữ liệu xác thực duy nhất, và vẫn có mong muốn duy trì bộ dữ liệu xác thực đó ở trạng thái riêng tư.

Theo phương án của sáng chế, hệ thống và phương pháp theo sáng chế được sử dụng nhờ bên tương tác xuất trình như thế để đưa ra bộ dữ liệu xác thực kết hợp với bên tương tác xuất trình đó cho một hoặc nhiều bên tiếp nhận được chỉ định theo cách thức để duy trì tính riêng tư thường thấy của bộ dữ liệu xác thực. Theo các phương án khác của sáng chế, hệ thống và phương pháp theo sáng chế có thể được sử dụng nhờ bên tương tác tiếp nhận để đưa ra bộ dữ liệu xác thực kết hợp với bên tương tác tiếp nhận cho một hoặc nhiều bên tiếp nhận được chỉ định trong khi vẫn bảo tồn được trạng thái riêng tư. Các phương án khác của sáng chế dự tính sự bộc lộ đồng thời của cả hai bên xuất trình và bên tiếp nhận các bộ dữ liệu xác thực lần lượt kết hợp với bên tương tác xuất trình và bên tương tác tiếp nhận. Cả hai bên xuất trình và bên tiếp nhận phối hợp để tạo thuận lợi cho việc đưa ra các bộ dữ liệu xác thực như thế từ hệ thống. Bên tiếp nhận được chỉ định có thể là bên tương tác tiếp nhận, bên tương tác xuất trình hoặc có thể là bên thứ ba tin cậy.

Hệ thống 100 bao gồm ít nhất một máy chủ 101, máy chủ bao gồm tập hợp các bản ghi xuất trình 102. Mỗi bản ghi xuất trình liên quan đến một bên tham gia có sẵn đã được đăng ký là bên xuất trình với máy chủ 101, và mỗi bản ghi có chứa một hoặc nhiều bộ dữ liệu xác thực liên quan đến bên xuất trình đó. Cụ thể hơn, mỗi bản ghi xuất trình có chứa mã nhận biết bên xuất trình, mã khóa bí mật của bên xuất trình, ít nhất một bộ dữ liệu xác thực được kết hợp với bên xuất trình đó, và ít nhất một tên hiệu, trong đó mỗi bộ dữ liệu xác thực được kế nối tương ứng với một tên hiệu nhờ đó mỗi tên hiệu thuộc bản ghi xuất trình có khả năng phân biệt với các tên hiệu còn lại đối với bản ghi đó của bên xuất trình. Mã nhận biết bên xuất trình là chuỗi ký tự duy nhất

được sử dụng để nhận biết bản ghi đã cho của bên xuất trình trong tập hợp các bản ghi xuất trình. Mã khóa bí mật của bên xuất trình là chuỗi ký tự chỉ có bên xuất trình được biết. Khi bên xuất trình tương tác với hệ thống với mục đích đưa ra bộ dữ liệu xác thực của bên xuất trình cho bên tiếp nhận được chỉ định (bên xuất trình đó được gọi là "bên tương tác xuất trình"), chúng cung cấp mã nhận biết bên xuất trình của chúng, và mã khóa bí mật của bên xuất trình của chúng có thể được sử dụng sau đó để xác thực cho bên tương tác xuất trình trước khi các bộ dữ liệu xác thực bất kỳ được đưa ra. Bên cạnh mã nhận biết bên xuất trình và mã khóa bí mật của bên xuất trình, mỗi bản ghi xuất trình có chứa ít nhất một bộ dữ liệu xác thực. Như được mô tả trước đây, mỗi bộ dữ liệu xác thực có chứa bộ dữ liệu cá nhân là thông tin chi tiết về cá nhân và cần thiết cho tương tác đã cho. Mỗi bộ dữ liệu xác thực cũng được kết hợp với tên hiệu có khả năng phân biệt. Ví dụ, cá nhân có tên "John Brown" có thể có bộ dữ liệu xác thực thứ nhất liên quan đến giấy phép lái xe, và bộ dữ liệu xác thực thứ hai liên quan đến thẻ khách hàng thân thiết của một cửa hàng. Bộ dữ liệu xác thực thứ nhất có thể gồm có tên "John Brown", ngày sinh, số giấy phép lái xe, và ngày hết hạn. Bộ dữ liệu xác thực thứ hai có thể gồm có tên "John Brown", địa chỉ, mã số thành viên câu lạc bộ khách hàng thân thiết. Bộ dữ liệu xác thực thứ nhất có thể được kết hợp với tên hiệu "giấy phép lái xe", trong khi bộ dữ liệu xác thực thứ hai có thể được kết hợp với tên hiệu "thẻ khách hàng thân thiết 1". Có thể đánh giá rằng các phương án theo sáng chế trong đó sáng chế được dự tính là mỗi bản ghi xuất trình sẽ chỉ có một bộ dữ liệu xác thực, có thể không cần thiết để các bản ghi xuất trình còn có thêm tên hiệu được kết nối với mỗi bộ dữ liệu xác thực. Đúng hơn, trong các trường hợp này, sự nhận biết bản ghi liên quan đến bên xuất trình đang tương tác cũng sẽ tự động chỉ ra bộ dữ liệu xác thực cần được đưa ra.

Ngoài ra, trong một số phương án của sáng chế, máy chủ 101 cũng bao gồm tập hợp các bản ghi tiếp nhận riêng biệt. Mỗi bản ghi tiếp nhận liên quan đến cá nhân hoặc tổ chức đã đăng ký là bên tiếp nhận với máy chủ, và có chứa mọt hoặc nhiều bộ dữ liệu xác thực kết hợp với bên tiếp nhận đó. Mỗi bản ghi tiếp nhận còn có chứa mã nhận biết bên tiếp nhận, và mã khóa bí mật của bên tiếp nhận tùy chọn. Mã nhận biết bên tiếp nhận là chuỗi ký tự duy nhất được sử dụng để nhận biết bản ghi đã cho của bên tiếp nhận trong tập hợp các bản ghi tiếp nhận. Mã khóa bí mật của bên tiếp nhận (nếu có) là chuỗi ký tự chỉ có bên tiếp nhận biết. Khi bên tiếp nhận tương tác với hệ

thống với mục đích để tạo thuận lợi cho việc đưa ra bộ dữ liệu xác thực của bên xuất trình kết hợp với bên tương tác xuất trình với bên tiếp nhận được chỉ định (bên tiếp nhận này được gọi là "bên tương tác tiếp nhận") mã nhận biết bên tiếp nhận của bên tương tác tiếp nhận được cung cấp, và mã khóa bí mật bên tiếp nhận của bên tương tác tiếp nhận (nếu sử dụng) có thể được sử dụng sau đó để chứng thực cho bên tương tác tiếp nhận trước khi các bộ dữ liệu xác thực bất kỳ được bộc lộ.

Có thể đánh giá rằng trong khi trong các phương án được mô tả của sáng chế, các bản ghi xuất trình và các bản ghi tiếp nhận là riêng biệt và thường được duy trì dưới dạng các tập hợp bản ghi riêng biệt, trong các phương án khác của sáng chế, máy chủ 101 có thể bao gồm tập hợp bản ghi duy nhất chứa cả các bản ghi xuất trình và bên tiếp nhận. Ngoài ra, cũng có thể đánh giá rằng trong khi trong một phương án, các bộ dữ liệu xác thực của bên tiếp nhận và/hoặc của bên xuất trình được lưu trong một máy chủ, nhiều máy chủ cũng có thể được tính đếnm trong đó mỗi máy chủ chịu trách nhiệm lưu trữ các bản ghi có một hoặc nhiều kiểu bộ dữ liệu xác thực.

Cũng có dự tính rằng trong một số phương án của sáng chế, máy chủ 101 sẽ chỉ có các bản ghi xuất trình, và sẽ không có các bản ghi tiếp nhận. Tốt nhất là, theo các phương án này, máy chủ 101 và các bên có thể là bên tương tác tiếp nhận sẽ có khả năng giao tiếp với nhau thông qua hệ thống phần mềm tồn tại giữa chúng. Phương án này của sáng chế có ưu điểm vì không đòi hỏi các bên tiếp nhận đăng ký trước, và loại bỏ các trở ngại đến hệ thống và phương pháp theo sáng chế trong số các bên có thể là bên tương tác tiếp nhận. Do đó, điều này làm cải thiện khả năng dễ sử dụng của hệ thống và phươn pháp.

Máy chủ 101 có khả năng giao tiếp với một hoặc nhiều thiết bị 108 thông qua kênh truyền thông. Có thể đánh giá rằng kênh truyền thông 106 có thể bao gồm mạng Internet, mạng nội bộ hoặc sự kết hợp của hai loại mạng này. Thiết bị 108 có thể được đặt lẫn lộn và có thể kết nối với kênh truyền thông 106 bằng phương pháp theo một hoặc nhiều công nghệ khác nhau, ví dụ như PSTN, Ethernet, DSL, ISDN, Wi-Fi, WiMax, 2G, 3G, LTE, 4G, v.v.. Các thiết bị 108 có thể là thiết bị bất kỳ trong số các thiết bị bao gồm máy tính cá nhân để bàn, máy tính xách tay, máy tính bảng cá nhân, thiết bị kỹ thuật số hỗ trợ cá nhân, điện thoại di động, điện thoại thông minh, v.v.. Thiết bị 108 có thể còn bao gồm các hệ thống máy tính dành riêng như được sử dụng trong nhiều ngành nghề khác nhau bao gồm ngân hàng, tài chính, hàng không, du lịch,

an ninh quốc gia, kiểm soát biên giới, năng lượng, giao thông vận tải, bán lẻ và/hoặc viễn thông. Theo đó, các thiết bị có thể bao gồm các thiết bị được tạo cấu hình để hoạt động như là thiết bị điểm bán lẻ. Trong phạm vi của sáng chế, các thiết bị này sẽ được gọi là "các thiết bị tiếp nhận".

Máy chủ 101 cũng có thể giao tiếp trên kênh truyền thông 107 với một hoặc nhiều thiết bị 109. Các thiết bị này có thể bao gồm, ví dụ, thiết bị vô tuyến có thể giao tiếp với máy chủ 101 thông qua trạm cơ sở vô tuyến hoặc bộ định tuyến vô tuyến. Các thiết bị vô tuyến có thể bao gồm dạng thiết bị vô tuyến bất kỳ bao gồm máy tính xác tay, máy tính cá nhân để bàn, thiết bị kỹ thuật số hỗ trợ cá nhân, điện thoại di động, điện thoại thông minh, v.v.. Các thiết bị ngoại vi có thể bao gồm thiết bị có thể giao tiếp trên kênh truyền thông 104 thông qua mạng kết nối hữu tuyến, và có thể bao gồm, ví dụ, máy tính để bàn cũng như các hệ thống máy tính dành riêng cụ thể cho từng ngành như được đề cập ở trên, bao gồm, nhưng không giới hạn ở hệ thống diểm bán lẻ. Trong nội dung của sáng chế, các thiết bị ngoại vi này sẽ được gọi là "các thiết bị xuất trình". Theo một phương án, thiết bị xuất trình cũng có thể được bảo vệ bằng mật khẩu hoặc có thể đòi hỏi sự cấp phép bổ sung từ bên xuất trình để khởi tạo truyền thông. Các thiết bị xuất trình có thể được bố trí rời rạc, và có thể giao tiếp với máy chủ 101 trên kênh truyền thông 107 thông qua nhiều phương tiện chẳng hạn như PSTN, Ethernet, DSL và ISDN. Các thiết bị xuất trình bao gồm các thiết bị vô tuyến có thể giao tiếp với bộ định tuyến 103 theo cách thuộc một hoặc nhiều công nghệ truyền thông vô tuyến, ví dụ như Wi-Fi, WiMax, 2G, 3G, LTE, 4G, v.v.. Kênh truyền thông 107 có thể bao gồm mạng Internet, mạng nội bộ hoặc sự kết hợp của cả hai loại mạng này. Các thiết bị xuất trình được tạo cấu hình với ứn dụng tạo thuận lợi cho sự truyền thông với máy chủ 101. Do sự kết nối giữa các thiết bị tiếp nhận 109 và máy chủ 101 bao gồm kênh truyền thông thứ nhất 106 và sự kết nối giữa các thiết bị xuất trình bao gồm kênh truyền thông thứ hai 107, hệ thống 100 có thể được xem là “đa kênh” trong kết cấu. Điều này đảm bảo cho cơ chế đảm mật mà nhờ đó các bộ dữ liệu xác thực và dữ liệu nhạy cảm khác có thể được lưu trữ và phát hành đến điểm nút mạng 110 trong khi vẫn duy trì trạng thái riêng tư. Điểm nút mạng 110 theo một số phương án có thể là thiết bị riêng biệt hoặc chính là thiết bị tiếp nhận phụ thuộc vào mục đích được chỉ định trong sự truyền thông của thiết bị tiếp nhận.

Trong khi theo phương án này, sáng chế bộc lộ rằng các bộ dữ liệu xác thực và

các tên hiệu gắn liền được bao gồm trong bên xuất trình và/hoặc các bản ghi tiếp nhận trên máy chủ, theo phương án khác, rõ ràng là các bộ dữ liệu xác thực nàu và các tên hiệu gắn liền có thể được liên kết với bên xuất trình và/hoặc các bản ghi tiếp nhận theo các cách khác nhau. Ví dụ, các bộ dữ liệu xác thực và các tên hiệu liên kết có thể được bao gồm trong một hoặc nhiều bộ bản ghi phân tách với (các) bộ bản ghi trên máy chủ bao gồm các bản ghi chứa các mã nhận biệt và mã khóa bí mật. Các bộ bản ghi riêng biệt này có thể được chứa trong một hoặc nhiều máy chủ khác nhau. Theo một phương án của sáng chế, các máy chủ khác nhau chứa các bộ dữ liệu xác thực được quản lý bởi các bộ điều khiển chịu trách nhiệm phát hành các dụng cụ chứa các bộ dữ liệu xác thực nêu trên.

Fig.2 là lưu đồ minh họa cách để một bên yêu cầu tiềm năng mới đăng ký với máy chủ 101 là bên xuất trình theo phương án của sáng chế. Ở bước 200, trang web được quản lý bởi máy chủ 101 được người đăng ký là bên xuất trình mới sử truy cập, tốt nhất là sử dụng các thiết bị xuất trình 105, 107, và 109 của chúng. Trang web được tạo cấu hình sao cho ở bước này, người đăng ký là bên xuất trình mới cung cấp các chi tiết đăng ký chung chẳng hạn như tên, địa chỉ, địa chỉ email, nơi cư trú, v.v... và trình chúng cho máy chủ 101. Có thể đánh giá rằng trong khi ở một số phương án của sáng chế, các chi tiết đăng ký được cung cấp trực tiếp cho máy chủ 101, theo các phương án khác, các chi tiết đăng ký có thể được cung cấp sơ bộ gián tiếp để xử lý sơ bộ trước khi đi vào chi tiết trong máy chủ 101. Trang web có thể được truy cập qua kết nối trong suốt thời gian của quá trình, hoặc nếu không thì các kết nối bảo mật có thể đơn thuần được sử dụng chỉ nơi thông tin nhạy cảm (ví dụ như bộ dữ liệu xác thực hoặc dữ liệu bổ sung như mã khóa bí mật của bên xuất trình) đang được truyền. Cũng có thể đánh giá rằng cũng có thể có các cách thức khác để đăng ký, ví dụ như theo cách bổ sung mẫu điền thông tin qua thư, fax, v.v..

Sau đó, ở bước 202, tài khoản mới được tạo ra trên máy chủ 101 cho người đăng ký là bên xuất trình. Điều này được thực hiện bằng cách tạo ra bản ghi xuất trình mới trong tập hợp các bản ghi xuất trình. Ở bước 200 hoặc ở bước 202, người đăng ký là bên xuất trình mới được gợi ý lựa chọn và nhập mã khóa bí mật của bên xuất trình mới, mà sau đó được bổ sung vào bản ghi xuất trình của người đăng ký là bên xuất trình mới. Theo các phương án khác của sáng chế, bản ghi xuất trình mới có thể được cung cấp tự động với mã khóa bí mật của bên xuất trình tạm thời, mà sau đó có thể

được người đăng ký là bên xuất trình cập nhật thành mã khóa bí mật của khách hàng. Mã khóa bí mật tạm thời này có thể được cung cấp bằng phương tiện trang web, hoặc tốt nhất là theo con đường kênh truyền thông thứ hai mà có thể bao gồm kiểm truyền thông bất kỳ, bao gồm email, tin nhắn SMS, điện thoại hoặc thư tín. Theo một số phương án của sáng chế, có mục đích bổ sung là cung cấp mã khóa bí mật thay thế ví dụ trong trường hợp quên mã khóa bí mật ban đầu hoặc mã khóa này đã không còn an toàn. Các mã khóa bí mật thay thế này có thể được cung cấp tương tự thông qua dạng truyền thông bất kỳ bao gồm qua website, email, SMS, điện thoại hoặc thư tín.

Ở bước 204, người đăng ký là bên xuất trình mới được gợi ý bổ sung các bộ dữ liệu xác thực cho tài khoản mới được tạo của người đăng ký là bên xuất trình mới. Như được mô tả trước đó, các bộ dữ liệu xác thực này có thể bao gồm nhiều dữ liệu cá nhân và có thể liên quan đến các dụng cụ mang bộ dữ liệu xác thực được phát hành bởi các cơ quan giám sát thương mại hoặc thuộc chính phủ khác nhau. Mỗi bộ dữ liệu xác thực sẽ được kết nối với tên hiệu duy nhất với bản ghi xuất trình ban đầu của nó (tức là, mỗi tên hiệu "duy nhất mang tính cục bộ"). Theo một phương án, người đăng ký là bên xuất trình mới có thể được gợi ý ở bước 206 để cung cấp tên hiệu duy nhất mang tính cục bộ cho mỗi bộ dữ liệu xác thực được cung cấp. Theo phương án khác, tên hiệu mặc định có thể được cung cấp cho mỗi bộ dữ liệu xác thực. Theo một phương án, các tên hiệu có thể hiệu chỉnh được về sau bởi bên xuất trình. Theo một số phương án của sáng chế, bản ghi xuất trình có thể hiệu chỉnh được sau khi đăng ký đến mức các bộ dữ liệu xác thực và các tên hiệu gắn liền hiện có có thể được chỉnh sửa hoặc xóa và/hoặc các bộ dữ liệu xác thực và các tên hiệu gắn liền mới có thể được bổ sung. Theo một số phương án của sáng chế, bản ghi của bên tương tác xuất trình có thể chỉnh sửa được sau khi đăng ký đến mức các bộ dữ liệu xác thực và các tên hiệu gắn liền hiện có có thể được chỉnh sửa hoặc xóa và các bộ dữ liệu xác thực và các tên hiệu gắn liền mới có thể được bổ sung.

Ở bước 206, người đăng ký là bên xuất trình mới được trao cơ hội để đặt các sự ưu tiên cụ thể được kết hợp với quá trình xử lý và việc sử dụng các bộ dữ liệu xác thực kết hợp với các cơ quan giám sát chính phủ hoặc thương mại cụ thể và các kiểu tương tác mà chúng liên quan. Ví dụ, đối với bộ dữ liệu xác thực liên quan đến khách hàng thân thiết của hãng hàng không, bên xuất trình có thể được trao quyền lựa chọn để đặt các ưu tiên bổ sung theo sự ưu tiên thành viên của họ, ví dụ như bữa ăn ưu thích, tham

khảo chỗ ngồi hoặc sân bay địa phương. Theo ví dụ khác, đối với bộ dữ liệu xác thực liên quan đến thẻ tín dụng, bên xuất trình có thể được trao lựa chọn cho phép các chức năng như sử dụng ưu tiên thẻ, chuyển tiền trực tiếp, hoàn thuế giá trị gia tăng cho khách du lịch hoặc chia nhỏ thanh toán trên nhiều thẻ.

Ở bước 208, người đăng ký là bên xuất trình mới sau đó được gợi ý cài đặt ứng dụng chuyên trên thiết bị xuất trình của họ. Ứng dụng chuyên biệt được thiết kế để tạo thuận lợi cho sự giao tiếp với máy chủ như được yêu cầu trong quá trình xử lý cho phép máy chủ phát hành bộ dữ liệu xác thực và quá trình xác thực như cho phép truyền như sẽ được mô tả chi tiết hơn dưới đây. Trong quá trình cài đặt ứng dụng chuyên biệt, ứng dụng được kết hợp với mã nhận biết bên xuất trình duy nhất được giữ trên thiết bị xuất trình. Theo phương án ưu tiên, mã nhận biết bên xuất trình được máy chủ ấn định, và được nhúng trong ứng dụng trước đó, trong khi hoặc sau khi ứng dụng được cài đặt trên thiết bị xuất trình. Ngoài ra, mã nhận biết bên xuất trình có thể được xuất phát từ chuỗi ký tự riêng của thiết bị xuất trình, ví dụ, số IMEI hoặc số seri. Chuỗi ký tự này có thể được sửa đổi để đạt được mã nhận biết bên xuất trình duy nhất. Bên cạnh sự duy trì trên thiết bị xuất trình, mã nhận biết bên xuất trình cũng được bổ sung vào bản ghi xuất trình trong tập hợp bản ghi xuất trình trên máy chủ 101. Trong quá trình cài đặt ứng dụng chuyên biệt, ứng dụng cũng được cung cấp với các tên hiệu được kết nối với các bộ dữ liệu xác thực được lưu trong bước 204 cho bên xuất trình đã cho. Theo đó, khi ứng dụng được sử dụng trong tương tác bởi bên xuất trình mới, có khi cả mã nhận biết bên xuất trình và các tên hiệu được kết nối với các bộ dữ liệu xác thực của bên xuất trình sao cho mã nhận biết bên xuất trình và tên hiệu có thể được truyền thông với máy chủ 101 là phù hợp.

Theo phương án ưu tiên, phiên bản chung của ứng dụng có thể được cài đặt ban đầu trên thiết bị xuất trình của người đăng ký là bên xuất trình mới. Tiếp theo quy trình được mô tả trong các bước 200-208, người đăng ký là bên xuất trình mới có thể được gợi ý để xác thực tài khoản của chúng bằng cách trả lời email, và/hoặc bằng cách xác nhận mã khóa bí mật của bên xuất trình khi trả lời gợi ý từ máy chủ. Tiếp theo bước xác thực này, phiên bản chung của ứng dụng trên thiết bị xuất trình của người đăng ký là bên xuất trình mới có thể được tùy chỉnh với mã nhận biết bên xuất trình của người đăng ký là bên xuất trình mới, các tên hiệu được kết nối với các bộ dữ liệu xác thực của người đăng ký là bên xuất trình mới, và các ưu tiên của người đăng ký là

bên xuất trình mới như được tạo cấu hình trong bước 206. Dữ liệu này có thể được lưu trong định dạng mã hóa trên thiết bị xuất trình của người đăng ký là bên xuất trình mới. Fig.3 là lưu đồ tương tự với lưu đồ trên Fig.2 mô tả các bước thông qua đó một bên có thể đăng ký là bên tiếp nhận với máy chủ 101 theo phương án của sáng chế. Như được chỉ rõ trước đây, sáng chế dự trù các phương án mà bên tiếp nhận phải tích cực đăng ký với máy chủ, cũng như các phương án mà không cần thiết để bên tiếp nhận đăng ký với máy chủ. Ngoài ra, theo các phương án khác của sáng chế, việc đăng ký của bên tiếp nhận có thể được thực hiện "một cách bị động" như sẽ được mô tả chi tiết hơn dưới đây. Ở bước 300, trang web được điều hành bởi máy chủ 101 được một bên (sau đây được gọi là "người đăng ký là bên tiếp nhận mới") truy cập, tốt nhất là sử dụng thiết bị tiếp nhận 111. Theo cách thức tương tự với bước 200 trên Fig.2, trang web được xây dựng sao cho ở bước này, người đăng ký là bên tiếp nhận mới cung cấp các chi tiết đăng ký chung chung chẳng hạn như tên của cá nhân hoặc tổ chức, địa chỉ, địa chỉ email, v.v... và trình các chi tiết này cho máy chủ 101. Trang web có thể được truy cập trên sự kết nối đảm bảo trong suốt giá trình, hoặc nếu không thì các sự sự kết nối đảm bảo có thể được sử dụng đơn thuần chỉ khi thông tin nhạy cảm (ví dụ như mã khóa bí mật của bên tiếp nhận hoặc bộ dữ liệu xác thực của bên tiếp nhận) được truyền. Còn có thể đánh giá rằng việc đăng ký của người đăng ký là bên tiếp nhận mới có thể diễn ra theo cách của các phương tiện khác như mail hoặc fax. Ngoài ra, nếu bên tiếp nhận vận hành thiết bị tiếp nhận được điều khiển từ xa bởi bên thứ ba được kết nối (ví dụ như Hệ thống quản lý đầu cuối được sử dụng bởi Bên thu lợi để quản lý thiết bị điểm bán thanh toán qua thẻ), việc đăng ký của bên tiếp nhận có thể được khởi tạo bởi bên thứ ba được kết nối. Theo các kịch bản này, có thể không cần thiết để bên tiếp nhận cung cấp thông tin bất kỳ nào của họ.

Ở bước 302, tài khoản mới được tạo ra trên máy chủ 101 bằng cách tạo ra bản ghi người đăng ký là bên tiếp nhận mới trong tập hợp các bản ghi tiếp nhận.

Để bố trí bộc lộ bộ dữ liệu xác thực của bên xuất trình, sự cấp phép phải được cho như được mô tả thêm dưới đây, theo một phương án của sáng chế, sự cấp phép bất kỳ bắt nguồn từ bên tiếp nhận để đưa ra bộ dữ liệu xác thực của bên xuất trình sẽ đòi hỏi là bên tiếp nhận được nhận biết, và do đó, sự cấp phép bất lỳ để đưa ra bộ dữ liệu xác thực của bên xuất trình có thể đòi hỏi sự cung cấp ban đầu bộ dữ liệu xác thực của bên tiếp nhận. Theo đó, có dự tính là cũng như các bản ghi xuất trình, bộ dữ liệu xác

thực của bên tiếp nhận riêng biệt được đòi hỏi trong bản ghi tiếp nhận đối với mỗi loại tương tác mà bên tiếp nhận muốn tham gia. Các kiểu tương tác có thể được định nghĩa rộng, ví dụ, việc phát hành công cụ giấy phép lái xe và phát hành công cụ thẻ thanh toán có thể được xem là các kiểu tương tác khác nhau. Ngoài ra, các kiểu tương tác có thể được định nghĩa hẹp, ví dụ, việc phát hành các công cụ thẻ thanh toán khác nhau (ví dụ, thẻ Mastercard, thẻ Visa Debit) có thể được xem là các kiểu tương tác khác nhau. Theo đó, trong khi ở một số phương án, ví dụ, bộ dữ liệu xác thực của bên tiếp nhận có thể áp dụng chung cho tất cả các thẻ thanh toán, theo các phương án khác, bên tiếp nhận có thể có bộ dữ liệu xác thực riêng cho mỗi kiểu thẻ thanh toán riêng được quản lý bởi bên tiếp nhận.

Ở bước 306, người đăng ký là bên tiếp nhận mới được trao cơ hội để đặt sự ưu tiên cụ thể được kết hợp với các kiểu tương tác cụ thể. Ví dụ, đối với bộ dữ liệu xác thực liên quan đến thẻ tín dụng, người đăng ký là bên tiếp nhận mới có thể được cấp lựa chọn để chỉ ra liệu họ có muốn cung cấp các chức năng theo sau được kết hợp với bộ dữ liệu xác thực ngay khi bộ dữ liệu xác thực của bên tiếp nhận đã được phát hành, chẳng hạn như, chuyển đổi tiền tệ trực tiếp, hoàn thuế giá trị gia tăng cho khách du lịch hoặc chia nhỏ thanh toán qua nhiều thẻ.

Ở bước 308, thiết bị tiếp nhận sau đó được tạo cấu hình sao cho nó có thể giao tiếp với máy chủ. Điều này có thể được thực hiện theo nhiều cách. Theo các phương án của sáng chế, với thiết bị tiếp nhận được điều khiển từ xa bởi bên thứ ba, bên thứ ba có thể khởi tại sự kết cấu lại tự động đối với thiết bị tiếp nhận nếu cần. Theo các phương án khác của sáng chế, người đăng ký là bên tiếp nhận mới có thể khởi tạo sự kết cấu lại thông qua sự cài đặt ứng dụng dành riêng theo cách thức tương tự với cách được mô tả trên Fig.2.

Fig.4 là lưu đồ minh họa phương pháp cho phép phát hành ít nhất một bộ dữ liệu xác thực đã được kiểm soát kết nối với bên xuất trình trong khi vẫn duy trì tính riêng tư liên quan trong các dữ liệu xác thực nêu trên theo phương án của sáng chế. Máy chủ điều khiển nhận thông tin truyền thông thiết bị tiếp nhận chứa mã khóa bí mật và mã khóa chia sẻ một lần và thông tin truyền thông thiết bị xuất trình chứa mã nhận biết bên xuất trình và mã khóa chia sẻ một lần. Ở bước 403, các tin nhắn truyền thông được so sánh. Sự so sánh không thành công làm chấm dứt phương pháp và sự chỉ dẫn tương tác không hoàn tất. Nếu có sự phù hợp mã khóa chia sẻ, ở bước 404, tìm

bản ghi đích trên máy chủ được khởi tạo bằng cách liên kết mã khóa bí mật và mã nhận biết bên xuất trình. Sự dò tìm đối với bản ghi đích bất kỳ bao gồm cùng một mã nhận biết bên xuất trình và mã khóa bí mật như có trong thông tin truyền thông thiết bị tiếp nhận và thông tin truyền thông thiết bị xuất trình. Nếu bản ghi đích được tìm ra, bộ dữ liệu xác thực liên quan đến vị trí lưu trữ hiện có trong bản ghi được tìm thấy và được cho phép để được phát hành cho đích được chỉ định là điểm nút mạng.

Fig.5A và Fig.5B bộc lộ quy trình được thực hiện ở thiết bị tiếp nhận. Mã khóa chia sẻ một lần được tạo ra bởi thiết bị tiếp nhận và được chuyển thành thiết bị xuất trình. Thiết bị tiếp nhận còn nhận mã khóa bí mật của bên xuất trình và tạo ra thông tin truyền thông để được gửi vào máy chủ điều khiển như được mô tả số chỉ 101 trên Fig.1. Thông tin truyền thông nêu trên có chứa mã khóa bí mật của bên xuất trình và mã khóa chia sẻ một lần.

Fig.6A và Fig.6B bộc lộ quy trình được thực hiện ở thiết bị xuất trình. Mã nhận biết bên xuất trình được lấy lại từ bộ nhớ. Ngay khi nhận mã khóa chia sẻ một lần từ thiết bị tiếp nhận, thông tin truyền thông bao gồm mã nhận biết bên xuất trình và mã khóa chia sẻ một lần được truyền tới máy chủ điều khiển 101. Các hình vẽ Fig.7 và Fig.8 là các hình vẽ đại diện cho các mục liên quan đến các dữ liệu xác thực được điều khiển kết nối với bên xuất trình. Mỗi mục được kết hợp với mã nhận biết bên xuất trình và mã khóa bí mật. Các hình vẽ từ Fig.7A đến Fig.7E thể hiện các phương án khác nhau để lưu các bản ghi trên máy chủ điều khiển hoặc máy chủ dữ liệu xác thực 101. Theo một số phương án, các bản ghi của các bên tương tác xuất trình có thể được che và được định vị sử dụng danh sách tìm kiếm như được mô tả trên Fig.7A và Fig.7C. Có thể có phương án khác trong đó mỗi bản ghi tương tác bên xuất trình được kết hợp với một tên hiệu.

Fig.9A và Fig.9B bộc lộ các hình vẽ đại diện bằng đồ thị liên quan đến quy trình truyền thông các tin nhắn ở máy chủ điều khiển từ các bên tương tác hiện tại và các bên tương tác tiếp nhận và quá trình gửi các dữ liệu xác thực được điều khiển đến các đích đến được cấp phép. Fig.10 là sơ đồ chuỗi minh họa quy trình nhờ đó sự cấp phép có thể được cấp theo phương án của sáng chế liên quan đến máy chủ 1001, bên tương tác xuất trình 1002, thiết bị xuất trình 1003, điểm nút mạng 1004, và thiết bị tiếp nhận 1005, để lấy lại bộ dữ liệu xác thực lưu tại vị trí được xác định bởi bên tương tác xuất trình 1002 và phát hành bộ dữ liệu xác thực tới dụng cụ của bên tiếp nhận được

cho phép bởi bên tương tác xuất trình 1002. Có thể đánh giá rằng việc cấp phép để lấy lại và phát hành bộ dữ liệu xác thực của bên xuất trình cũng có thể được kết hợp đồng thời với yêu cầu lấy lại bộ dữ liệu xác thực của bên tiếp nhận, trong đó thiết bị tiếp nhận 1005 và thiết bị xuất trình 1003 vẫn chuyển các thông tin truyền thông tương ứng của chúng tới máy chủ 1001. Cũng có thể đánh giá rằng theo một số phương án của sáng chế, sự cấp phép để phát hành bộ dữ liệu xác thực sẽ đặc biệt là sự cấp phép để phát hành bộ dữ liệu xác thực của bên xuất trình (được kết hợp với bên tương tác xuất trình 1002) tới điểm nút mạng 1004 hoặc tới thiết bị tiếp nhận 1005. Tuy nhiên, theo các phương án khác của sáng chế, sự cấp phép sẽ là để chia sẻ bộ dữ liệu xác thực của bên tiếp nhận hoặc bên xuất trình với bên thứ ba tin cậy được liên kết với điểm nút mạng 1004 hoặc thiết bị tiếp nhận 1005. Ví dụ, khi sự cấp phép được gợi ý để chia sẻ bộ dữ liệu xác thực của bên xuất trình liên quan đến dụng cụ thẻ thanh toán; có thể là nó được dự định để bộ dữ liệu xác thực của thẻ thanh toán được gửi tới bộ xử lý giao dịch của bên thứ ba tin cậy.

Trên Fig.10, bên tương tác xuất trình 1002 xử lý thiết bị xuất trình 1003 được tạo cấu hình để tạo và thông tin truyền thông thiết bị xuất trình tới máy chủ 1001, nhận biết phương tiện hoạt động tại bên tương tác tiếp nhận có chứa điểm nút mạng 1004 hoặc/và thiết bị tiếp nhận 1005 (trong đó điểm nút mạng 1004 là thiết bị tiếp nhận 1005, hoặc trong đó điểm nút mạng 1004 được liên kết với thiết bị tiếp nhận 1005), và nhờ đó thiết bị tiếp nhận được tạo cấu hình để tạo và truyền thông tin truyền thông thiết bị tiếp nhận tới máy chủ 1001. Bên tương tác xuất trình 1002 có thể quyết định tương tác tại phương tiện đó dựa trên việc cho phép đọc bộ dữ liệu xác thực được kết nối với bên tương tác xuất trình 1002 để được phát hành tới điểm nút mạng 1004 hoặc thiết bị tiếp nhận 1005. Bên tương tác tiếp nhận cũng có thể quyết định tương tác tại phương tiện đó dựa trên yêu cầu đọc bộ dữ liệu xác thực được kết nối với bên tương tác tiếp nhận để được đưa trở lại điểm nút mạng 1004 hoặc thiết bị tiếp nhận 1005 khi nhận bộ dữ liệu xác thực được kết nối với bên tương tác xuất trình 1002 tại điểm nút mạng 1004 hoặc thiết bị tiếp nhận 1005. Cụ thể hơn, trạng thái riêng tư thường thấy trong các dữ liệu xác thực được kết nối với bên tương tác xuất trình 1002 được bảo tồn theo phương án ưu tiên của sáng chế, nhờ đó việc đọc bộ dữ liệu xác thực được kết nối với bên tương tác xuất trình 1002 là không có thể nhìn thấy hoặc truy cập được bởi bên tương tác tiếp nhận cũng không được truyền thông với hoặc bởi thiết bị xuất trình

1003, mà chỉ được truyền thông kín đáo với điểm nút mạng 1004 hoặc thiết bị tiếp nhận 1005.

Trên Fig.10, và ở tình huống 1010, tín hiệu được chuyển đi tại điểm nút mạng 1004 hoặc thiết bị tiếp nhận 1005 tới bên tương tác xuất trình 1002, chỉ rõ rằng phương pháp được đề xuất theo sáng chế là phương pháp hiện dùng tại điểm nút mạng 1004 hoặc thiết bị tiếp nhận 1005 cho bên tương tác xuất trình 1002, nhờ đó điểm nút mạng 1004 được trang bị với thiết bị tiếp nhận 1005 và trong đó thiết bị tiếp nhận 1005 đó được tạo cấu hình để truyền thông với máy chủ 1001. Về hiệu quả, phương pháp được đề xuất theo sáng chế là một trong số các phương pháp hiện dùng tại điểm nút mạng 1004 để thu được các dữ liệu xác thực từ bên tương tác xuất trình 1002

Trên Fig.10, và ở tình huống 1011, bên tương tác xuất trình 1002 quyết định khởi tạo tương tác tại phương tiện được vận hành tại bên tương tác tiếp nhận theo quy trình của phương pháp được đề xuất bởi sáng chế bằng cách tạo sẵn thiết bị xuất trình 1003 được tạo cấu hình để tạo và truyền thông tin truyền thông thiết bị xuất trình tới máy chủ 1001, và tạo sẵn thiết bị tiếp nhận 1005, được tạo cấu hình để tạo và truyền thông tin truyền thông thiết bị tiếp nhận tới máy chủ 1001. Về hiệu quả, bên tương tác xuất trình 1002 lựa chọn khởi tạo tương tác tại phương tiện của bên tương tác tiếp nhận theo quy trình của phương pháp được đề xuất bởi sáng chế, từ chối khởi tạo tương tác tại phương tiện được vận hành ở bên tương tác tiếp nhận theo quy trình khác của các phương pháp đã có sẵn có tại điểm nút mạng 1004 để thu được các dữ liệu xác thực từ bên tương tác xuất trình 1002.

Ở giai đoạn 1012, tương tác được khởi tạo bằng cách kích hoạt thiết bị tiếp nhận 1005 được tạo cấu hình để tạo thuân lợi cho việc truyền thông các thông tin truyền thông thiết bị tiếp nhận với máy chủ 1001. Khi kích hoạt ở giai đoạn 1012, mã khóa chia sẻ một lần được đưa ra tại thiết bị tiếp nhận 1005. Theo một phương án của giai đoạn 1012, mã khóa chia sẻ được tạo ra bởi máy chủ 1001 và được truyền đến thiết bị tiếp nhận 1005. Theo phương án khác của giai đoạn 2012, mã khóa chia sẻ được tạo ra ở thiết bị tiếp nhận 1005.

Ở giai đoạn 1013, tương tác được khởi tạo bằng cách kích hoạt thiết bị xuất trình 1003 để tạo thuận lợi cho việc truyền thông các thông tin truyền thông thiết bị xuất trình với máy chủ 1001. Khi kích hoạt ở giai đoạn 1013, mã nhận biết bên xuất

trình được nhận từ vị trí lưu trữ trên thiết bị xuất trình 1003. Theo một phương án của giai đoạn 1013, danh sách các tên hiện kết hợp với các dữ liệu xác thực kết nối với bên tương tác xuất trình 1002 liên quan đến mã nhận biết bên xuất trình cũng được lấy lại từ một số vị trí lưu trữ trên thiết bị xuất trình 1003. Theo phương án của giai đoạn1012, danh sách các tên hiệu này kết hợp với các dữ liệu xác thực được kết nối với bên tương tác xuất trình được phân loại trên thiết bị xuất trình 1003 cho sự lựa chọn mã nhận biết bên xuất trình 1002.

Ở giai đoạn 1014, mã khóa chia sẻ được hoàn lại sẵn sàng tại thiết bị tiếp nhận 1005 cho bên tương tác xuất trình 1002 và thiết bị xuất trình 1003. Theo một phương án của giai đoạn 1014, mã khóa này là mã được hoàn lại cho người sử dụng có thể đọc được tại thiết bị tiếp nhận 1005. Theo phương án khác của giai đoạn 1014, mã khóa này là mã được hoàn lại có thể đọc được bằng máy tại thiết bị tiếp nhận 1005.

Ở giai đoạn 1015, mã khóa chia sẻ thu được tại thiết bị xuất trình 1003. Theo một phương án của giai đoạn 1015, mã khóa này được thu bằng cách đọc tại thiết bị tiếp nhận 1005 và nhập vào thiết bị xuất trình 1003. Theo phương án khác của giai đoạn 1015, mã khóa này được thu bằng cách quét tại thiết bị tiếp nhận 1005 và chụp ảnh trên thiết bị xuất trình 1003. Theo một phương án, thiết bị tiếp nhận 1005 truyền mã khóa chia sẻ một lần trực tiếp tới thiết bị xuất trình 1003, trong khi theo phương án khác, thiết bị tiếp nhận 1005 làm cho mã khóa chia sẻ sẵn sàng với bên tương tác xuất trình 1002, người nhập mã này vào thiết bị xuất trình 1003 ở giai đoạn 1016. Theo một số phương án của sáng chế, thời hạn hiệu lực có thể được ấn định cho mã khóa chia sẻ. Điều này đảm bảo rằng nếu thông tin truyền thông thiết bị tiếp nhận nhận được và thông tin truyền thông thiết bị xuất trình nhận được không được chứng thực trong khoảng thời gian nhất định bằng cách tìm để phối chọn mã khóa chia sẻ một lần (như sẽ được mô tả rõ hơn dưới đây) trong khoảng thời gian nhất định (thời hạn hiệu lực), thì sự tương tác có thể bị bỏ lỡ và từ đó trở nên mất giá trị để thực hiện các quy trình sau đó. Khi hết thời hạn hiệu lực của mã khóa chia sẻ, mã khóa chia sẻ giống thế có thể được sử dụng lại trong tương tác sau đó của phương pháp. Theo đó, thời hạn hiệu lực có thể đảm bảo có thể sử dụng các mã khóa bí mất ngắn hơn và ít phức tạo vì nhờ đó sự tái sử dụng mã khóa chia sẻ là khả thi. Đây là lợi ích đạt được theo các phương án của sáng chế khi cần thiết để bên tương tác xuất trình nhập mã khóa chia sẻ vào thiết bị xuất trình, do độ phức tạp của mã khóa được giảm xuống làm cho phương án

này có thể quản lý dễ dàng hơn.

Theo một số phương án, thiết bị xuất trình cũng có thể hiển thị danh sách các tên hiệu liên quan đến các bộ dữ liệu xác thực bên xuất trình khác nhau được kết nối với bên tương tác xuất trình. Sau đó, bên tương tác xuất trình lựa chọn tên hiệu kết hợp với bộ dữ liệu xác thực mong muốn được kết nối với bên tương tác xuất trình.

Ở giai đoạn 1016, thiết bị tiếp nhận tìm để thu được mã khóa bí mật của bên tương tác xuất trình bằng cách gợi ý bên tương tác xuất trình 1002 nhập mã khóa bí mật của bên xuất trình trên thiết bị tiếp nhận 1 005. Theo một phương án, thiết bị tiếp nhận 1005 có thể hiển thị bổ sung tham số phụ định trước ở giai đoạn 1012 cho bên tương tác xuất trình 1002 để phối hợp sự tương tác và chứng thực thông tin truyền thông thiết bị tiếp nhận và thông tin truyền thông thiết bị xuất trình.

Ở giai đoạn 1017, mã khóa bí mật thu được bằng thiết bị tiếp nhận 1005. Theo một phương án, bên tương tác xuất trình 1002 sử dụng bàn phím để nhập mã khóa bí mật trên thiết bị tiếp nhận 1005. Theo phương án khác, bên tương tác xuất trình 1002 có thể sử dụng thiết bị để chuyển mã khóa bí mật tới thiết bị tiếp nhận 1005.

Ở giai đoạn 1019, thiết bị tiếp nhận 1005 sau đó truyền thông tin truyền thông thiết bị tiếp nhận tới máy chủ 1001 cho phép phát hành (các) bộ dữ liệu xác thực cụ thể được kết nối với bên tương tác xuất trình 1003 tới phương tiện của bên tiếp nhận được cấp phép bởi bên tương tác xuất trình 1002. Thông tin truyền thông thiết bị tiếp nhận chứa mã khóa bí mật của bên xuất trình như đã thu được ở giai đoạn 1017 và mã khóa chia sẻ một lần như được tạo ra ở giai đoạn 1012. Thông tin truyền thông thiết bị tiếp nhận cũng có thể chứa mã nhận biết liên quan đến bên tương tác tiếp nhận nếu được lấy lại tiếp sau giai đoạn 1012 và các tham số phụ định trước bất kỳ nếu được chụp sau giai đoạn 1012.

Ở giai đoạn 1018, thiết bị xuất trình 1003 truyền thông tin truyền thông thiết bị xuất trình tới máy chủ 1001 cho phép lấy lại (các) bộ dữ liệu xác thực cụ thể được kết nối với bên tương tác xuất trình 1002, trong bộ nhớ ở vị trí được xác định bởi bên tương tác xuất trình 1002. Thông tin truyền thông thiết bị xuất trình chứa mã nhận biết bên xuất trình lấy lại được ở giai đoạn 1013 và mã khóa chia sẻ một lần thu được ở giai đoạn 1015. Thông tin truyền thông thiết bị xuất trình cũng có thể chứa tên hiệu kết hợp với bộ dữ liệu xác thực được chọn nếu được phân loại ở giai đoạn 1013 và được

lựa chọn ở giai đoạn 1016, và cũng có thể chứa các tham số phụ định trước bất kỳ nếu được chụp sau giai đoạn 1016.

Ở giai đoạn 1020, máy chủ 1001 tìm để phối chọn các thông tin truyền thông thiết bị tiếp nhận nhận được và các thông tin truyền thông thiết bị xuất trình nhận được bằng cách tìm để phối chọn mã khóa chia sẻ một lần có trong các thông tin truyền thông thiết bị tiếp nhận và mã khóa chia sẻ một lần có trong các thông tin truyền thông thiết bị xuất trình. Theo một số phương án của giai đoạn 1020, thông tin truyền thông thiết bị tiếp nhận và/hoặc thông tin truyền thông thiết bị xuất trình có thể được ấn định thời hạn hiệu lực 1020. Nếu các thông tin truyền thông thiết bị tiếp nhận và thông tin truyền thông thiết bị xuất trình không được phối chọn trong thời hạn hiệu lực được chỉ định, tương tác bị bỏ lỡ và được coi là mất giá trị để thực hiện các quy trình sau đó. Trong trường hợp tương tác bị bỏ lỡ và trở nên mất giá trị để thực hiện các quy trình sau đó, dữ liệu liên quan đến sự tương tác (tức là các thông tin truyền thông bên tương tác) có thể được loại bỏ khỏi hệ thống, mở thông các tài nguyên để xử lý các cấp phép nhận được sau. Theo các phương án khác của giai đoạn 1020, giá trị hoặc các tham số phụ định trước có thể được bao gồm trong thông tin truyền thông thiết bị tiếp nhận ở giai đoạn 1019 và thông tin truyền thông thiết bị xuất trình ở giai đoạn 1018. Nếu vậy, giá trị được sử dụng bên cạnh mã khóa chia sẻ dưới dạng tham số phụ định trước để tìm sự phù hợp của thông tin truyền thông thiết bị tiếp nhận và thông tin truyền thông thiết bị xuất trình trong giai đoạn 1020.

Ở giai đoạn 1021, và trong tình huống phát hiện sự phù hợp ở giai đoạn 1020, máy chủ 1001 khởi tạo tìm kiếm bằng cách liên kết mã nhận biết xuất trình có trong thông tin truyền thông thiết bị xuất trình và mã khóa bí mật có trong thông tin truyền thông thiết bị tiếp nhận, trong đó mã khóa chia sẻ có trong thông tin truyền thông thiết bị xuất trình là giống với mã khóa chia sẻ có trong thông tin truyền thông thiết bị tiếp nhận theo giai đoạn 1020. Nếu không tìm thấy sự phù hợp ở giai đoạn 1020, phương pháp không tiếp tục với giai đoạn 1021, và máy chủ 1001 có thể hoàn lại tin nhắn theo thiết bị tiếp nhận 1005 hoặc thiết bị xuất trình 1003.

Ở giai đoạn 1022, máy chủ 1001 tiến hành tìm kiếm đối với bản ghi đích thuộc tập hợp các bản ghi xuất trình có chứa mã nhận biết bên xuất trình có trong thông tin truyền thông thiết bị xuất trình phù hợp và mã khóa bí mật có trong thông tin truyền thông thiết bị tiếp nhận phù hợp. Theo một phương án về giai đoạn 1022, và trong

trường hợp tên hiệu kết hợp với mã nhận biết bên xuất trình là có trong thông tin truyền thông thiết bị xuất trình theo giai đoạn 1018, tên hiệu cũng được sử dụng để xác định bản ghi đích có chứa tên hiệu bên cạnh mã nhận biết bên xuất trình và mã khóa bí mật của bên tương tác xuất trình 1002.

Ở giai đoạn 1023, và trong trường hợp bản ghi có chứa mã nhận biết bên xuất trình và mã khóa bí mật của bên xuất trình được định vị ở giai đoạn 1022, tìm kiếm được tiếp tục bằng cách xác định mục liên kết với bản ghi đích được định vị ở giai đoạn 1022, trong đó mục liên quan đến bộ dữ liệu xác thực được kết nối với bên tương tác xuất trình 1002. (Theo một phương án, bộ dữ liệu xác thực liên quan có thể là bộ dữ liệu xác thực được kết nối với tên hiệu được chọn bởi bên tương tác xuất trình ở giai đoạn 1022). Theo một phương án, mục được xác định chứa nội dung đọc bao gồm các dữ liệu xác thực được kết nối với bên tương tác xuất trình 1002. Theo phương án khác, mục được xác định chứa diểm con trỏ định vị các dữ liệu xác thực được kết nối với bên tương tác xuất trình 1002. Trong trường hợp bản ghi có chứa mã nhận biết bên xuất trình và mã khóa bí mật của bên xuất trình không được định vị ở giai đoạn 1022, quy trình do đó không tiếp tục với giai đoạn 1023 và máy chủ 1001 có thể hoàn lại tin nhắn theo thiết bị tiếp nhận 1005 hoặc/và thiết bị xuất trình 1003.

Ở giai đoạn 1024, tìm kiếm được hoàn tất bằng cách cho phép lấy lại nội dung đọc các dữ liệu xác thực được kết nối với bên tương tác xuất trình 1002 trong bộ nhớ ở vị trí được xác định trong giai đoạn 1023, và cho phép phát hành nội dung đọc của các dữ liệu xác thực được kết nối với bên tương tác xuất trình tới phương tiện của bên tiếp nhận được cho phép bởi bên tương tác xuất trình 1002.

Ở giai đoạn 1025, nội dung đọc được lấy lại từ bộ nhớ ở vị trí được xác định bởi bên tương tác xuất trình 1002. Theo một phương án, nội dung đọc được lưu và lấy lại ở giai đoạn 1025 tại máy chủ điều khiển được tạo cấu hình để thực hiện phương pháp được đề xuất trong các giai đoạn từ 1020 đến 1024. Theo phương án khác, nội dung đọc được lưu và lấy lại ở giai đoạn 1025 ở máy chủ khác tách biệt với máy chủ điều khiển được tạo cấu hình để thực hiện phương pháp được đề xuất trong các giai đoạn từ 1020 đến 1024.

Ở giai đoạn 1026, nội dung đọc của các dữ liệu xác thực được phát hành cho phương tiện của của bên tiếp nhận được cho phép bởi bên tương tác xuất trình 1002.

Theo một phương án về giai đoạn 1026, nội dung đọc được phát hành và gửi tới điểm nút mạng 1004. Theo phương án khác về giai đoạn 1026, nội dung đọc được phát hành và gửi đến thiết bị tiếp nhận 1005.

Trên Fig.10, và do các tình huống sau đó ở các giai đoạn 1027 và 1028, tin nhắn được quay lại bởi máy chủ 1001 tới thiết bị xuất trình 1003 để bên tương tác xuất trình 1002 chỉ ra nếu nội dung đọc được lấy lại như dược xác định và phát hành như được cho phép bởi bên tương tác xuất trình 1002; theo các phương án thay thế này, bản ghi được lấy lại tại máy chủ 1001 liệt kê trạng thái của các tình huống xuất hiện giữa giai đoạn 1020 và 1024, và có thể thấy được đối với bên tương tác xuất trình 1002 ở thiết bị xuất trình 1003.

Các phương án của sáng chế đã được mô tả dựa trên các hình vẽ bao gồm thiết máy tính và/hoặc các quy trình được thực hiện trong thiết bị máy tính. Tuy nhiên, sáng chế cũng mở rộng sang các chương trình máy tính, cụ thể là các chương trình máy tính được lưu trên hoặc vật mang được làm thích ứng để áp dụng sáng chế vào ứng dụng trong thực tế. Chương trình có thể ở dạng mã nguồn, mã đối tượng hoặc mã nguồn trung gian và mã đối tượng, ví dụ như ở dạng kết hợp một phần hoặc ở dạng bất kỳ thích hợp để sử dụng trong việc thực hiện phương pháp theo sáng chế. Vật mang có thể bao gồm phương tiện lưu trữ chẳng hạn như ROM (bộ nhớ chỉ đọc), ví dụ CD ROM, hoặc phương tiện ghi từ trường, ví dụ đĩa mềm hoặc đĩa cứng. Vật có thể là tín hiệu điện hoặc tín hiệu quang có thể được truyền thông qua cáp điện hoặc cáp quang hoặc bằng các phương tiện vô tuyến hoặc phương tiện khác.

Các từ "có chứa/bao gồm" và các từ "có/chứa" khi được sử dụng ở đây theo sáng chế được sử dụng để mà rõ sự có mặt của các đặc điểm, số, bước hoặc các thành phần đã định nhưng không loại từ sự có mặt hoặc bổ sung của một hoặc nhiều đặc điểm, số, bước thành phần hoặc nhóm khác.

Có thể đánh giá rằng một số đặc điểm nhất định của sáng chế, để làm rõ, được mô tả trong nội dung của các phương án riêng biệt, cũng có thể được cung cấp kết hợp trong một phương án duy nhất. Ngược lại, các đặc điểm khác của sáng chế, để ngắn gọn, được mô tả trong nội dung của một phương án duy nhất, cũng được cung cấp riêng biệt trong sự kết hợp phù hợp bất kỳ.

Yêu cầu bảo hộ

1. Hệ thống (100) cho phép truyền thông ít nhất một bộ dữ liệu xác thực đã được kiểm soát kết nối với bên xuất trình từ máy chủ tới điểm nút mạng, hệ thống bao gồm:

ít nhất một điểm nút mạng;

ít nhất một thiết bị tiếp nhận (109) được tạo cấu hình để gửi thông tin truyền thông thiết bị tiếp nhận (104), thông tin truyền thông thiết bị tiếp nhận này chứa mã khóa bí mật (109a) liên quan đến bên xuất trình nêu trên và mã khóa chia sẻ một lần (109b);

ít nhất một thiết bị xuất trình (108) được tạo cấu hình để gửi thông tin truyền thông thiết bị xuất trình (105), thông tin truyền thông thiết bị xuất trình chứa mã nhận biết bên xuất trình (108a) liên quan đến bên xuất trình và mã khóa chia sẻ một lần (108b);

ít nhất một máy chủ còn bao gồm bộ xử lý, ít nhất một giao diện truyền thông và bộ nhớ lưu trữ ít nhất một mục (103) liên quan đến ít nhất một bộ dữ liệu xác thực đã kết nối và kiểm soát nêu trên, mỗi mục được liên kết với ít nhất một bản ghi (102), bản ghi liên quan đến bên xuất trình bất kỳ và bao gồm mã nhận biết bên xuất trình và mã khóa bí mật gắn liền với mã nhận biết bên xuất trình;

trong đó ít nhất một máy chủ nêu trên được tạo cấu hình để:

a) nhận thông tin truyền thông thiết bị tiếp nhận (104);

b) nhận thông tin truyền thông thiết bị xuất trình (105);

c) tìm để phối chọn mã khóa chia sẻ một lần (109b) có trong thông tin truyền thông thiết bị tiếp nhận (104) với mã khóa chia sẻ một lần (108b) có trong thông tin truyền thông thiết bị xuất trình (105);

d) khởi tạo tìm kiếm đối với bản ghi đích bằng cách liên kết mã khóa bí mật trong thông tin truyền thông thiết bị tiếp nhận (104) với mã nhận biết bên xuất trình trong thông tin truyền thông thiết bị xuất trình (105), cả thông tin truyền thông thiết bị tiếp nhận và thông tin truyền thông thiết bị xuất trình đều chứa cùng một mã khóa chia sẻ một lần (108b, 109b);

e) tiến hành tìm kiếm đối với bản ghi đích nêu trên chứa cả mã khóa bí mật

(109a) và mã nhận biết bên xuất trình (108a);

f) xác định mục (103) được liên kết với bản ghi đích nêu trên;

g) cho phép lấy lại ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát liên quan đến mục (103) nêu trên và cho phép phát hành ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát đến điểm nút mạng (110) nêu trên, điểm nút mạng này là bên tiếp nhận được cấp phép của ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát nêu trên.

2. Hệ thống theo điểm 1, trong đó ít nhất một máy chủ nêu trên bao gồm máy chủ điều khiển (101).

3. Hệ thống theo điểm 2, trong đó máy chủ điều khiển (101) nêu trên còn được tạo cấu hình để tạo ra mã khóa chia sẻ một lần, và làm cho mã này sẵn sàng tại thiết bị tiếp nhận (109)

4. Hệ thống theo điểm 2, trong đó thiết bị tiếp nhận nêu trên còn được tạo cấu hình để tạo ra mã khóa chia sẻ một lần, nhận mã khóa bí mật (109a) từ bên xuất trình nêu trên và truyền thông tin truyền thông thiết bị tiếp nhận tới máy chủ điều khiển (101).

5. Hệ thống theo điểm 3, trong đó thiết bị xuất trình nêu trên còn được tạo cấu hình để nhận mã khóa chia sẻ một lần từ thiết bị tiếp nhận (109), lấy lại mã nhận biết bên xuất trình từ bộ nhớ của nó và truyền thông tin truyền thông thiết bị xuất trình (105) tới máy chủ điều khiển (101).

6. Hệ thống theo điểm bất kỳ trong số các điểm nêu trên, trong đó bản ghi có chứa mã nhận biết bên xuất trình và mã khóa bí mật còn có chứa tên hiệu được kết hợp với mã nhận biết bên xuất trình và được liên kết với mục (103) liên quan đến ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát.

7. Hệ thống theo điểm bất kỳ trong số các điểm nêu trên, trong đó thông tin truyền thông thiết bị xuất trình còn chứa tên hiệu được kết hợp với mã nhận biết bên xuất trình và được liên kết với mục (103) liên quan đến ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát, và trong đó việc tìm kiếm đối với bản ghi đích còn sử dụng tên hiệu có trong thông tin truyền thông thiết bị xuất trình (105) để tìm kiếm đối với bản ghi đích chứa tên hiệu bên cạnh mã nhận biết bên xuất trình (108a) và mã khóa bí

mật.

8. Hệ thống theo điểm bất kỳ trong số các điểm nêu trên, trong đó điểm nút mạng bao gồm thiết bị tiếp nhận (109) và được tạo cấu hình dưới dạng bên tiếp nhận được chỉ định đối với một hoặc nhiều kiểu dữ liệu trong số ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát.

9. Hệ thống theo điểm bất kỳ trong số các điểm từ 1 đến 7, trong đó điểm nút mạng được liên kết với thiết bị tiếp nhận và được tạo cấu hình dưới dạng bên tiếp nhận được chỉ định đối với một hoặc nhiều kiểu dữ liệu trong số ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát.

10. Hệ thống theo điểm 2, trong đó ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát bao gồm mục trong bản ghi đích (102) trên máy chủ điều khiển (101).

11. Hệ thống theo điểm 2, trong đó ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát bao gồm mục trên máy chủ khác của ít nhất một máy chủ được liên kết với bản ghi đích trên máy chủ điều khiển (101).

12. Hệ thống theo điểm bất kỳ trong số các điểm nêu trên, trong đó thời hạn hiệu lực được ấn định cho thông tin truyền thông thiết bị tiếp nhận (104), và trong đó bước c) còn bao gồm thiết lập thời điểm mà thời hạn hiệu lực này hết hạn.

13. Hệ thống theo điểm bất kỳ trong số các điểm từ 1 đến 11, trong đó thời hạn hiệu lực được ấn định cho thông tin truyền thông thiết bị xuất trình (105), và trong đó bước c) còn bao gồm thiết lập thời điểm mà thời hạn hiệu lực này hết hạn.

14. Hệ thống theo điểm bất kỳ trong số các điểm từ 1 đến 11, trong đó thời hạn hiệu lực được ấn định cho mã khóa chia sẻ một lần, và trong đó bước c) còn bao gồm thiết lập thời điểm mà thời hạn hiệu lực này hết hạn.

15. Hệ thống theo điểm 14, trong đó mã khóa chia sẻ một lần là duy nhất trong suốt thời hạn hiệu lực của nó.

16. Hệ thống theo điểm bất kỳ trong số các điểm nêu trên, trong đó thông tin truyền thông thiết bị tiếp nhận (104) còn chứa một hoặc nhiều các tham số phụ định trước, và thông tin truyền thông thiết bị xuất trình cũng còn bao gồm một hoặc nhiều các tham

số phụ định trước nêu trên.

17. Hệ thống theo điểm 16, khi phụ thuộc vào điểm bất kỳ trong số các điểm từ 2 đến 5, trong đó máy chủ điều khiển (101) tìm để phối chọn ít nhất một trong số các tham số phụ định trước nêu trên từ thông tin truyền thông thiết bị xuất trình (105) với (các) tham số phụ định trước tương ứng từ thông tin truyền thông thiết bị tiếp nhận (104) để cung cấp thêm ít nhất một trong hai tình huống: tương quan và chứng thực.

18. Hệ thống theo điểm bất kỳ trong số các điểm từ 2 đến 5, trong đó, nếu các bản ghi nêu trên bao gồm các mục của ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát trên máy chủ điều khiển (101), các bước f) và g) được thực hiện ở máy chủ điều khiển, và sự truyền thông của ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát được thực hiện từ máy chủ điều khiển.

19. Hệ thống theo điểm bất kỳ trong số các điểm từ 2 đến 5, trong đó, nếu các bản ghi nêu trên bao gồm các mục của ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát trên máy chủ khác không phải máy chủ điều khiển, các bước f) và g) được thực hiện ở máy chủ khác nêu trên, và sự truyền thông của ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát được thực hiện sử dụng một trong hai máy chủ bao gồm máy chủ điều khiển nêu trên và máy chủ khác nêu trên.

20. Hệ thống theo điểm bất kỳ trong số các điểm từ 2 đến 5, trong đó, nếu không có sự phù hợp giữa thông tin truyền thông thiết bị tiếp nhận (104) và thông tin truyền thông thiết bị xuất trình (1 05) được tìm thấy tại máy chủ điều khiển (101), máy chủ điều khiển đó kết thúc các hoạt động tạo cấu hình thêm và ghi lại trạng thái đó.

21. Hệ thống theo điểm bất kỳ trong số các điểm từ 2 đến 5, trong đó, nếu không tìm thấy bản ghi đích tại máy chủ điều khiển (101), máy chủ điều khiển đó kết thúc các hoạt động tạo cấu hình thêm và ghi lại trạng thái đó.

22. Hệ thống theo điểm bất kỳ trong số các điểm từ 2 đến 5, trong đó máy chủ điều khiển (101) còn được tạo cấu hình để ghi lại trạng thái của sự kiện xảy ra và chuyển tiếp trạng thái đó tới ít nhất một trong số các thiết bị bao gồm thiết bị tiếp nhận (109) và thiết bị xuất trình (108).

23. Hệ thống theo điểm bất kỳ trong số các điểm nêu trên, trong đó mỗi máy chủ nêu

trên, mỗi điểm nút mạng (110), và mỗi thiết bị trong số các thiết bị xuất trình và tiếp nhận (108, 109) còn bao gồm ít nhất một trong số các bộ phận bao gồm bộ xử lý, các giao diện truyền thông, bộ nhớ, các bảng điều khiển nhập và các bảng điều khiển xuất.

24. Hệ thống theo điểm bất kỳ trong số các điểm nêu trên, trong đó hệ thống có thể vận hành trên mạng truyền thông (106, 107, 111).

25. Phương pháp cho phép sự truyền thông của ít nhất một bộ dữ liệu xác thực đã được kiểm soát kết nối với bên xuất trình từ ít nhất một máy chủ đến điểm nút mạng (110), phương pháp bao gồm các bước được thực hiện tại ít nhất một máy chủ như sau:

(a) nhận thông tin truyền thông thiết bị tiếp nhận (104), thông tin truyền thông này chứa mã khóa bí mật (109a) liên quan đến bên xuất trình và mã khóa chia sẻ một lần (109b);

(b) nhận thông tin truyền thông thiết bị xuất trình (105), thông tin truyền thông này chứa mã nhận biết bên xuất trình (108a) liên quan đến bên xuất trình và mã khóa chia sẻ một lần (108b);

(c) tìm để phối chọn mã khóa chia sẻ một lần (109b) có trong thông tin truyền thông thiết bị tiếp nhận (104) và mã khóa chia sẻ một lần (108b) có trong thông tin truyền thông thiết bị xuất trình (105);

(d) khởi tạo tìm kiếm đối với bản ghi đích bằng cách liên kết mã khóa bí mật (109a) của thông tin truyền thông thiết bị tiếp nhận (104) và mã nhận biết bên xuất trình (108a) trong thông tin truyền thông thiết bị xuất trình (105), cả hai thông tin truyền thông thiết bị tiếp nhận và thông tin truyền thông thiết bị xuất trình đều chứa cùng một mã khóa chia sẻ một lần (1 08b, 109b);

(e) tiến hành tìm kiếm đối với bản ghi đích bao gồm cả hai mã khóa bí mật (109a) và mã nhận biết bên xuất trình (108a);

(f) xác định mục (103) được liên kết với bản ghi đích nêu trên, mục này liên quan đến ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát; và

(g) cho phép lấy lại ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát liên quan đến mục nêu trên và cho phép phát hành bộ dữ liệu xác thực đã được kết nối và kiểm soát đó tới điểm nút mạng (110), điểm nút này là bên tiếp nhận được cấp phép

đối với ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát.

26. Phương pháp theo điểm 25, trong đó bản ghi đích bao gồm mã nhận biết bên xuất trình (108a) và mã khóa bí mật (109a) còn có chứa tên hiệu được kết hợp với mã nhận biết bên xuất trình (108a) và được liên kết với mục (103) liên quan đến ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát, và thông tin truyền thông thiết bị xuất trình (105) còn chứa tên hiệu được kết hợp với mã nhận biết bên xuất trình (108a) và được liên kết với mục nêu trên liên quan đến ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát, và trong đó bước (e) còn bao gồm làm phù hợp các tên hiệu tương ứng của bản ghi nêu trên và thông tin truyền thông thiết bị xuất trình nêu trên.

27. Phương pháp theo điểm 25 hoặc 26, trong đó ít nhất một máy chủ nêu trên bao gồm máy chủ điều khiển (101) và các bước từ (a) đến (g) được thực hiện trên đó.

28. Phương pháp theo điểm 25 hoặc 26, trong đó ít nhất một máy chủ bao gồm máy chủ điều khiển (101) và ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát bao gồm mục trên máy chủ khác với máy chủ điều khiển (101), mục này được liên kết với bản ghi đích nêu trên, và trong đó bước xác định bộ dữ liệu xác thực được thực hiện trên máy chủ khác nêu trên, và trong đó các bước từ (e) đến (g) được thực hiện ở một trong hai máy chủ trong số máy chủ điều khiển (101) và máy chủ khác.

29. Phương pháp theo điểm bất kỳ trong số các điểm từ 25 đến 28, còn bao gồm ấn định thời hạn hiệu lực cho ít nhất một trong số: thông tin truyền thông thiết bị tiếp nhận (104), thông tin truyền thông thiết bị xuất trình (105) và mã khóa chia sẻ một lần, và bước (c) còn bao gồm thiết lập thời điểm mà thời hạn hiệu lực này hết hạn.

30. Phương pháp theo điểm 29, trong đó mã khóa chia sẻ một lần là duy nhất trong suốt thời hạn hiệu lực của nó.

31. Phương pháp theo điểm bất kỳ trong số các điểm từ 25 đến 29, trong đó mỗi thông tin trong số thông tin truyền thông thiết bị xuất trình (105) và thông tin truyền thông thiết bị tiếp nhận (104) còn chứa một hoặc nhiều các tham số phụ định trước, và trong đó bước (c) còn bao gồm bước tìm để phối chọn ít nhất một trong số các tham số phụ định trước nêu trên trong thông tin truyền thông thiết bị xuất trình nêu trên với ít nhất một trong số các tham số phụ định trước tương ứng trong thông tin truyền thông thiết

bị tiếp nhận nêu trên.

32. Phương pháp theo điểm 27, trong đó, nếu các bản ghi nêu trên bao gồm các mục của ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát trên máy chủ điều khiển (101), thực hiện các bước (f) và (g) ở máy chủ điều khiển, và phương pháp còn bao gồm phát hành ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát nêu trên từ máy chủ điều khiển nêu trên.

33. Phương pháp theo điểm 25 hoặc 26, trong đó ít nhất một máy chủ nêu trên bao gồm máy chủ điều khiển (101), và, nếu các bản ghi nêu trên bao gồm các mục của ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát trên máy chủ khác không phải máy chủ điều khiển (101), thực hiện các bước (f) và (g) ở máy chủ khác đó, và phương pháp còn bao gồm phát hành ít nhất một bộ dữ liệu xác thực đã được kết nối và kiểm soát từ một trong số: máy chủ điều khiển và máy chủ khác nêu trên.

34. Phương pháp theo điểm 27 hoặc 28, trong đó, nếu không có sự phù hợp giữa thông tin truyền thông thiết bị tiếp nhận (104) và thông tin truyền thông thiết bị xuất trình (105) được tìm thấy, kết thúc các hoạt động tạo cấu hình thêm và ghi lại trạng thái đó tại máy chủ điều khiển (101).

35. Phương pháp theo điểm 27 hoặc 28, trong đó, nếu không có bản ghi đích nào được tìm thấy, kết thúc các hoạt động tạo cấu hình thêm và ghi lại trạng thái đó tại máy chủ điều khiển (101).

36. Phương pháp theo điểm 27 hoặc 28, còn bao gồm ghi lại trạng thái của các tình huống xảy ra tại máy chủ điều khiển (101) và chuyển tiếp trạng thái đó tới ít nhất một trong số: thiết bị tiếp nhận (109) và thiết bị xuất trình (108).

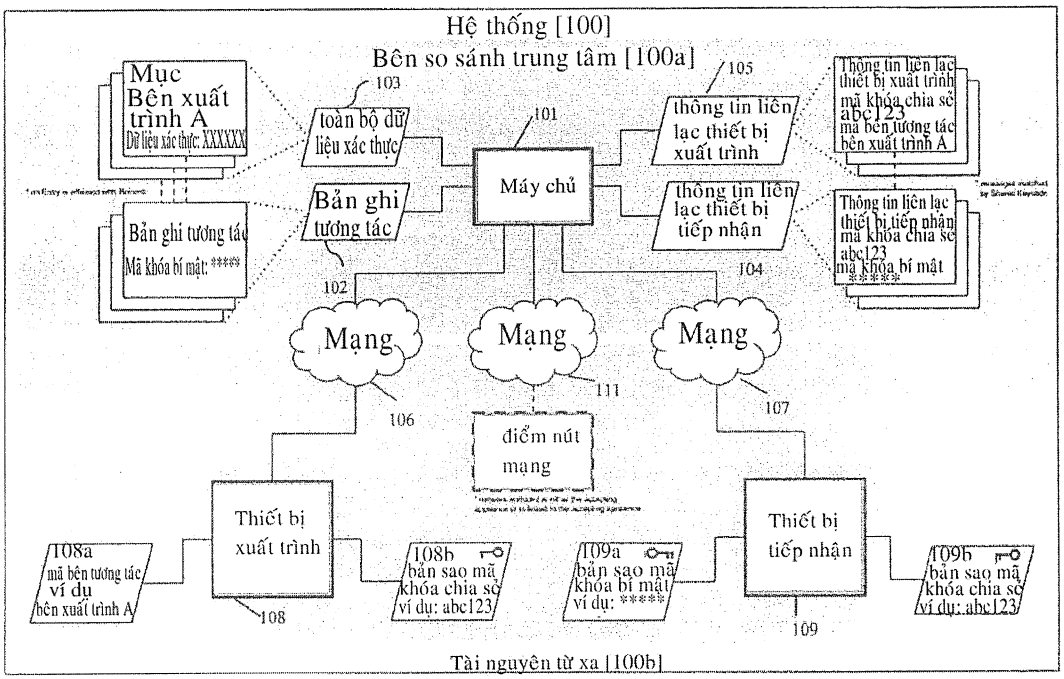

Hệ thống [100]
Bên so sánh trung tâm [100a]
Mục Bên xuất trình A
Dữ liệu xác thực: XXXXXX
Bản ghi tương tác
Mã khóa bí mật: *****
103
toàn bộ dữ liệu xác thực
Bản ghi tương tác
102
101
Máy chủ
105
thông tin liên lạc thiết bị xuất trình
thông tin liên lạc thiết bị tiếp nhận
104
Thông tin liên lạc thiết bị xuất trình mã khóa chia sẻ abc123 mã bên tương tác bên xuất trình A
Thông tin liên lạc thiết bị tiếp nhận mã khóa chia sẻ abc123 mã khóa bí mật *****
Mạng
Mạng
Mạng
106
111
107
điểm nút mạng
Thiết bị xuất trình
108
Thiết bị tiếp nhận
109
108a mã bên tương tác ví dụ bên xuất trình A
108b bản sao mã khóa chia sẻ ví dụ: abc123
109a bản sao mã khóa bí mật ví dụ: *****
109b bản sao mã khóa chia sẻ ví dụ: abc123
Tài nguyên từ xa [100b]

Fig. 1

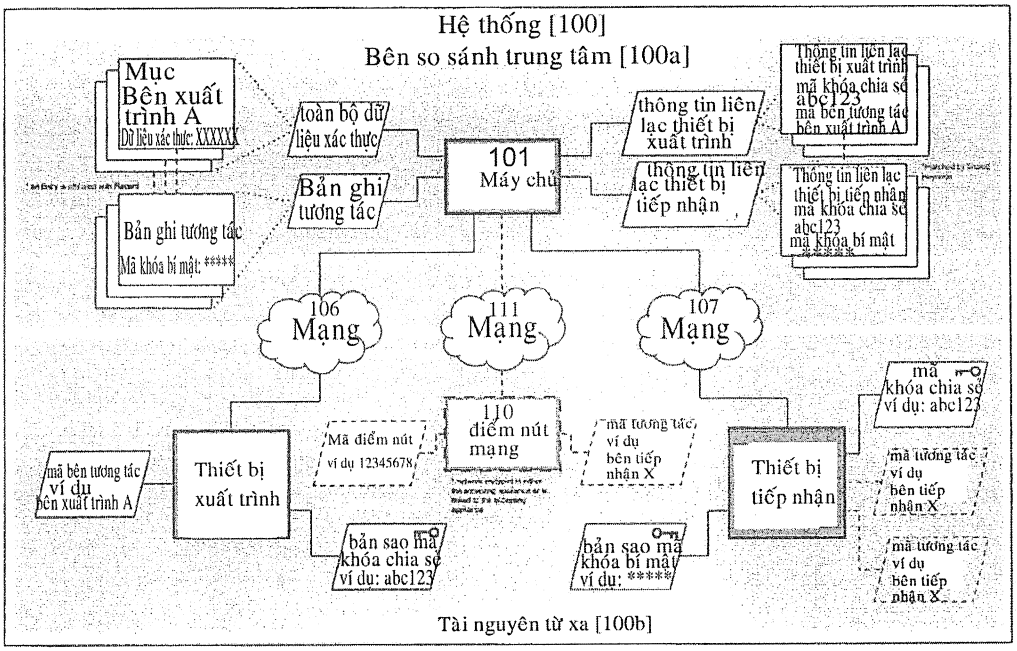

Hệ thống [100]
Bên so sánh trung tâm [100a]
Mục Bên xuất trình A
Dữ liệu xác thực: XXXXX
Bản ghi tương tác
Mã khóa bí mật: *****
toàn bộ dữ liệu xác thực
Bản ghi tương tác
101 Máy chủ
thông tin liên lạc thiết bị xuất trình
thông tin liên lạc thiết bị tiếp nhận
Thông tin liên lạc thiết bị xuất trình
mã khóa chia sẻ abc123
mã bên tương tác bên xuất trình A
Thông tin liên lạc thiết bị tiếp nhận
mã khóa chia sẻ abc123
mã khóa bí mật *****
106 Mạng
111 Mạng
107 Mạng
110 điểm nút mạng
Mã điểm nút ví dụ 12345678
mã tương tác ví dụ bên tiếp nhận X
mã khóa chia sẻ ví dụ: abc123
mã bên tương tác ví dụ bên xuất trình A
Thiết bị xuất trình
Thiết bị tiếp nhận
mã tương tác ví dụ bên tiếp nhận X
bản sao mã khóa chia sẻ ví dụ: abc123
bản sao mã khóa bí mật ví dụ: *****
mã tương tác ví dụ bên tiếp nhận X
Tài nguyên từ xa [100b]

Fig. 1A

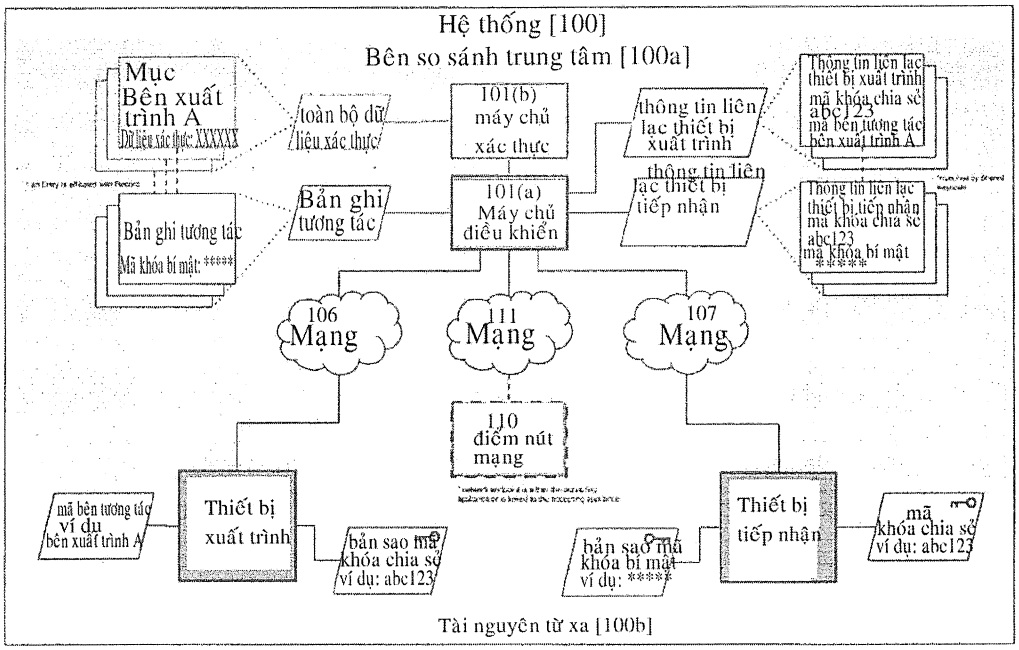

Hệ thống [100]
Bên so sánh trung tâm [100a]
Mục Bên xuất trình A
Dữ liệu xác thực: XXXXX
Bản ghi tương tác
Mã khóa bí mật: *****
toàn bộ dữ liệu xác thực
Bản ghi tương tác
101(b) máy chủ xác thực
101(a) Máy chủ điều khiển
thông tin liên lạc thiết bị xuất trình
thông tin liên lạc thiết bị tiếp nhận
Thông tin liên lạc thiết bị xuất trình
mã khóa chia sẻ abc123
mã bên tương tác bên xuất trình A
Thông tin liên lạc thiết bị tiếp nhận
mã khóa chia sẻ abc123
mã khóa bí mật *****
106 Mạng
111 Mạng
107 Mạng
110 điểm nút mạng
mã bên tương tác ví dụ bên xuất trình A
Thiết bị xuất trình
Thiết bị tiếp nhận
bản sao mã khóa chia sẻ ví dụ: abc123
bản sao mã khóa bí mật ví dụ: *****
mã khóa chia sẻ ví dụ: abc123
Tài nguyên từ xa [100b]

Fig. 1B

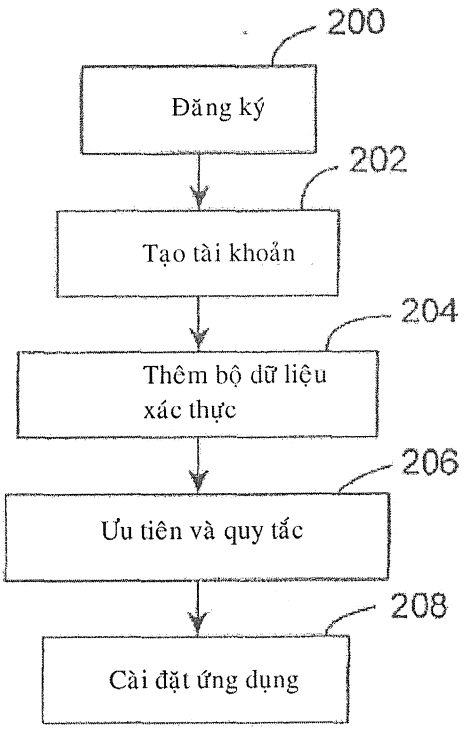

200
Đăng ký
202
Tạo tài khoản
204
Thêm bộ dữ liệu xác thực
206
Ưu tiên và quy tắc
208
Cài đặt ứng dụng

Fig. 2

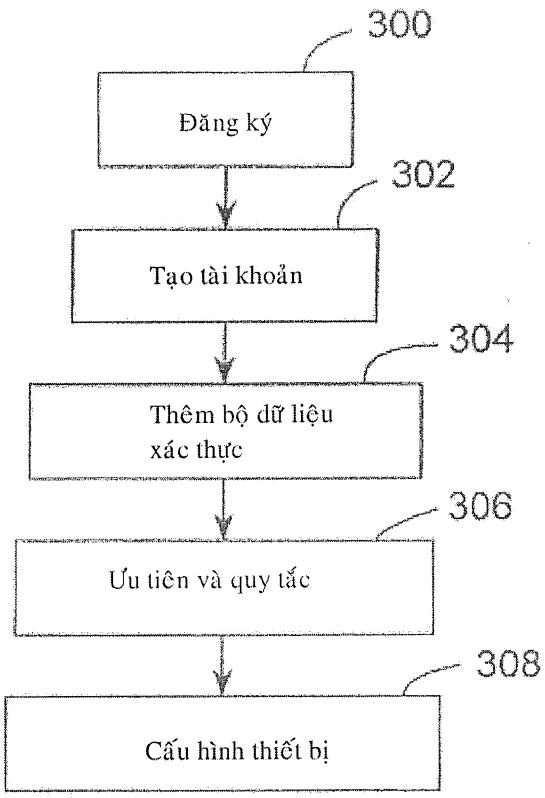

300
Đăng ký
302
Tạo tài khoản
304
Thêm bộ dữ liệu
xác thực
306
Ưu tiên và quy tắc
308
Cấu hình thiết bị

Fig. 3

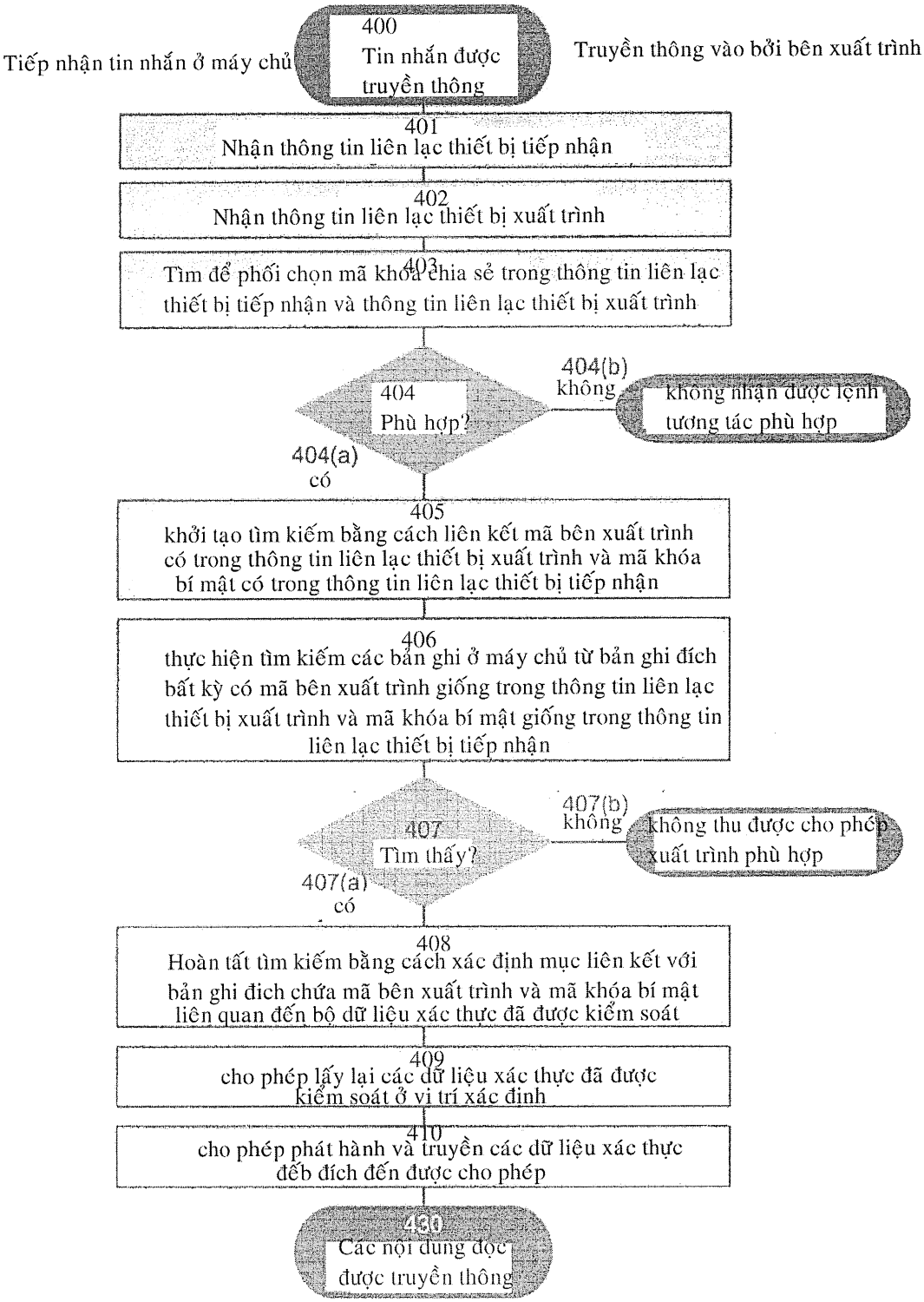

Tiếp nhận tin nhắn ở máy chủ
400
Tin nhắn được truyền thông
Truyền thông vào bởi bên xuất trình
401
Nhận thông tin liên lạc thiết bị tiếp nhận
402
Nhận thông tin liên lạc thiết bị xuất trình
403
Tìm để phối chọn mã khóa chia sẻ trong thông tin liên lạc thiết bị tiếp nhận và thông tin liên lạc thiết bị xuất trình
404
Phù hợp?
404(b)
không
không nhận được lệnh tương tác phù hợp
404(a)
có
405
khởi tạo tìm kiếm bằng cách liên kết mã bên xuất trình có trong thông tin liên lạc thiết bị xuất trình và mã khóa bí mật có trong thông tin liên lạc thiết bị tiếp nhận
406
thực hiện tìm kiếm các bản ghi ở máy chủ từ bản ghi đích bất kỳ có mã bên xuất trình giống trong thông tin liên lạc thiết bị xuất trình và mã khóa bí mật giống trong thông tin liên lạc thiết bị tiếp nhận
407
Tìm thấy?
407(b)
không
không thu được cho phép xuất trình phù hợp
407(a)
có
408
Hoàn tất tìm kiếm bằng cách xác định mục liên kết với bản ghi đích chứa mã bên xuất trình và mã khóa bí mật liên quan đến bộ dữ liệu xác thực đã được kiểm soát
409
cho phép lấy lại các dữ liệu xác thực đã được kiểm soát ở vị trí xác định
410
cho phép phát hành và truyền các dữ liệu xác thực đến đích được cho phép
Các nội dung độc được truyền thông

Fig. 4

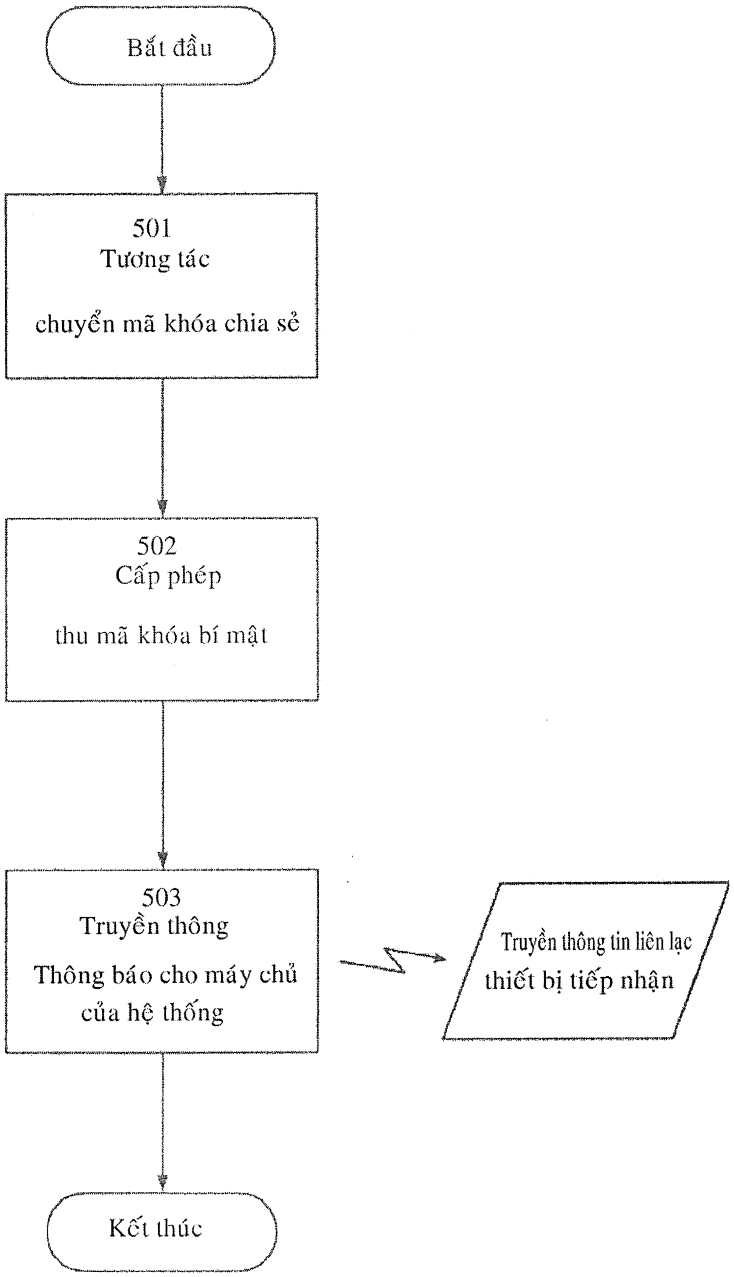

Bắt đầu
501
Tương tác
chuyển mã khóa chia sẻ
502
Cấp phép
thu mã khóa bí mật
503
Truyền thông
Thông báo cho máy chủ
của hệ thống
Truyền thông tin liên lạc
thiết bị tiếp nhận
Kết thúc

Fig. 5A


Bắt đầu
501
Tương tác
chuyển mã khóa chia sẻ
(i)
chọn tham số tương
tác phụ
giá trị tương quan với
tương tác dự tính
502
Cấp phép
thu mã khóa bí mật
(ii)
xác nhận tham số tương
tác phụ
mã điểm nút hoặc
mã bên tiếp nhận
Truyền thông tin liên lạc
thiết bị tiếp nhận
503
Truyền thông
Thông báo cho máy chủ
của hệ thống
(iii)
nhận phản hồi
cho phép xuất
Kết thúc

Fig. 5B

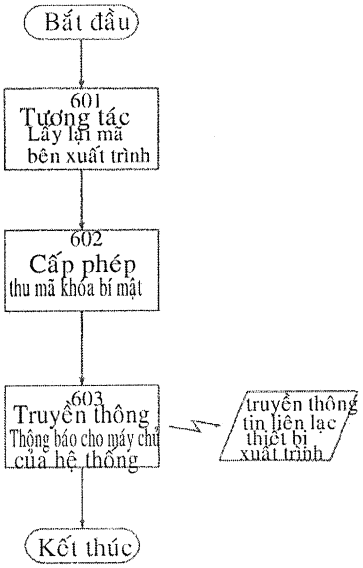

Bắt đầu
601
Tương tác
Lấy lại mã
bên xuất trình
602
Cấp phép
thu mã khóa bí mật
603
Truyền thông
Thông báo cho máy chủ
của hệ thống
truyền thông
tin liên lạc
thiết bị
xuất trình
Kết thúc

Fig. 6A

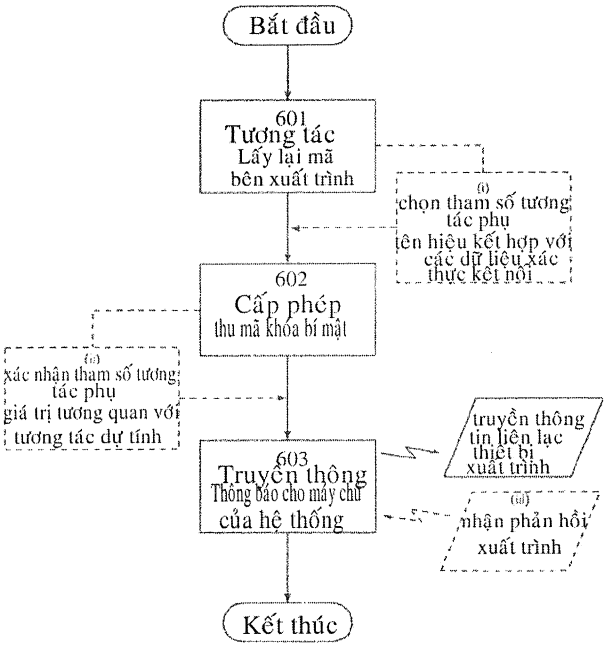
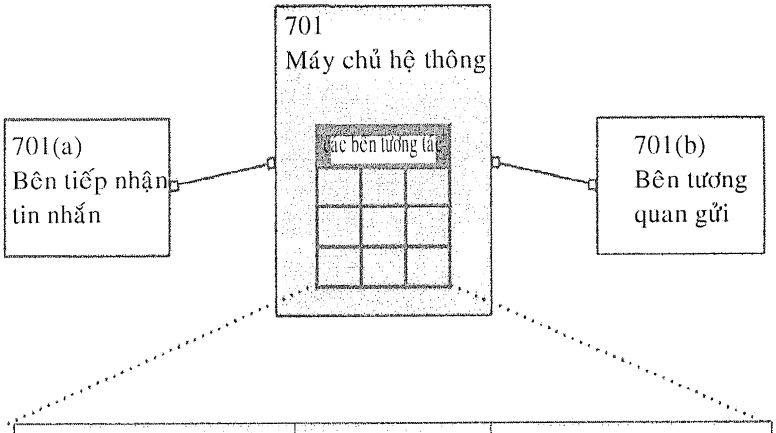

Bắt đầu
601
Tương tác
Lấy lại mã
bên xuất trình
(i)
chọn tham số tương
tác phụ
tên hiệu kết hợp với
các dữ liệu xác
thực kết nối
602
Cấp phép
thu mã khóa bí mật
(ii)
xác nhận tham số tương
tác phụ
giá trị tương quan với
tương tác dự tính
truyền thông
tin liên lạc
thiết bị
xuất trình
603
Truyền thông
Thông báo cho máy chủ
của hệ thống
(iii)
nhận phản hồi
xuất trình
Kết thúc

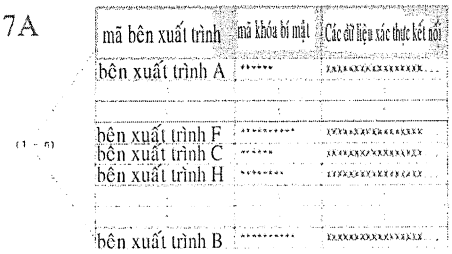
Fig. 6B



701 (xác định) mã bên xuất trình	702 (cho phép) mã khóa bí mật	703 (vị trí) Các dữ liệu xác thực kết nối
bên xuất trình A	******	XXXXXXXXXXXXXXXXX...
:	:	:
bên xuất trình Z	********	http://XXXXXXXXXXX...
:	:	:

Fig. 7

Fig. 7A



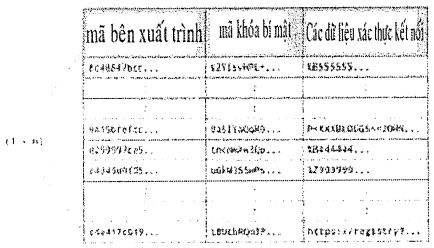


Fig. 7B

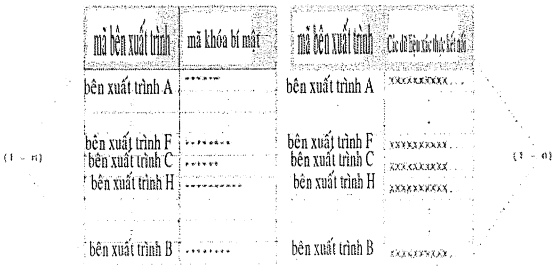


Fig. 7C

Fig. 7D

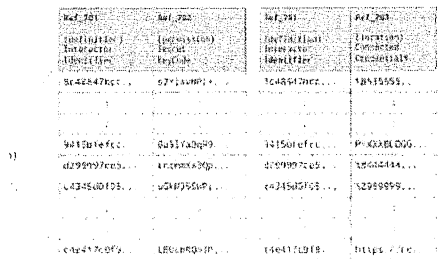


Fig. 7E

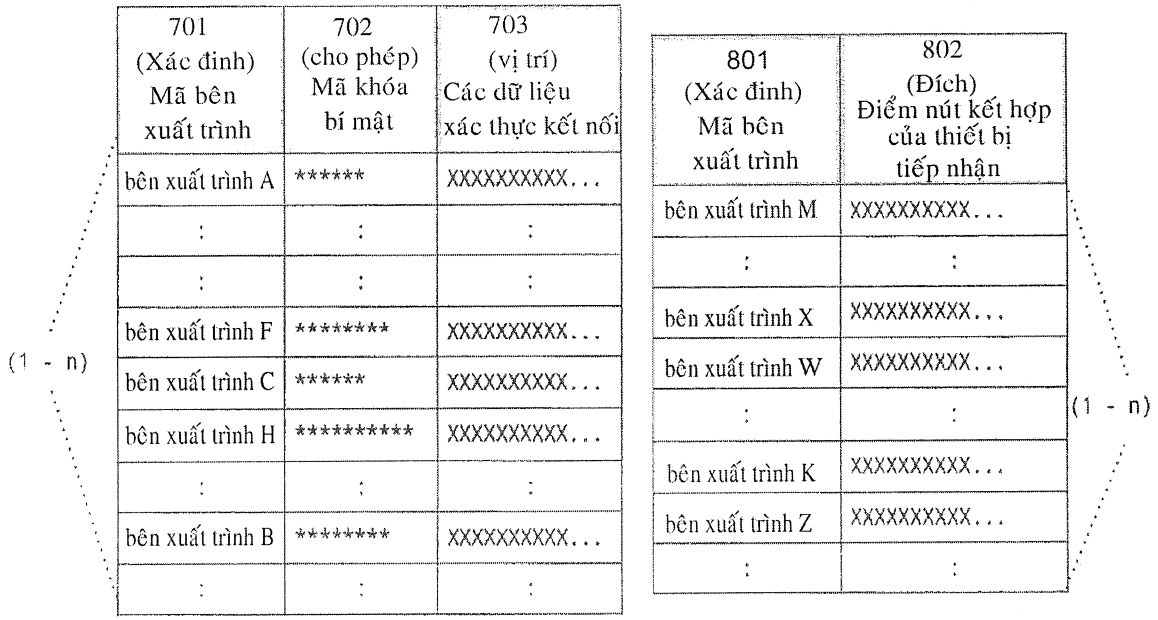

701
(Xác đinh)
Mã bên
xuất trình
702
(cho phép)
Mã khóa
bí mật
703
(vị trí)
Các dữ liệu
xác thực kết nối
bên xuất trình A
******
XXXXXXXXXX...
bên xuất trình F
****
XXXXXXXXXX...
bên xuất trình C
******
XXXXXXXXXX...
bên xuất trình H
****
XXXXXXXXXX...
bên xuất trình B
****
XXXXXXXXXX...
(1 - n)
801
(Xác đinh)
Mã bên
xuất trình
802
(Đích)
Điểm nút kết hợp
của thiết bị
tiếp nhận
bên xuất trình M
XXXXXXXXXX...
bên xuất trình X
XXXXXXXXXX...
bên xuất trình W
XXXXXXXXXX...
bên xuất trình K
XXXXXXXXXX...
bên xuất trình Z
XXXXXXXXXX...
(1 - n)

Fig. 8

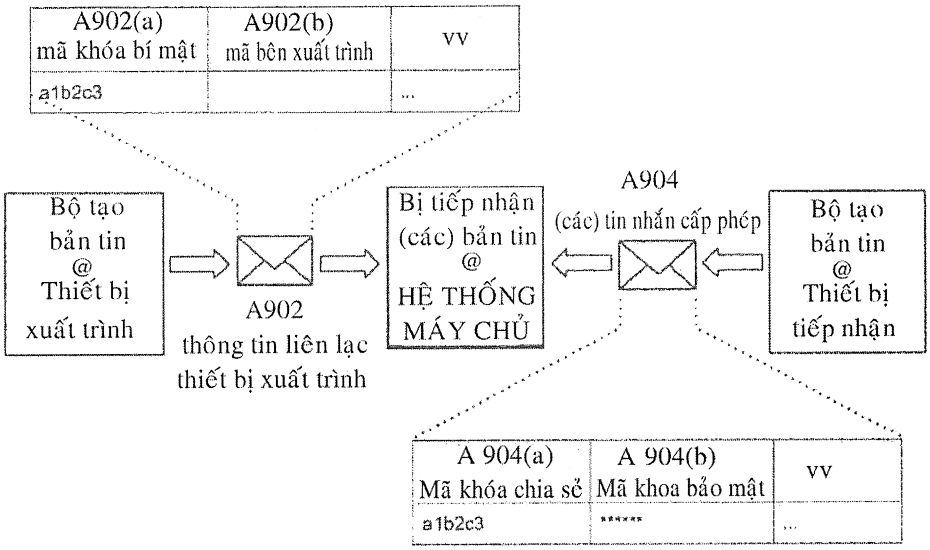

A902(a)
mã khóa bí mật
A902(b)
mã bên xuất trình
vv
a1b2c3
...
Bộ tạo bản tin @ Thiết bị xuất trình
A902
thông tin liên lạc thiết bị xuất trình
Bị tiếp nhận (các) bản tin @ HỆ THỐNG MÁY CHỦ
A904
(các) tin nhắn cấp phép
Bộ tạo bản tin @ Thiết bị tiếp nhận
A 904(a)
Mã khóa chia sẻ
A 904(b)
Mã khoa bảo mật
vv
a1b2c3
******
...

Fig. 9A

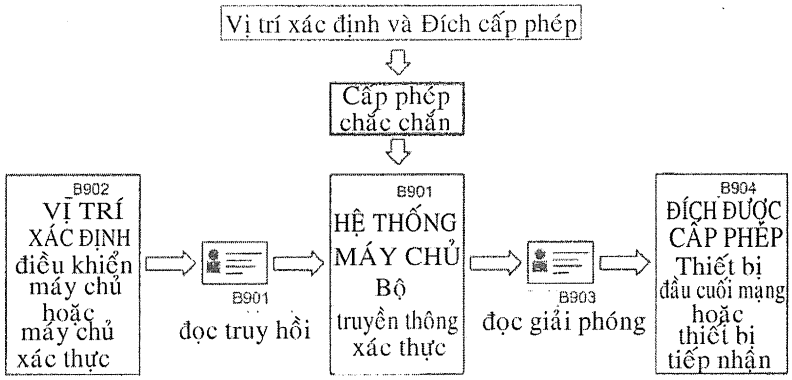

Vị trí xác định và Đích cấp phép
Cấp phép chắc chắn
B902
VỊ TRÍ XÁC ĐỊNH điều khiển máy chủ hoặc máy chủ xác thực
B901
đọc truy hồi
B901
HỆ THỐNG MÁY CHỦ Bộ truyền thông xác thực
B903
đọc giải phóng
B904
ĐÍCH ĐƯỢC CẤP PHÉP Thiết bị đầu cuối mạng hoặc thiết bị tiếp nhận

Fig. 9B

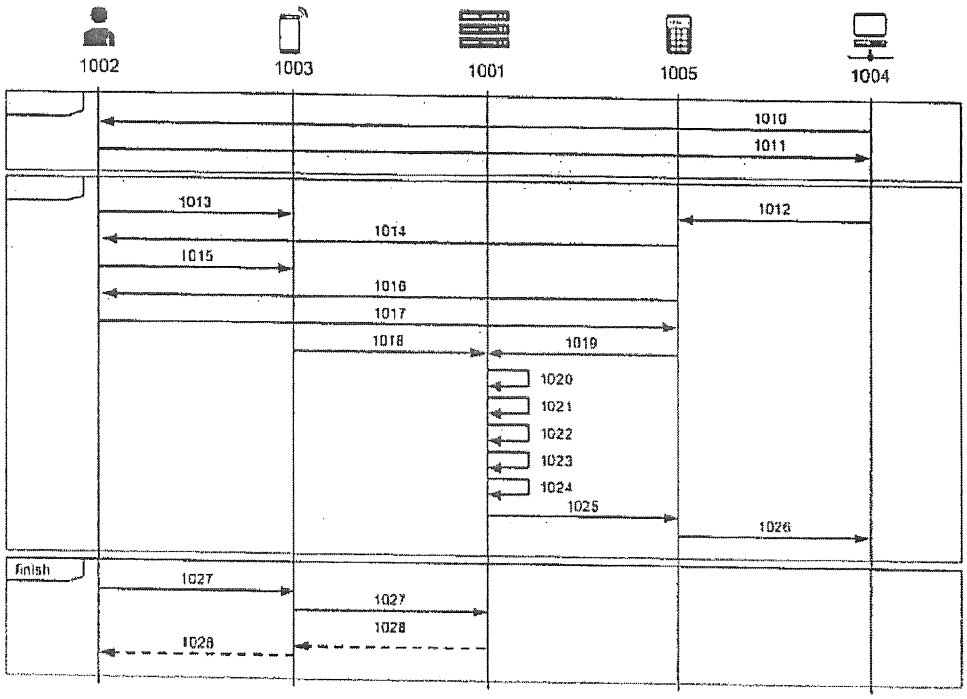

1002
1003
1001
1005
1004
1010
1011
1013
1012
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
finish
1027
1027
1028
1028

Fig. 10