(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) **1-0053886**

(51)[7] **G06Q 20/38**; H04L 9/32; G06Q 20/32

(13) **B**

(21) 1-2017-00972

(22) 21/10/2015

(86) PCT/KR2015/011134 21/10/2015

(87) WO 2016/064184 A1 28/04/2016

(30) 10-2014-0142627 21/10/2014 KR

(45) 25/11/2025 452

(43) 26/06/2017 351A

(73) SAMSUNG ELECTRONICS CO., LTD. (KR)
129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do, 16677, Republic of Korea

(72) Chol-Seo PARK (KR); Eun-Jik KIM (KR).

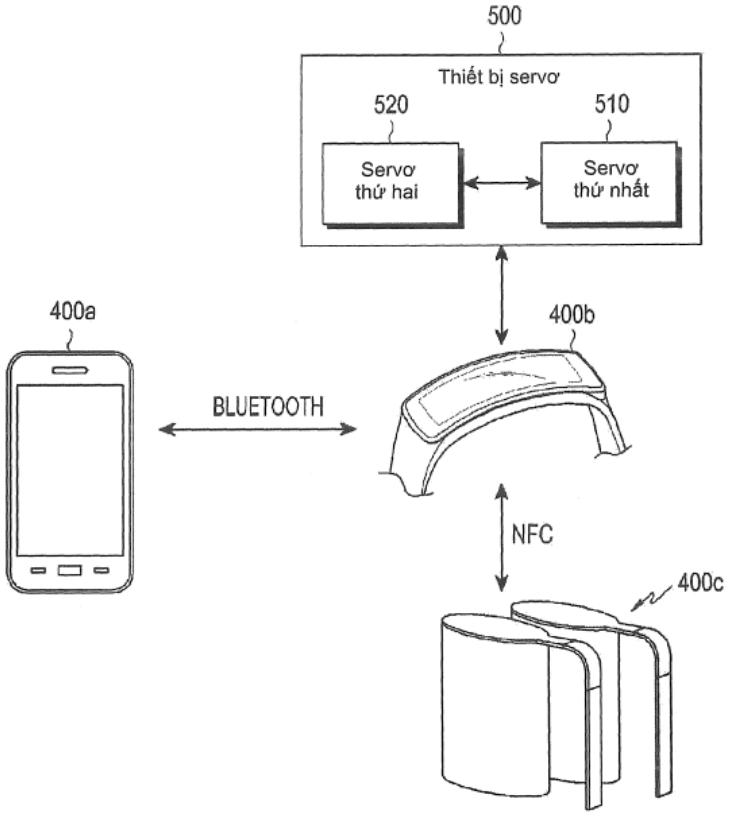
(74) Công ty Luật TNHH WINCO (WINCO LAW FIRM)

(54) THIẾT BỊ ĐIỆN TỬ VÀ PHƯƠNG PHÁP KẾT NỐI AN TOÀN CỦA THIẾT BỊ ĐIỆN TỬ

(21) 1-2017-00972

(57) Sáng chế đề cập tới thiết bị điện tử và phương pháp kết nối an toàn của thiết bị điện tử. Thiết bị điện tử bao gồm: môđun truyền thông tầm gần thứ nhất được làm thích ứng để thực hiện truyền thông tầm gần với thiết bị điện tử thứ hai, môđun an toàn được làm thích ứng để lưu trữ thông tin an toàn, và bộ xử lý được làm thích ứng để tiếp nhận, từ thiết bị điện tử thứ hai, khóa ghép cặp để đăng ký thiết bị điện tử ở trạng thái được liên kết với thiết bị điện tử thứ hai, truyền thông tin tạo ra khóa giao tiếp tới thiết bị điện tử thứ hai khi việc xác nhận với thiết bị điện tử thứ hai được hoàn thành dựa trên khóa ghép cặp, tạo ra khóa giao tiếp dựa trên thông tin tạo ra khóa giao tiếp, mã hóa thông tin an toàn dựa trên khóa giao tiếp, và truyền thông tin đã mã hóa tới thiết bị điện tử thứ hai.

Fig.4



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập tới thiết bị và phương pháp dùng cho kết nối an toàn. Cụ thể hơn, sáng chế đề cập tới thiết bị điện tử và phương pháp kết nối an toàn của thiết bị điện tử để truyền an toàn thông tin an toàn của thiết bị điện tử thứ nhất tới thiết bị điện tử thứ hai, vì thế các dịch vụ được thực hiện một cách thuận tiện bằng cách sử dụng thiết bị điện tử thứ hai.

Tình trạng kỹ thuật của sáng chế

Dịch vụ truyền thông trường gần (NFC) hiện được vận hành ở ba loại chế độ lần lượt là chế độ mô phỏng thẻ, chế độ bình đẳng (P2P), và chế độ đọc/ghi. Trong số ba chế độ này, chế độ mô phỏng thẻ được sử dụng cho dịch vụ thanh toán NFC.

Trong chế độ mô phỏng thẻ, các dịch vụ thanh toán NFC, chẳng hạn, dịch vụ thanh toán bằng thẻ vận tải, dịch vụ thanh toán bằng thẻ ghi nợ, và dịch vụ tương tự, có thể được thực hiện bằng cách sử dụng thiết bị điện tử tiến hành truyền thông tin an toàn lưu trữ trong một chip an toàn (chip phần tử an toàn gắn sẵn (eSE), chip thẻ mạch tích hợp vạn năng (UICC), hoặc chip mô phỏng thẻ chủ (HCE)) tới bộ đọc NFC nhờ một chip NFC.

Trong chế độ mô phỏng thẻ, truyền thông giữa chip an toàn (chip eSE, chip UICC, hoặc chip HCE) và chip NFC cần phải được kết nối trực tiếp. Ví dụ, chip an toàn (chip eSE, chip UICC, hoặc chip HCE) cần phải được nối với chip NFC từ quan điểm phần cứng trong một thiết bị điện tử sao cho thông tin an toàn lưu trữ trong chip an toàn được truyền tới bộ đọc NFC qua chip NFC, hoặc chip an toàn cần phải được nối với chip NFC nhờ bộ xử lý (bộ xử lý ứng dụng (AP)) trong một thiết bị điện tử.

Khi người dùng có nhiều thiết bị điện tử, ví dụ, điện thoại thông minh, điện thoại đồng hồ, và máy tính bảng, chip an toàn (chip phần tử an toàn gắn sẵn (eSE), chip thẻ mạch tích hợp vạn năng (UICC), hoặc chip mô phỏng thẻ chủ

(HCE)) và chip truyền thông trường gần (NFC) cần thiết đối với dịch vụ thanh toán NFC cần phải có mặt trong từng thiết bị điện tử. Ví dụ, khi chip eSE/UICC/HCU và chip NFC dùng cho dịch vụ thanh toán NFC chỉ có trong điện thoại thông minh, người dùng cần phải tiến hành dịch vụ thanh toán bằng cách sử dụng điện thoại thông minh mặc dù điện thoại thông minh được kết nối với điện thoại đồng hồ bằng Bluetooth.

Thông tin như nêu trên được đưa ra chỉ ở dạng thông tin cơ sở để trợ giúp việc hiểu rõ sáng chế. Không hề có xác định hoặc khẳng định rằng chi tiết bất kỳ như đã mô tả trên đây có thể áp dụng được làm các giải pháp kỹ thuật đã biết đối với sáng chế hay không.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là giải quyết ít nhất các vấn đề và/hoặc các nhược điểm như nêu trên và tạo ra ít nhất các ưu điểm như sẽ được mô tả sau đây. Do đó, theo một khía cạnh, sáng chế đề xuất đề xuất thiết bị và phương pháp dùng cho kết nối an toàn, để truyền an toàn thông tin an toàn của thiết bị điện tử thứ nhất tới thiết bị điện tử thứ hai, vì thế các dịch vụ, chẳng hạn dịch vụ thanh toán cho hàng hóa hoặc các dịch vụ có thể được thực hiện thuận tiện và/hoặc an toàn bằng cách sử dụng thiết bị điện tử thứ hai, nhờ đó tạo cho người dùng phạm vi mở rộng đối với các thiết bị có thể được sử dụng để thực hiện dịch vụ.

Theo một khía cạnh, sáng chế đề xuất thiết bị điện tử. Thiết bị điện tử này bao gồm: môđun truyền thông tầm gần thứ nhất được làm thích ứng để thực hiện truyền thông tầm gần với thiết bị điện tử thứ hai, môđun an toàn được làm thích ứng để lưu trữ thông tin an toàn, và bộ xử lý được làm thích ứng để tiếp nhận, từ thiết bị điện tử thứ hai, khóa ghép cặp để đăng ký thiết bị điện tử ở trạng thái được liên kết với thiết bị điện tử thứ hai (nghĩa là với thiết bị điện tử thứ hai), truyền thông tin tạo ra khóa giao tiếp tới thiết bị điện tử thứ hai khi việc xác nhận với thiết bị điện tử thứ hai được hoàn thành dựa trên khóa ghép cặp, tạo ra khóa giao tiếp dựa trên thông tin tạo ra khóa giao tiếp, mã hóa thông tin an toàn dựa trên khóa giao tiếp, và truyền thông tin đã mã hóa tới thiết bị điện tử thứ hai.

Theo một số ví dụ của sáng chế, bộ xử lý của thiết bị điện tử tiếp nhận và

truyền thông tin từ và tới thiết bị điện tử thứ hai bằng cách sử dụng môđun truyền thông tầm gần, ví dụ, môđun này có thể là môđun Bluetooth.

Theo một khía cạnh khác, sáng chế đề xuất thiết bị điện tử. Thiết bị điện tử có môđun truyền thông tầm gần thứ nhất được làm thích ứng để thực hiện truyền thông tầm gần với thiết bị điện tử thứ nhất, môđun truyền thông tầm gần thứ hai được làm thích ứng để thực hiện truyền thông tầm gần với thiết bị điện tử thứ ba, và bộ xử lý được làm thích ứng để truyền, khi khóa ghép cặp để đăng ký thiết bị điện tử thứ nhất ở trạng thái được liên kết với thiết bị điện tử được tiếp nhận từ thiết bị máy chủ, khóa ghép cặp tới thiết bị điện tử thứ nhất, truyền thông tin tạo ra khóa giao tiếp nhận được từ thiết bị điện tử thứ nhất tới thiết bị máy chủ, giải mã thông tin an toàn đã mã hóa được tiếp nhận từ thiết bị điện tử thứ nhất, dựa trên khóa giao tiếp nhận được từ thiết bị máy chủ, và truyền thông tin đã giải mã tới thiết bị điện tử thứ ba.

Theo một số ví dụ của sáng chế, bộ xử lý tiếp nhận và truyền thông tin từ và tới thiết bị điện tử thứ ba bằng cách sử dụng môđun truyền thông tầm gần thứ hai, môđun này có thể là môđun truyền thông trường gần (NFC).

Theo một khía cạnh khác, sáng chế đề xuất thiết bị máy chủ. Thiết bị máy chủ có bộ xử lý được làm thích ứng để tạo ra và lưu trữ khóa ghép cặp để đăng ký thiết bị điện tử thứ nhất ở trạng thái được liên kết với thiết bị điện tử, dựa trên thông tin duy nhất của thiết bị điện tử thứ nhất nhận được từ thiết bị điện tử, và truyền khóa ghép cặp tới thiết bị điện tử, và tạo ra khóa giao tiếp giống hệt khóa giao tiếp của thiết bị điện tử thứ nhất dựa trên thông tin tạo ra khóa giao tiếp của thiết bị điện tử thứ nhất nhận được từ thiết bị điện tử, và truyền khóa giao tiếp tới thiết bị điện tử.

Theo một khía cạnh khác, sáng chế đề xuất phương pháp kết nối an toàn của thiết bị điện tử. Phương pháp kết nối an toàn này có các bước: tiếp nhận khóa ghép cặp để đăng ký thiết bị điện tử ở trạng thái được liên kết với thiết bị điện tử thứ hai từ thiết bị điện tử thứ hai được kết nối qua kết nối truyền thông tầm gần thứ nhất, truyền thông tin tạo ra khóa giao tiếp tới thiết bị điện tử thứ hai khi việc xác nhận đối với thiết bị điện tử thứ hai được hoàn thành dựa trên

khóa ghép cặp, và tạo ra khóa giao tiếp dựa trên thông tin tạo ra khóa giao tiếp, mã hóa thông tin an toàn nhờ khóa giao tiếp, và truyền thông tin đã mã hóa tới thiết bị điện tử thứ hai.

Theo một khía cạnh khác, sáng chế đề xuất phương pháp kết nối an toàn của thiết bị điện tử. Phương pháp kết nối an toàn có các bước: các bước: truyền, khi khóa ghép cặp để đăng ký thiết bị điện tử thứ nhất ở trạng thái được liên kết với thiết bị điện tử, được tiếp nhận từ thiết bị máy chủ, khóa ghép cặp tới thiết bị điện tử thứ nhất được kết nối qua kết nối truyền thông tầm gần thứ nhất, truyền, tới thiết bị máy chủ, thông tin tạo ra khóa giao tiếp nhận được từ thiết bị điện tử thứ nhất, và giải mã, khi khóa giao tiếp được tiếp nhận từ thiết bị máy chủ, thông tin an toàn đã mã hóa được tiếp nhận từ thiết bị điện tử thứ nhất, dựa trên khóa giao tiếp, và truyền thông tin đã giải mã tới thiết bị điện tử thứ ba được kết nối qua kết nối truyền thông tầm gần thứ hai.

Theo một khía cạnh khác, sáng chế đề xuất phương pháp kết nối an toàn của thiết bị máy chủ. Phương pháp kết nối an toàn có các bước: tạo ra và lưu trữ, khi thông tin duy nhất của thiết bị điện tử thứ nhất được tiếp nhận từ thiết bị điện tử, khóa ghép cặp để đăng ký thiết bị điện tử thứ nhất ở trạng thái được liên kết với thiết bị điện tử, dựa trên thông tin duy nhất của thiết bị điện tử thứ nhất, và truyền khóa ghép cặp tới thiết bị điện tử, và tạo ra, khi thông tin tạo ra khóa giao tiếp của thiết bị điện tử thứ nhất được tiếp nhận từ thiết bị điện tử, khóa giao tiếp giống hệt khóa giao tiếp của thiết bị điện tử thứ nhất dựa trên thông tin tạo ra khóa giao tiếp, và truyền khóa giao tiếp tới thiết bị điện tử.

Một khía cạnh khác của sáng chế là đề xuất chương trình máy tính bao gồm các lệnh được làm thích ứng, khi được chạy, để thực hiện phương pháp và/hoặc thiết bị theo khía cạnh bất kỳ trong số các khía cạnh nêu trên. Một khía cạnh nữa của sáng chế là đề xuất bộ nhớ đọc được bằng máy lưu trữ chương trình như vậy.

Theo một số ví dụ về sáng chế, thông tin tạo ra khóa giao tiếp là ít nhất một trong số thông tin nhãn thời gian (Timestamp) hoặc thông tin số đếm.

Thiết bị và phương pháp kết nối an toàn, theo các phương án khác nhau

của sáng chế, cung cấp theo cách an toàn thông tin an toàn của thiết bị điện tử thứ nhất tới thiết bị điện tử thứ hai, vì thế các dịch vụ được thực hiện một cách thuận tiện bằng cách sử dụng thiết bị điện tử thứ hai.

Các khía cạnh khác, các ưu điểm, và các dấu hiệu chính của sáng chế sẽ trở nên rõ ràng đối với người có hiểu biết trung bình trong lĩnh vực này qua phần mô tả chi tiết sau đây, có dựa vào các hình vẽ kèm theo, trong đó đề xuất các phương án khác nhau của sáng chế.

Các hiệu quả có lợi

Do đó, sáng chế cho phép đề xuất thiết bị và phương pháp dùng cho kết nối an toàn để truyền an toàn thông tin an toàn của thiết bị điện tử thứ nhất tới thiết bị điện tử thứ hai, vì thế các dịch vụ được thực hiện một cách thuận tiện bằng cách sử dụng thiết bị điện tử thứ hai.

Mô tả vắn tắt các hình vẽ

Các khía cạnh nêu trên và khác nữa, các dấu hiệu, và các ưu điểm của sáng chế sẽ trở nên rõ ràng hơn qua phần mô tả sau đây có dựa vào các hình vẽ kèm theo, trong đó:

Fig.1 là hình vẽ dạng sơ đồ thể hiện môi trường mạng theo các phương án khác nhau của sáng chế;

Fig.2 là sơ đồ khối thể hiện thiết bị điện tử theo các phương án khác nhau của sáng chế;

Fig.3 là sơ đồ khối thể hiện môđun lập trình theo các phương án khác nhau của sáng chế;

Fig.4 là hình vẽ dạng sơ đồ thể hiện hệ thống kết nối an toàn theo các phương án khác nhau của sáng chế;

Fig.5 là sơ đồ khối thể hiện thiết bị kết nối an toàn theo các phương án khác nhau của sáng chế;

Fig.6A và Fig.6B là các lưu đồ thể hiện phương pháp đăng ký đối với kết nối an toàn theo các phương án khác nhau của sáng chế; và

Fig.7A và Fig.7B là các lưu đồ thể hiện phương pháp kết nối an toàn theo các phương án khác nhau của sáng chế.

Trên tất cả các hình vẽ kèm theo, các số chỉ dẫn tương tự sẽ biểu thị các bộ phận, các phần tử và các kết cấu tương tự.

Mô tả chi tiết sáng chế

Phần mô tả sau đây có dựa vào các hình vẽ kèm theo được đưa ra để có thể hiểu rõ hoàn toàn các phương án khác nhau của sáng chế như được xác định bằng các điểm yêu cầu bảo hộ và các phương án tương đương. Phần mô tả này có các chi tiết cụ thể khác nhau để có thể hiểu rõ sáng chế nhưng các chi tiết này chỉ nhằm mục đích minh họa. Do đó, người có hiểu biết trung bình trong lĩnh vực này cần phải hiểu rằng các thay đổi và cải biến khác nhau từ các phương án khác nhau được mô tả ở đây có thể được tạo ra mà không nằm ngoài phạm vi của sáng chế. Ngoài ra, phần mô tả về các chức năng và kết cấu đã biết có thể được loại bỏ cho dễ hiểu và ngắn gọn.

Các thuật ngữ và các từ ngữ dùng trong phần mô tả và yêu cầu bảo hộ sau đây không bị giới hạn ở các ý nghĩa theo thư mục, và được sử dụng bởi tác giả sáng chế chỉ để cho phép hiểu rõ ràng và đầy đủ nội dung của sáng chế. Do đó, người có hiểu biết trung bình trong lĩnh vực kỹ thuật này cần phải hiểu rằng phần mô tả sau đây về các phương án khác nhau của sáng chế được đưa ra chỉ nhằm mục đích minh họa và không nhằm giới hạn phạm vi của sáng chế như được xác định bằng các điểm yêu cầu bảo hộ kèm theo và các phương án tương đương của chúng.

Cần phải hiểu rằng các dạng thức theo số ít gồm cả các dạng số nhiều trừ khi được xác định khác đi. Như vậy, ví dụ, cụm từ "bề mặt bộ phận" có liên quan tới một hoặc nhiều bề mặt như vậy.

Thuật ngữ "gần như" có nghĩa là đặc tính, tham số hoặc giá trị vừa nêu không nhất thiết thu được một cách chính xác, và các độ lệch hoặc các biến đổi, bao gồm, ví dụ, dung sai, sai số đo, giới hạn độ chính xác đo và các yếu tố khác đã biết đối với người có hiểu biết trung bình trong lĩnh vực kỹ thuật này, có thể xuất hiện với lượng không ngăn cản hiệu quả liên quan tới đặc tính dự kiến được tạo ra.

Theo các phương án của sáng chế, cách diễn đạt "có", "có thể có", "gồm"

hoặc “có thể gồm” mô tả sự có mặt của dấu hiệu tương ứng (ví dụ, một trị số, chức năng, hoạt động, hoặc các bộ phận, chẳng hạn các phần tử), và không loại trừ sự có mặt của các dấu hiệu bổ sung.

Theo các phương án của sáng chế, cách diễn đạt "A hoặc B", "ít nhất một trong A và/hoặc B", hoặc "một hoặc nhiều trong số A và/hoặc B" có thể có tất cả các kết hợp khả dĩ của các mục được liệt kê. Ví dụ, cách diễn đạt "A hoặc B", "ít nhất một trong số A và B", hoặc "ít nhất một trong số A hoặc B" bao gồm tất cả trong số (1) có ít nhất một A, (2) có ít nhất một B, hoặc (3) có tất cả trong số ít nhất một A và ít nhất một B.

Cách diễn đạt "thứ nhất”, hoặc "thứ hai” dùng trong các phương án khác nhau của sáng chế có thể cải biến các bộ phận khác nhau bất kể thứ tự và/hoặc mức độ quan trọng nhưng không giới hạn các bộ phận tương ứng. Các cách diễn đạt nêu trên được sử dụng chỉ nhằm mục đích phân biệt một phần tử với các phần tử khác. Ví dụ, thiết bị người dùng thứ nhất và thiết bị người dùng thứ hai biểu thị những thiết bị người dùng khác nhau mặc dù cả hai đều là các thiết bị người dùng. Ví dụ, phần tử thứ nhất có thể được quy định là phần tử thứ hai, và tương tự, phần tử thứ hai có thể được quy định là phần tử thứ nhất mà không nằm ngoài phạm vi của sáng chế.

Khi mô tả rằng một phần tử (ví dụ, phần tử thứ nhất) được " liên kết hoặc nối (hoạt động hoặc truyền thông) với" một phần tử khác (ví dụ, phần tử thứ hai), cần phải hiểu rằng một phần tử này được nối trực tiếp với một phần tử khác hoặc một phần tử này được nối gián tiếp với một phần tử khác qua một phần tử khác nữa (ví dụ, phần tử thứ ba). Trái lại, cần phải hiểu rằng khi một phần tử (ví dụ, phần tử thứ nhất) được mô tả là được "nối trực tiếp”, hoặc "liên kết trực tiếp" với một phần tử khác (phần tử thứ hai), không có phần tử (ví dụ, phần tử thứ ba) nằm xen giữa chúng.

Cách diễn đạt "được làm thích ứng để" được sử dụng theo các phương án của sáng chế có thể được thay thế bằng, ví dụ, "phù hợp để", "có khả năng để", "được thiết kế để", “thích ứng để”, “được tạo ra để”, hoặc "có khả năng” theo trường hợp cụ thể. Thuật ngữ "được làm thích ứng để" có thể không nhất thiết

phải là "được thiết kế đặc biệt để" ở phần cứng (phần cứng). Theo cách khác, trong một số trường hợp, cách diễn đạt "thiết bị được làm thích ứng để" có thể nghĩa là thiết bị, cùng với các thiết bị hoặc các bộ phận khác, "có thể". Ví dụ, cụm từ "bộ xử lý thích ứng (hoặc được làm thích ứng) để thực hiện A, B, và C" có thể nghĩa là bộ xử lý chuyên dụng (ví dụ, bộ xử lý gắn sẵn) chỉ để thực hiện các hoạt động tương ứng hoặc bộ xử lý thông dụng (ví dụ, bộ xử lý trung tâm (CPU) hoặc bộ xử lý ứng dụng (AP)) có thể thực hiện các hoạt động tương ứng bằng cách chạy một hoặc nhiều chương trình phần mềm được lưu trữ trong thiết bị bộ nhớ.

Trong toàn bộ phần mô tả và yêu cầu bảo hộ của sáng chế, các từ ngữ "bao gồm" và "chứa" và các biến thể của các từ này, ví dụ " gồm" và "gồm có", nghĩa là “có nhưng không bị giới hạn", và không dự kiến để (và không) loại trừ các phần tử, chi tiết bổ sung, các bộ phận, các số nguyên hoặc các bước khác.

Các dấu hiệu, các số nguyên, các đặc tính, các hợp chất, các thành phần hóa học hoặc các nhóm được mô tả cùng với một khía cạnh, phương án hoặc ví dụ cụ thể của sáng chế cần được hiểu là có thể áp dụng cho khía cạnh, phương án hoặc ví dụ bất kỳ khác được mô tả ở đây trừ khi không phù hợp.

Ngoài ra, cần phải hiểu rằng, trong toàn bộ phần mô tả và yêu cầu bảo hộ của sáng chế, cụm từ ở dạng chung là "X để Y" (trong đó Y là hoạt động, chức năng hoặc bước nhất định và X là phương tiện nhất định để thực hiện hoạt động, chức năng hoặc bước nhất định này) có nghĩa là phương tiện X được làm thích ứng hoặc bố trí cụ thể, nhưng không phải là duy nhất, để thực hiện Y.

Các thuật ngữ dùng ở đây chỉ nhằm mục đích mô tả các phương án cụ thể của sáng chế và không nhằm giới hạn phạm vi của các phương án khác. Trừ khi được xác định khác đi, tất cả các thuật ngữ dùng ở đây, kể cả các thuật ngữ kỹ thuật và khoa học, đều có hàm nghĩa giống như được hiểu thông thường bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật này. Các thuật ngữ như vậy là các thuật ngữ được xác định trong từ điển thông dụng được diễn giải sao cho có hàm nghĩa tương đương với các hàm nghĩa theo ngữ cảnh liên quan tới kỹ thuật tương ứng, và không được diễn giải sao cho có hàm nghĩa lý tưởng hoặc

quá máy móc trừ khi được xác định rõ ràng theo các phương án của sáng chế. Trong một số trường hợp, thậm chí thuật ngữ được xác định theo các phương án của sáng chế không bị diễn giải để loại trừ các phương án của sáng chế.

Ví dụ, thiết bị điện tử có thể là ít nhất một trong số điện thoại thông minh, máy tính cá nhân (PC) bảng, điện thoại di động, điện thoại viđeo, máy đọc sách điện tử (e-book), máy PC để bàn, máy PC xách tay, máy tính sổ tay, thiết bị trợ giúp số cá nhân (PDA), máy chơi đa phương tiện xách tay (PMP), máy chơi tệp nhóm chuyên gia ảnh động pha 1 hoặc pha 2 (MPEG-1 hoặc MPEG-2) lớp auđio 3 (MP3), thiết bị y tế di động, camêra, và thiết bị đeo được (ví dụ, thiết bị gắn ở đầu (HMD), chẳng hạn kính điện tử, trang phục điện tử, vòng đeo tay điện tử, vòng cổ điện tử, phụ kiện điện tử, vết xăm điện tử, đồng hồ thông minh, và thiết bị tương tự).

Theo các phương án khác nhau của sáng chế, thiết bị điện tử có thể là một thiết bị gia dụng thông minh. Thiết bị gia dụng này có thể là ít nhất một trong số, ví dụ, máy thu hình (TV), máy chơi đĩa số đa năng (DVD), dàn âm thanh, tủ lạnh, máy điều hòa không khí, máy hút bụi, lò nướng, lò vi sóng, máy giặt, máy lọc không khí, thiết bị Set-top box, bảng điều khiển tự động gia đình, bảng điều khiển an ninh, thiết bị TV box (ví dụ, Samsung HomeSync™, Apple TV™, hoặc Google TV™), máy điều khiển trò chơi (ví dụ, Xbox™ và PlayStation™), từ điển điện tử, khóa điện tử, máy quay viđeo, và khung ảnh điện tử.

Theo một phương án của sáng chế, thiết bị điện tử có thể là ít nhất một trong số các thiết bị y tế khác nhau (ví dụ, các thiết bị đo y tế xách tay khác nhau (thiết bị giám sát đường máu, thiết bị giám sát nhịp tim, thiết bị đo huyết áp, thiết bị đo nhiệt độ cơ thể, và thiết bị tương tự), máy chụp mạch cộng hưởng từ (MRA), thiết bị tạo ảnh cộng hưởng từ (MRI), thiết bị chụp cắt lớp bằng máy tính (CT), và máy siêu âm), thiết bị dẫn đường, thiết bị thu hệ thống định vị toàn cầu (GPS), thiết bị ghi dữ liệu sự kiện (EDR), thiết bị ghi dữ liệu chuyến bay (FDR), thiết bị giải trí trên ô tô, thiết bị điện tử dùng cho tàu thủy (ví dụ, thiết bị dẫn đường dùng cho tàu thủy, và la bàn hồi chuyển), thiết bị hàng không, thiết bị an ninh, bộ thiết bị gắn ở đầu ô tô, robot gia dụng hoặc công nghiệp, máy giao

dịch tự động (ATM) ở ngân hàng, thiết bị phục vụ điểm bán hàng (POS) tại cửa hàng, hoặc thiết bị liên quan tới mạng Internet vạn năng (ví dụ, bóng đèn, các bộ cảm biến khác nhau, đồng hồ đo điện năng hoặc khí đốt, thiết bị vòi phun, thiết bị báo cháy, bộ ổn nhiệt, đèn đường, thiết bị nướng, đồ dùng thể thao, bình nước nóng, thiết bị sưởi, thiết bị đun, và thiết bị tương tự).

Theo các phương án khác nhau của sáng chế, thiết bị điện tử có thể là ít nhất một trong số một phần của đồ nội thất hoặc công trình/kết cấu, bảng điện tử, thiết bị tiếp nhận chữ ký điện tử, máy chiếu, và các loại thiết bị đo khác nhau (ví dụ, đồng hồ đo nước, đồng hồ đo điện, đồng hồ đo khí đốt, và đồng hồ đo sóng vô tuyến). Thiết bị điện tử theo các phương án khác nhau của sáng chế có thể là kết hợp của một hoặc nhiều trong số các thiết bị khác nhau như nêu trên. Hơn nữa, thiết bị điện tử theo một phương án của sáng chế không bị giới hạn ở các thiết bị như nêu trên, và có thể có thiết bị điện tử mới theo sự phát triển của công nghệ.

Sau đây, thiết bị điện tử theo các phương án khác nhau của sáng chế sẽ được mô tả có dựa vào các hình vẽ kèm theo. Như được sử dụng ở đây, thuật ngữ "người dùng" có thể biểu thị một người sử dụng thiết bị điện tử hoặc một thiết bị (ví dụ, thiết bị điện tử trí tuệ nhân tạo) sử dụng thiết bị điện tử này.

Fig.1 là hình vẽ dạng sơ đồ thể hiện môi trường mạng theo các phương án khác nhau của sáng chế.

Theo Fig.1, thiết bị điện tử 101 trong môi trường mạng 100, theo các phương án khác nhau của sáng chế, sẽ được mô tả.

Theo Fig.1, thiết bị điện tử 101 có thể có bus 110, bộ xử lý 120, bộ nhớ 130, giao diện nhập/xuất 150, màn hình 160, và giao diện truyền thông 170. Theo một phương án của sáng chế, thiết bị điện tử 101 có thể loại bỏ ít nhất một số phần tử nêu trên hoặc còn có thể có các phần tử khác.

Ví dụ, bus 110 có thể có mạch để kết nối các phần tử 110 tới 170 với nhau, và thực hiện truyền thông (ví dụ, tin nhắn điều khiển và/hoặc dữ liệu) giữa các phần tử.

Bộ xử lý 120 có thể có một hoặc nhiều trong số CPU, AP, và bộ xử lý

truyền thông (CP). Bộ xử lý 120 có thể điều khiển, ví dụ, ít nhất một phần tử khác của thiết bị điện tử 101 và/hoặc xử lý tính toán hoặc dữ liệu liên quan tới truyền thông.

Bộ nhớ 130 có thể là bộ nhớ khả biến và/hoặc bộ nhớ bất khả biến. Bộ nhớ 130 có thể lưu trữ, ví dụ, các lệnh hoặc dữ liệu liên quan tới ít nhất một phần tử khác của thiết bị điện tử 101. Theo một phương án của sáng chế, bộ nhớ 130 có thể lưu trữ phần mềm và/hoặc chương trình 140. Chương trình 140 có thể có, ví dụ, phần nhân 141, phần trung gian 143, giao diện lập trình ứng dụng (API) 145, và/hoặc chương trình ứng dụng (hoặc ứng dụng) 147. Ít nhất một số trong số phần nhân 141, phần trung gian 143, và API 145 có thể liên quan tới một hệ điều hành (OS).

Phần nhân 141 có thể điều khiển hoặc quản lý các tài nguyên hệ thống (ví dụ, bus 110, bộ xử lý 120, hoặc bộ nhớ 130) dùng để thực hiện hoạt động hoặc chức năng được thực hiện bởi các chương trình khác (ví dụ, phần trung gian 143, API 145, hoặc chương trình ứng dụng 147). Hơn nữa, phần nhân 141 có thể tạo ra giao diện mà nhờ đó phần trung gian 143, API 145, hoặc chương trình ứng dụng 147 có thể truy nhập các phần tử riêng biệt của thiết bị điện tử 101 để điều khiển hoặc quản lý các tài nguyên hệ thống.

Phần trung gian 143 có thể có tác dụng làm phần trung gian sao cho, ví dụ, API 145 hoặc chương trình ứng dụng 147 truyền thông với phần nhân 141 để truyền/nhận dữ liệu. Hơn nữa, liên quan tới các yêu cầu nhiệm vụ nhận được từ chương trình ứng dụng 147, phần trung gian 143 có thể thực hiện điều khiển (ví dụ, lập kế hoạch hoặc cân bằng tải) đối với các yêu cầu nhiệm vụ bằng cách sử dụng, ví dụ, phương pháp gán, cho ít nhất một ứng dụng, một quyền ưu tiên để sử dụng các tài nguyên hệ thống (ví dụ, bus 110, bộ xử lý 120, hoặc bộ nhớ 130) của thiết bị điện tử 101.

API 145 là một giao diện mà nhờ đó các ứng dụng 147 điều khiển các chức năng được tạo ra từ phần nhân 141 hoặc phần trung gian 143, và có thể có, ví dụ, ít nhất một giao diện hoặc chức năng (ví dụ, các lệnh) để kiểm soát tệp, kiểm soát cửa sổ, xử lý ảnh, hoặc điều khiển văn bản.

Giao diện nhập/xuất 150 có thể có tác dụng làm giao diện để có thể truyền các lệnh hoặc dữ liệu nhập vào từ người dùng hoặc một thiết bị bên ngoài khác tới (các) phần tử khác của thiết bị điện tử 101. Hơn nữa, giao diện nhập/xuất 150 có thể xuất các lệnh hoặc dữ liệu nhận được từ (các) phần tử khác của thiết bị điện tử 101 tới người dùng hoặc một thiết bị bên ngoài khác.

Màn hình 160 có thể là, ví dụ, màn hình tinh thể lỏng (LCD), màn hình điot phát quang (LED), màn hình LED hữu cơ (OLED), màn hình hệ vi điện cơ (MEMS), hoặc màn hình giấy điện tử. Màn hình 160 có thể hiển thị các loại nội dung khác nhau (ví dụ, văn bản, ảnh, viđeo, các biểu tượng, hoặc các ký hiệu) cho người dùng. Màn hình 160 có thể là màn hình xúc giác, và có thể tiếp nhận, ví dụ, trạng thái chạm, cử chỉ, trạng thái lân cận, hoặc nhập bằng thao tác vuốt bằng cách sử dụng bút điện tử hoặc một phần cơ thể người dùng.

Giao diện truyền thông 170 có thể thiết lập truyền thông giữa, ví dụ, thiết bị điện tử 101 và một thiết bị bên ngoài (ví dụ, thiết bị điện tử bên ngoài thứ nhất 102, thiết bị điện tử bên ngoài thứ hai 104, hoặc máy chủ 106). Ví dụ, giao diện truyền thông 170 có thể được nối với mạng 162 bằng truyền thông không dây hoặc truyền thông có dây để truyền thông với thiết bị bên ngoài (ví dụ, thiết bị điện tử bên ngoài thứ hai 104 hoặc máy chủ 106). Theo một ví dụ khác, giao diện truyền thông 170 có thể được nối với thiết bị điện tử bên ngoài thứ nhất 102 nhờ truyền thông không dây 164.

Truyền thông không dây có thể sử dụng, ví dụ, ít nhất một trong số công nghệ tiến hóa dài hạn (LTE), công nghệ LTE cải tiến (LTE-A), công nghệ truy nhập đa phân mã (CDMA), công nghệ CDMA dải rộng (WCDMA), hệ thống viễn thông di động toàn cầu (UMTS), hệ thống dải rộng không dây (WiBro), và hệ thống truyền thông di động toàn cầu (GSM), làm giao thức truyền thông di động. Truyền thông có dây có thể có, ví dụ, ít nhất một trong số bus nối tiếp đa năng (USB), giao diện đa phương tiện chất lượng cao (HDMI), tiêu chuẩn khuyến nghị 232 (RS-232), và dịch vụ điện thoại truyền thống (POTS). Mạng 162 có thể có ít nhất một trong số các mạng truyền thông, chẳng hạn máy tính mạng (ví dụ, mạng cục bộ (LAN) hoặc mạng vùng rộng (WAN)), mạng Internet,

và mạng điện thoại.

Từng thiết bị điện tử bên ngoài thứ nhất 102 và thiết bị điện tử bên ngoài thứ hai 104 có thể là một thiết bị giống hoặc khác với thiết bị điện tử 101. Theo một phương án của sáng chế, máy chủ 106 có thể là một nhóm gồm một hoặc nhiều máy chủ. Theo các phương án khác nhau của sáng chế, một số hoặc tất cả các hoạt động được thực hiện trong thiết bị điện tử 101 có thể được thực hiện nhờ một thiết bị điện tử khác hoặc nhờ các thiết bị điện tử (ví dụ, thiết bị điện tử bên ngoài thứ nhất 102 hoặc thiết bị điện tử bên ngoài thứ hai 104, hoặc máy chủ 106). Theo một phương án của sáng chế, khi thiết bị điện tử 101 cần phải thực hiện chức năng hoặc dịch vụ một cách tự động hoặc theo yêu cầu, thiết bị điện tử 101 có thể yêu cầu một thiết bị khác (ví dụ, thiết bị điện tử bên ngoài thứ nhất 102 hoặc thiết bị điện tử bên ngoài thứ hai 104, hoặc máy chủ 106) thực hiện ít nhất một số chức năng liên quan tới chức năng hoặc dịch vụ, để thay thế hoặc bổ sung vào việc thực hiện chức năng hoặc dịch vụ. Thiết bị điện tử khác (ví dụ, thiết bị điện tử bên ngoài thứ nhất 102 hoặc thiết bị điện tử bên ngoài thứ hai 104 hoặc máy chủ 106) có thể thực hiện chức năng được yêu cầu hoặc chức năng bổ sung, và có thể truyền kết quả của nó tới thiết bị điện tử 101. Thiết bị điện tử 101 có thể tạo ra chức năng hoặc dịch vụ được yêu cầu dựa trên kết quả nhận được khi nó đang hoặc sau khi xử lý bổ sung kết quả nhận được. Nhằm mục đích này, ví dụ, công nghệ điện toán đám mây, công nghệ điện toán phân tán, hoặc công nghệ điện toán khách hàng-máy chủ có thể được sử dụng.

Fig.2 là sơ đồ khối thể hiện thiết bị điện tử theo các phương án khác nhau của sáng chế.

Theo Fig.2, thiết bị điện tử 201 có thể có, ví dụ, một phần hoặc toàn bộ chi tiết của thiết bị điện tử 101 như được thể hiện trên Fig.1. Thiết bị điện tử 201 này có thể có ít nhất một AP 210, môđun truyền thông 220, thẻ môđun nhận dạng thuê bao (SIM) 224, bộ nhớ 230, môđun cảm biến 240, thiết bị đầu vào 250, màn hình 260, giao diện 270, môđun auđio 280, môđun camêra 291, môđun quản lý nguồn điện 295, bộ pin 296, bộ chỉ báo 297, và môtơ 298.

AP 210 có thể điều khiển các phần tử phần cứng hoặc phần mềm nối với

nó bằng cách kích hoạt một hệ điều hành hoặc chương trình ứng dụng, và có thể thực hiện các loại xử lý dữ liệu và tính toán khác nhau. AP 210 có thể được cải biến ở dạng, ví dụ, một hệ thống trên chip (SoC). Theo một phương án của sáng chế, AP 210 còn có thể có bộ xử lý đồ họa (GPU) và/hoặc bộ xử lý tín hiệu ảnh. AP 210 có thể có ít nhất một số phần tử (ví dụ, môđun truyền thông di động 221) như được thể hiện trên Fig.2. AP 210 có thể nạp các lệnh hoặc dữ liệu, nhận được từ ít nhất một phần tử khác (ví dụ, bộ nhớ bất khả biến), trong bộ nhớ khả biến để xử lý các lệnh hoặc dữ liệu được nạp, và có thể lưu trữ các loại dữ liệu khác nhau trong bộ nhớ bất khả biến.

Môđun truyền thông 220 có thể có cấu hình giống hoặc tương tự với giao diện truyền thông 170 theo Fig.1. Môđun truyền thông 220 có thể có, ví dụ, môđun truyền thông di động 221, môđun Wi-Fi 223, môđun Bluetooth (BT) 225, môđun GPS 227, môđun truyền thông trường gần (NFC) 228, và môđun tần số vô tuyến (RF) 229.

Môđun truyền thông di động 221 có thể tạo ra cuộc gọi tiếng nói, cuộc gọi viđeo, dịch vụ tin nhắn văn bản, hoặc các dịch vụ Internet nhờ, ví dụ, một mạng truyền thông. Theo một phương án của sáng chế, môđun truyền thông di động 221 có thể phân biệt và xác nhận các thiết bị điện tử 201 trong một mạng truyền thông bằng cách sử dụng môđun nhận dạng thuê bao (ví dụ, thẻ SIM 224). Theo một phương án của sáng chế, môđun truyền thông di động 221 có thể thực hiện ít nhất một số chức năng có thể được tạo ra bởi AP 210. Theo một phương án của sáng chế, môđun truyền thông di động 221 có thể có một bộ xử lý truyền thông (CP).

Môđun Wi-Fi 223, môđun BT 225, môđun GPS 227, và môđun NFC 228 có thể có, ví dụ, bộ xử lý để xử lý dữ liệu được phát/thu nhờ môđun tương ứng. Theo phương án bất kỳ của sáng chế, ít nhất một số (hai hoặc nhiều hơn) trong số môđun truyền thông di động 221, môđun Wi-Fi 223, môđun BT 225, môđun GPS 227, và môđun NFC 228 có thể có trong một chip tích hợp (IC) hoặc gói IC.

Môđun RF 229 có thể truyền/tiếp nhận, ví dụ, một tín hiệu truyền thông

(ví dụ, một tín hiệu RF). Môđun RF 229 có thể có, ví dụ, bộ thu-phát, môđun khuếch đại công suất (PAM), bộ lọc tần số, bộ khuếch đại nhiễu thấp (LNA) hoặc anten. Theo một phương án của sáng chế, ít nhất một trong số môđun truyền thông di động 221, môđun Wi-Fi 223, môđun BT 225, môđun hệ thống vệ tinh dẫn đường toàn cầu (GNSS) 227, và môđun NFC 228 có thể truyền và tiếp nhận các tín hiệu RF nhờ một môđun RF riêng biệt.

Thẻ SIM 224 có thể là một thẻ có SIM và/hoặc SIM gắn sẵn, và có thể có thông tin nhận dạng duy nhất (ví dụ, bộ nhận dạng thẻ IC (ICCID)) hoặc thông tin thuê bao (ví dụ, dấu hiệu nhận dạng thuê bao di động quốc tế (IMSI)).

Bộ nhớ 230 có thể có, ví dụ, bộ nhớ gắn sẵn 232 hoặc bộ nhớ ngoài. Bộ nhớ gắn sẵn 232 có thể là ít nhất một trong số, ví dụ, bộ nhớ khả biến (ví dụ, bộ nhớ truy nhập ngẫu nhiên động (DRAM), RAM tĩnh (SRAM), DRAM đồng bộ (SDRAM), và bộ nhớ tương tự) và bộ nhớ bất khả biến (ví dụ, bộ nhớ chỉ đọc khả lập trình một lần (OTPROM), PROM, ROM xóa được và khả lập trình (EPROM), ROM xóa được và khả lập trình bằng điện (EEPROM), bộ nhớ tia chớp (ví dụ, bộ nhớ tia chớp NAND hoặc bộ nhớ tia chớp NOR), ổ đĩa cứng, hoặc ổ đĩa mạch rắn (SSD).

Bộ nhớ ngoài 234 còn có thể có ổ đĩa tia chớp, ví dụ, bộ nhớ Compact Flash (CF), bộ nhớ Secure Digital (SD), bộ nhớ micro-SD, bộ nhớ mini-SD, bộ nhớ Extreme Digital (xD), thẻ nhớ, và bộ nhớ tương tự. Bộ nhớ ngoài 234 có thể được nối chức năng và/hoặc vật lý với thiết bị điện tử 201 nhờ các giao diện khác nhau.

Môđun cảm biến 240 có thể đo một đại lượng vật lý hoặc phát hiện trạng thái hoạt động của thiết bị điện tử 201, và có thể biến đổi thông tin đo được hoặc phát hiện được thành một tín hiệu điện. Môđun cảm biến 240 có thể có, ví dụ, ít nhất một trong số bộ cảm biến cử chỉ 240A, bộ cảm biến con quay hồi chuyển 240B, bộ cảm biến áp suất khí quyển 240C, bộ cảm biến từ tính 240D, bộ cảm biến gia tốc 240E, bộ cảm biến trạng thái cầm nắm 240F, bộ cảm biến trạng thái lân cận 240G, bộ cảm biến màu 240H (ví dụ, bộ cảm biến đỏ, xanh, và lục (RGB)), bộ cảm biến sinh trắc học 240I, bộ cảm biến nhiệt độ/độ ẩm 240J, bộ

cảm biến độ sáng 240K, và bộ cảm biến tia cực tím (UV) 240M. Ngoài ra hoặc theo cách khác, môđun cảm biến 240 có thể có, ví dụ, bộ cảm biến mùi điện tử, bộ cảm biến điện đồ cơ (EMG), bộ cảm biến điện não đồ (EEG), bộ cảm biến điện tâm đồ (ECG), bộ cảm biến tia hồng ngoại (IR), máy quét con ngươi, và/hoặc bộ cảm biến vân tay. Môđun cảm biến 240 còn có thể có mạch điều khiển để điều khiển ít nhất một bộ cảm biến có trong đó. Theo một phương án của sáng chế, thiết bị điện tử 201 còn có thể có bộ xử lý được làm thích ứng để điều khiển môđun cảm biến 240 là một phần của hoặc tách rời ra khỏi AP 210, và có thể điều khiển môđun cảm biến 240 trong khi AP 210 ở chế độ ngủ.

Thiết bị đầu vào 250 có thể có, ví dụ, panen xúc giác 252, bộ cảm biến bút (dạng số) 254, phím 256, hoặc thiết bị đầu vào siêu âm 258. Panen xúc giác 252 có thể sử dụng ít nhất một kiểu trong số, ví dụ, kiểu điện dung, kiểu điện trở, kiểu hồng ngoại, và kiểu siêu âm. Panen xúc giác 252 còn có thể có mạch điều khiển. Panen xúc giác 252 còn có thể có lớp xúc giác, và có thể tạo ra phản lực xúc giác đối với người dùng.

Bộ cảm biến bút (dạng số) 254 có thể có, ví dụ, tấm nhận dạng là một phần của panen xúc giác hoặc một tấm nhận dạng riêng biệt. Phím 256 có thể có, ví dụ, nút vật lý, phím quang học hoặc vùng phím. Thiết bị đầu vào siêu âm 258 có thể xác định dữ liệu bằng cách phát hiện sóng siêu âm được tạo ra bởi một bộ phận đầu vào, bằng cách sử dụng một micrô (ví dụ, micrô 288) của thiết bị điện tử 201.

Màn hình 260 (ví dụ, màn hình 160) có thể có panen 262, thiết bị ảnh toàn ký 264 hoặc máy chiếu 266. Panen 262 có thể có một phần tử giống hoặc tương tự với màn hình 160 theo Fig.1. Panen 262 có thể được cải biến sao cho, ví dụ, uốn được, trong suốt, hoặc đeo được. Panen 262 còn có thể được làm thích ứng để được tích hợp với panen xúc giác 252 ở dạng một môđun duy nhất. Thiết bị ảnh toàn ký 264 có thể thể hiện ảnh nổi trong không khí bằng cách sử dụng hiện tượng giao thoa ánh sáng. Máy chiếu 266 có thể chiếu ánh sáng lên một màn ảnh để hiển thị một ảnh. Màn ảnh này có thể được bố trí, ví dụ, bên trong hoặc bên ngoài thiết bị điện tử 201. Theo một phương án của sáng chế, màn hình 260 còn

có thể có mạch điều khiển để điều khiển panen 262, thiết bị ảnh toàn ký 264, hoặc máy chiếu 266.

Giao diện 270 có thể có, ví dụ, giao diện HDMI 272, USB 274, giao diện quang học 276, hoặc giao diện D-subminiature (D-sub) 278. Giao diện 270 có thể có trong, ví dụ, giao diện truyền thông 170 như được thể hiện trên Fig.1. Ngoài ra hoặc theo cách khác, giao diện 270 có thể có, ví dụ, giao diện liên kết chất lượng cao di động (MHL), giao diện thẻ SD/thẻ đa phương tiện (MMC), hoặc giao diện tiêu chuẩn Hiệp hội dữ liệu hồng ngoại (IrDA).

Môđun auđio 280 có thể biến đổi theo hai chiều, ví dụ, âm thanh và tín hiệu điện. Ít nhất một số phần tử của môđun auđio 280 có thể có trong, ví dụ, giao diện nhập/xuất 150 như được thể hiện trên Fig.1. Môđun auđio 280 có thể xử lý đầu vào thông tin âm thanh hoặc xuất ra nhờ, ví dụ, loa 282, bộ thu 284, tai nghe 286, micrô 288, và bộ phận tương tự.

Môđun camêra 291 là thiết bị có khả năng chụp ảnh cả ảnh tĩnh và ảnh viđeo. Theo một phương án của sáng chế, môđun camêra 291 có thể có một hoặc nhiều bộ cảm biến ảnh (ví dụ, bộ cảm biến trước hoặc bộ cảm biến sau), ống kính, bộ xử lý tín hiệu ảnh (ISP) hoặc đèn nháy (ví dụ, đèn LED hoặc đèn xenon).

Môđun quản lý nguồn điện 295 có thể quản lý, ví dụ, nguồn điện của thiết bị điện tử 201. Theo một phương án của sáng chế, môđun quản lý nguồn điện 295 có thể có IC quản lý nguồn điện (PMIC), IC bộ nạp điện, hoặc bộ pin hoặc đồng hồ đo bộ pin. PMIC có thể sử dụng kỹ thuật nạp điện có nối dây và/hoặc nạp điện không dây. Các ví dụ về phương pháp nạp điện không dây có thể có, ví dụ, phương pháp cộng hưởng từ, phương pháp cảm ứng từ, phương pháp điện từ, và phương pháp tương tự. Các mạch bổ sung (ví dụ, mạch vòng cuộn dây, mạch cộng hưởng, bộ chỉnh lưu, và mạch tương tự) để nạp điện không dây có thể được sử dụng. Đồng hồ đo bộ pin có thể đo, ví dụ, dung lượng còn lại của bộ pin 296, điện áp nạp điện, dòng điện, hoặc nhiệt độ. Bộ pin 296 có thể là, ví dụ, bộ pin nạp lại được và/hoặc bộ pin mặt trời.

Bộ chỉ báo 297 có thể thể hiện các trạng thái cụ thể của thiết bị điện tử

201 hoặc một phần (ví dụ, AP 210) của thiết bị điện tử 201, ví dụ, trạng thái khởi động, trạng thái tin nhắn, trạng thái nạp điện, và trạng thái tương tự. Môtơ 298 có thể biến đổi tín hiệu điện thành các rung động cơ học, và có thể tạo ra rung động hoặc tác dụng liên quan tới xúc giác. Mặc dù không được thể hiện trên hình vẽ, thiết bị điện tử 201 có thể có một bộ xử lý (ví dụ, GPU) để hỗ trợ chức năng TV di động. Bộ xử lý để hỗ trợ chức năng TV di động có thể xử lý dữ liệu phương tiện theo tiêu chuẩn của kỹ thuật phát rộng đa phương tiện số (DMB), kỹ thuật phát rộng viđeo số (DVB), luồng dữ liệu, và công nghệ tương tự.

Từng bộ phận của thiết bị điện tử theo sáng chế có thể được thực hiện bởi một hoặc nhiều phần tử và tên của phần tử tương ứng có thể thay đổi phụ thuộc vào kiểu của thiết bị điện tử. Theo các phương án khác nhau của sáng chế, thiết bị điện tử có thể có ít nhất một trong số các phần tử nêu trên. Một số phần tử nêu trên có thể được loại bỏ ra khỏi thiết bị điện tử, hoặc thiết bị điện tử còn có thể có các phần tử bổ sung. Hơn nữa, một số phần tử của thiết bị điện tử theo các phương án khác nhau của sáng chế có thể được kết hợp để tạo ra một thực thể duy nhất, và như vậy, có thể thực hiện theo cách tương đương các chức năng của các phần tử tương ứng trước khi kết hợp.

Fig.3 là sơ đồ khối thể hiện môđun chương trình theo các phương án khác nhau của sáng chế.

Theo Fig.3, theo một phương án của sáng chế, môđun chương trình 310 (ví dụ, chương trình 140) có thể có một hệ điều hành (OS) để điều khiển các tài nguyên liên quan tới thiết bị điện tử (ví dụ, thiết bị điện tử 101) và/hoặc các ứng dụng khác nhau (ví dụ, các chương trình ứng dụng 147) được thực hiện trong hệ điều hành. Hệ điều hành có thể là, ví dụ, Android, iOS, Windows, Symbian, Tizen, Bada, và hệ điều hành tương tự.

Môđun lập trình 310 có thể có phần nhân 320, phần trung gian 330, API 360, và/hoặc ứng dụng 370. Ít nhất một số môđun chương trình 310 có thể được nạp từ trước trong thiết bị điện tử hoặc được tải xuống từ máy chủ (ví dụ, máy chủ 106).

Phần nhân 320 (ví dụ, phần nhân 141) có thể có, ví dụ, bộ quản lý tài nguyên hệ thống 321 hoặc bộ điều vận thiết bị 323. Bộ quản lý tài nguyên hệ thống 321 có thể điều khiển, phân phối, hoặc thu thập các tài nguyên hệ thống. Theo một phương án của sáng chế, bộ quản lý tài nguyên hệ thống 321 có thể có bộ quản lý quy trình, bộ quản lý bộ nhớ, bộ quản lý hệ thống tệp và bộ quản lý tương tự. Bộ điều vận thiết bị 323 có thể có, ví dụ, bộ điều vận màn hình, bộ điều vận camêra, bộ điều vận BT, bộ điều vận bộ nhớ dùng chung, bộ điều vận USB, bộ điều vận vùng phím, bộ điều vận Wi-Fi, bộ điều vận auđio, hoặc bộ điều vận truyền thông giữa quá trình (IPC).

Phần trung gian 330 có thể tạo ra chức năng cần thiết đối với các ứng dụng 370 thông thường hoặc có thể tạo ra các chức năng khác nhau đối với các ứng dụng 370 nhờ API 360 sao cho các ứng dụng 370 có thể sử dụng theo cách hữu hiệu các tài nguyên hệ thống có giới hạn của thiết bị điện tử. Theo một phương án của sáng chế, phần trung gian 330 (ví dụ, phần trung gian 143) có thể có ít nhất một trong số thư viện thời gian hoạt động 335, bộ quản lý ứng dụng 341, bộ quản lý cửa sổ 342, bộ quản lý đa phương tiện 343, bộ quản lý tài nguyên 344, bộ quản lý nguồn điện 345, bộ quản lý cơ sở dữ liệu 346, bộ quản lý gói 347, bộ quản lý khả năng kết nối 348, bộ quản lý thông báo 349, bộ quản lý vị trí 350, bộ quản lý đồ họa 351, và bộ quản lý an ninh 352.

Thư viện thời gian hoạt động 335 có thể có, ví dụ, môđun thư viện mà một bộ biên dịch sử dụng để bổ sung các chức năng mới nhờ ngôn ngữ lập trình trong khi ứng dụng 370 được chạy. Thư viện thời gian hoạt động 335 có thể thực hiện việc quản lý nhập/xuất, quản lý bộ nhớ, chức năng đối với hàm số học, và chức năng tương tự.

Bộ quản lý ứng dụng 341 có thể quản lý, ví dụ, chu kỳ hoạt động của ít nhất một ứng dụng trong số các ứng dụng 370. Bộ quản lý cửa sổ 342 có thể quản lý tài nguyên giao diện người dùng đồ họa (GUI) đối với màn hình. Bộ quản lý đa phương tiện 343 có thể nhận dạng định dạng cần thiết để tái tạo các tệp trữ tin khác nhau, và có thể mã hóa hoặc giải mã một tệp trữ tin bằng cách sử dụng một bộ lập-giải mã thích hợp đối với định dạng tương ứng. Bộ quản lý tài

nguyên 344 có thể quản lý các tài nguyên, chẳng hạn mã nguồn, bộ nhớ, hoặc không gian lưu trữ của ít nhất một ứng dụng trong số các ứng dụng 370.

Bộ quản lý nguồn điện 345 có thể hoạt động cùng với một hệ nhập/xuất cơ sở (BIOS) để quản lý bộ pin hoặc nguồn điện, và có thể tạo ra thông tin nguồn điện cần thiết cho hoạt động của thiết bị điện tử. Bộ quản lý cơ sở dữ liệu 346 có thể tạo ra, tìm kiếm, hoặc thay đổi cơ sở dữ liệu sẽ được sử dụng bởi ít nhất một trong số các ứng dụng 370. Bộ quản lý gói 347 có thể quản lý việc cài đặt hoặc cập nhật các ứng dụng được phân phối ở dạng tệp đóng gói.

Ví dụ, bộ quản lý khả năng kết nối 348 có thể quản lý các kết nối không dây, chẳng hạn Wi-Fi, BT, và kết nối tương tự. Bộ quản lý thông báo 349 có thể hiển thị hoặc báo cáo một sự kiện, chẳng hạn trạng thái tiếp nhận một tin nhắn, một cuộc hẹn, thông báo về trạng thái lân cận, và trường hợp tương tự, đến người dùng mà không bị nhiễu loạn. Bộ quản lý vị trí 350 có thể quản lý thông tin địa điểm của thiết bị điện tử. Bộ quản lý đồ họa 351 có thể quản lý các hiệu ứng đồ họa sẽ được tạo ra cho người dùng và các giao diện người dùng liên quan tới các hiệu ứng đồ họa. Bộ quản lý an ninh 352 có thể tạo ra các chức năng an toàn khác nhau cần thiết đối với hệ thống an ninh, xác nhận người dùng, và chức năng tương tự. Theo một phương án của sáng chế, khi thiết bị điện tử (ví dụ, thiết bị điện tử 101) có chức năng cuộc gọi, phần trung gian 330 còn có thể có bộ quản lý điện thoại để quản lý chức năng cuộc gọi tiếng nói hoặc chức năng cuộc gọi viđeo của thiết bị điện tử.

Phần trung gian 330 có thể có môđun phần trung gian để tạo ra kết hợp của các chức năng khác nhau của các phần tử như nêu trên. Phần trung gian 330 có thể tạo ra môđun chuyên dụng đối với từng loại hệ điều hành để tạo ra một chức năng khác biệt. Ngoài ra, một vài phần tử hiện có có thể được loại bỏ chủ động ra khỏi phần trung gian 330, hoặc một phần tử mới có thể được bổ sung vào phần trung gian 330.

API 360 (ví dụ, API 145) là một tập hợp các chức năng lập trình API, và có thể được tạo ra ở cấu hình khác nhau đối với từng hệ điều hành. Ví dụ, đối với hệ điều hành Android hoặc iOS, một tập hợp API có thể được tạo ra đối với

từng nền. Đối với hệ điều hành Tizen, hai hoặc nhiều hơn tập hợp API có thể được tạo ra đối với từng nền.

Các ứng dụng 370 (ví dụ, các chương trình ứng dụng 147) có thể có, ví dụ, một hoặc nhiều ứng dụng có khả năng tạo ra các chức năng, chẳng hạn Home 371, quay số 372, dịch vụ tin nhắn ngắn (SMS)/dịch vụ tin nhắn đa phương tiện (MMS) 373, tin nhắn tức thời (IM) 374, trình duyệt 375, camêra 376, báo động 377, danh bạ 378, quay số giọng nói 379, thư điện tử 380, lịch 381, máy chơi phương tiện 382, anbum 383, đồng hồ 384, chăm sóc sức khỏe (ví dụ, đo mức hoạt động thể dục hoặc lượng đường máu), thông tin về môi trường (ví dụ, thông tin áp suất khí quyển, độ ẩm, hoặc nhiệt độ), và thông tin độ tương tự.

Theo một phương án của sáng chế, các ứng dụng 370 có thể có ứng dụng (sau đây được gọi là "ứng dụng trao đổi thông tin" cho dễ mô tả) hỗ trợ việc trao đổi thông tin giữa thiết bị điện tử (ví dụ, thiết bị điện tử 101) và thiết bị điện tử bên ngoài (ví dụ, thiết bị điện tử bên ngoài thứ nhất 102 hoặc thiết bị điện tử bên ngoài thứ hai 104). Ứng dụng trao đổi thông tin có thể có, ví dụ, ứng dụng chuyển tiếp thông báo để truyền thông tin định trước tới thiết bị điện tử bên ngoài, hoặc một ứng dụng quản lý thiết bị để quản lý thiết bị điện tử bên ngoài.

Ví dụ, ứng dụng chuyển tiếp thông báo có thể có chức năng phân phối, tới thiết bị bên ngoài điện tử (ví dụ, thiết bị điện tử bên ngoài thứ nhất 102 hoặc thiết bị điện tử bên ngoài thứ hai 104), thông tin thông báo được tạo ra bởi các ứng dụng khác (ví dụ, ứng dụng SMS/MMS, ứng dụng thư điện tử, ứng dụng chăm sóc sức khỏe, ứng dụng thông tin môi trường, và ứng dụng tương tự) của thiết bị điện tử. Hơn nữa, ứng dụng chuyển tiếp thông báo có thể tiếp nhận thông tin thông báo từ, ví dụ, thiết bị điện tử bên ngoài, và có thể cung cấp thông tin thông báo nhận được tới người dùng. Ví dụ, ứng dụng quản lý thiết bị có thể quản lý (ví dụ, cài đặt, xóa, hoặc cập nhật) ít nhất một chức năng của thiết bị điện tử bên ngoài (ví dụ, thiết bị điện tử bên ngoài thứ hai 104) truyền thông với thiết bị điện tử (ví dụ, chức năng Bật/Tắt chính thiết bị điện tử bên ngoài (hoặc một số bộ phận) hoặc chức năng điều chỉnh độ sáng (hoặc độ phân giải) của màn

hình), các ứng dụng hoạt động trong thiết bị điện tử bên ngoài, hoặc các dịch vụ được cung cấp bởi thiết bị điện tử bên ngoài (ví dụ, dịch vụ cuộc gọi và dịch vụ tin nhắn).

Theo một phương án của sáng chế, các ứng dụng 370 có thể có ứng dụng (ví dụ, ứng dụng quản lý sức khỏe) được quy định theo các thuộc tính (ví dụ, các thuộc tính của thiết bị điện tử, chẳng hạn loại của thiết bị điện tử tương ứng với thiết bị y tế di động) của thiết bị điện tử bên ngoài (ví dụ, thiết bị điện tử bên ngoài thứ nhất 102 hoặc thiết bị điện tử bên ngoài thứ hai 104). Theo một phương án của sáng chế, các ứng dụng 370 có thể có ứng dụng nhận được từ thiết bị điện tử bên ngoài (ví dụ, máy chủ 106, hoặc thiết bị điện tử bên ngoài thứ nhất 102 hoặc thiết bị điện tử bên ngoài thứ hai 104). Theo một phương án của sáng chế, các ứng dụng 370 có thể có ứng dụng nạp từ trước hoặc ứng dụng bên thứ ba, có thể được tải xuống từ một máy chủ. Tên của các phần tử của môđun chương trình 310, theo các phương án như nêu trên của sáng chế, có thể thay đổi phụ thuộc vào kiểu của hệ điều hành.

Theo các phương án khác nhau của sáng chế, ít nhất một số môđun chương trình 310 có thể được thực hiện trong phần mềm, phần trung gian, phần cứng, hoặc kết hợp của hai hoặc nhiều hơn trong số chúng. Ít nhất một số môđun lập trình 310 có thể được thực hiện (ví dụ, được chạy) bởi, ví dụ, bộ xử lý (ví dụ, AP 210). Ít nhất một số môđun lập trình 310 có thể có, ví dụ, môđun, chương trình, thường trình, các tập hợp các lệnh, quy trình, và công đoạn tương tự, để thực hiện một hoặc nhiều chức năng.

Thuật ngữ "môđun" được sử dụng theo các phương án của sáng chế có thể là, ví dụ, một phần tử là một hoặc nhiều kết hợp của phần cứng, phần mềm, và phần trung gian. Thuật ngữ “môđun” có thể được hoán đổi với một thuật ngữ khác, chẳng hạn phần tử, phần tử logic, khối logic, bộ phận, hoặc mạch. Thuật ngữ “môđun” có thể là phần tử nhỏ nhất của một bộ phận tích hợp hoặc một phần của nó. Thuật ngữ “môđun” có thể là phần tử nhỏ nhất để thực hiện một hoặc nhiều chức năng hoặc một phần của nó. Thuật ngữ “môđun” có thể được thực hiện bằng cơ khí hoặc điện tử. Ví dụ, thuật ngữ “môđun” theo sáng chế có

thể có ít nhất một trong số chip IC chuyên dụng (ASIC), mảng cổng khả lập trình (FPGA), và thiết bị logic khả lập trình để thực hiện các hoạt động đã biết hoặc sẽ được phát triển sau này.

Theo các phương án khác nhau của sáng chế, ít nhất một số thiết bị (ví dụ, môđun hoặc chức năng của nó) hoặc phương pháp (ví dụ, các hoạt động) theo sáng chế có thể được thực hiện bởi một lệnh lưu trữ trong vật ghi đọc được bằng máy tính bất khả biến ở dạng môđun lập trình. Lệnh, khi được chạy bởi bộ xử lý (ví dụ, bộ xử lý 120), có thể làm cho một hoặc nhiều bộ xử lý thực hiện chức năng tương ứng với lệnh. Vật ghi đọc được bằng máy tính bất khả biến có thể, ví dụ, là bộ nhớ 130.

Các khía cạnh nhất định của sáng chế còn có thể được cải biến ở dạng mã đọc được bằng máy tính trên vật ghi đọc được bằng máy tính bất khả biến. Vật ghi đọc được bằng máy tính bất khả biến là thiết bị nhớ dữ liệu bất kỳ có thể lưu trữ dữ liệu có thể đọc được sau đó nhờ một hệ máy tính. Các ví dụ về vật ghi đọc được bằng máy tính bất khả biến có Bộ nhớ chỉ đọc (ROM), bộ nhớ truy nhập ngẫu nhiên (RAM), ROM đĩa Compact (CD-ROM), băng từ, đĩa mềm, và thiết bị nhớ dữ liệu quang học. Vật ghi đọc được bằng máy tính bất khả biến còn có thể được phân bố trên các hệ máy tính được kết nối mạng sao cho mã đọc được bằng máy tính được lưu trữ và được thực hiện theo cách phân tán. Ngoài ra, các chương trình chức năng, mã, các đoạn mã để hoàn thành sáng chế có thể được dễ dàng dự kiến bởi các nhà lập trình là người có hiểu biết trung bình trong lĩnh vực kỹ thuật này.

Ở phương diện này, cần lưu ý rằng các phương án khác nhau của sáng chế như nêu trên đề cập cụ thể tới việc xử lý dữ liệu đầu vào và tạo ra dữ liệu đầu ra trong chừng mực nhất định. Việc xử lý dữ liệu đầu vào và tạo ra dữ liệu đầu ra này có thể được thực hiện ở phần cứng hoặc phần mềm kết hợp với phần cứng. Ví dụ, các bộ phận điện tử cụ thể có thể được sử dụng trong một thiết bị di động hoặc mạch tương tự hoặc có liên quan để thực hiện các chức năng liên quan tới các phương án khác nhau của sáng chế như nêu trên. Theo cách khác, một hoặc nhiều bộ xử lý hoạt động theo các lệnh lưu trữ có thể thực hiện các chức năng

liên quan tới các phương án khác nhau của sáng chế như nêu trên. Trong trường hợp như vậy, trong phạm vi của sáng chế, các lệnh như vậy có thể được lưu trữ trên một hoặc nhiều vật ghi đọc được bằng bộ xử lý bất khả biến. Các ví dụ về vật ghi đọc được bằng bộ xử lý có ROM, RAM, CD-ROM, băng từ, đĩa mềm, và thiết bị nhớ dữ liệu quang học. Vật ghi đọc được bằng bộ xử lý còn có thể được phân bố trên các hệ máy tính được kết nối mạng sao cho các lệnh được lưu trữ và được thực hiện theo cách phân tán. Ngoài ra, các chương trình máy tính chức năng, các lệnh, và các đoạn lệnh để hoàn thành sáng chế có thể được dễ dàng dự kiến bởi các nhà lập trình là người có hiểu biết trung bình trong lĩnh vực kỹ thuật này.

Môđun lập trình theo sáng chế có thể có một hoặc nhiều bộ phận như nêu trên hoặc còn có thể có các bộ phận bổ sung khác, hoặc một số bộ phận như nêu trên có thể được loại bỏ. Các hoạt động được thực hiện bởi môđun, môđun lập trình, hoặc các phần tử khác theo các phương án khác nhau của sáng chế có thể được thực hiện theo trình tự, song song, lặp lại, hoặc theo cách phân cấp. Hơn nữa, một số hoạt động có thể được thực hiện theo một trình tự khác hoặc có thể được loại bỏ, hoặc các hoạt động khác có thể được bổ sung.

Các phương án khác nhau như đã mô tả trên đây được đưa ra chỉ để mô tả dễ dàng các chi tiết kỹ thuật của sáng chế và trợ giúp việc hiểu rõ sáng chế, và không nhằm giới hạn phạm vi của sáng chế. Do đó, cần phải hiểu rằng tất cả các phương án cải biến và thay đổi hoặc các hình thức cải biến hoặc thay đổi dựa trên ý tưởng kỹ thuật của sáng chế đều nằm trong phạm vi của sáng chế.

Fig.4 là hình vẽ dạng sơ đồ thể hiện hệ thống kết nối an toàn theo các phương án khác nhau của sáng chế. Fig.5 là sơ đồ khối thể hiện thiết bị kết nối an toàn theo các phương án khác nhau của sáng chế. Fig.5 là sơ đồ khối thể hiện thiết bị điện tử thứ nhất 400a và thiết bị điện tử thứ hai 400b theo Fig.4.

Theo Fig.4 và Fig.5, hệ thống kết nối an toàn theo các phương án khác nhau có thể có thiết bị điện tử thứ nhất 400a (ví dụ, thiết bị điện tử 101, thiết bị điện tử bên ngoài thứ nhất 102, hoặc thiết bị điện tử bên ngoài thứ hai 104 theo Fig.1 và thiết bị điện tử 201 theo Fig.2), thiết bị điện tử thứ hai 400b (ví dụ, thiết

bị điện tử 101, thiết bị điện tử bên ngoài thứ nhất 102, hoặc thiết bị điện tử bên ngoài thứ hai 104 theo Fig.1, hoặc thiết bị điện tử 201 theo Fig.2), và thiết bị máy chủ 500 (ví dụ, máy chủ 106 theo Fig.1).

Theo các phương án khác nhau của sáng chế, thiết bị điện tử thứ nhất 400a có thể có bộ xử lý thứ nhất 410, môđun truyền thông tầm gần thứ nhất 411 (ví dụ, môđun BT 225 theo Fig.2), môđun an toàn 412, và bộ nhớ 413.

Theo các phương án khác nhau của sáng chế, bộ xử lý thứ nhất 410 (ví dụ, bộ xử lý 120 theo Fig.1 hoặc AP 201 theo Fig.2) có thể mã hóa thông tin an toàn lưu trữ trong môđun an toàn 412 bằng cách sử dụng khóa giao tiếp giống hệt khóa giao tiếp của thiết bị điện tử thứ hai 400b, và truyền thông tin an toàn đã mã hóa tới thiết bị điện tử thứ hai 400b được kết nối nhờ môđun truyền thông tầm gần thứ nhất 411.

Theo một phương án của sáng chế, ở trạng thái trong đó thiết bị điện tử thứ hai 400b được kết nối nhờ môđun truyền thông tầm gần thứ nhất 411 qua kết nối truyền thông tầm gần thứ nhất (ví dụ, BT), khi thông báo yêu cầu ghép cặp thứ nhất được tiếp nhận từ thiết bị điện tử thứ hai 400b, bộ xử lý thứ nhất 410 có thể truyền, tới thiết bị điện tử thứ hai 400b, thông báo trả lời ghép cặp thứ nhất cùng với thông tin duy nhất (thông tin nhận dạng (ID)) của thiết bị điện tử thứ nhất 400a. Sau khi truyền thông báo trả lời ghép cặp thứ nhất, bộ xử lý thứ nhất 410 có thể tiếp nhận, từ thiết bị điện tử thứ hai 400b, khóa ghép cặp để đăng ký, trên thiết bị máy chủ 500, thiết bị điện tử thứ nhất 400a là thiết bị điện tử được liên kết với thiết bị điện tử thứ hai 400b. Bộ xử lý thứ nhất 410 có thể lưu trữ, trong bộ nhớ 413, khóa ghép cặp được liên kết với thông tin duy nhất (ID) của thiết bị điện tử. Ngoài ra, khóa ghép cặp có thể được lưu trữ trong một bộ nhớ an toàn riêng biệt, chẳng hạn TrustZone, được chuẩn bị trong bộ xử lý thứ nhất 410 từ quan điểm phần mềm. Ngoài ra, khóa ghép cặp có thể được lưu trữ trong môđun an toàn 412, được thiết lập riêng biệt từ quan điểm phần cứng.

Theo một phương án của sáng chế, thông tin duy nhất (ID) của thiết bị điện tử 400a có thể là ít nhất một trong số thông tin duy nhất (ID) của môđun an toàn 412, và thông tin duy nhất (ID) của thông tin an toàn lưu trữ trong môđun

an toàn 412.

Theo một phương án của sáng chế, sau khi truyền thông báo trả lời ghép cặp thứ nhất tới thiết bị điện tử thứ hai 400b, bộ xử lý thứ nhất 410 có thể phát hiện một khóa chính được lưu trữ để được liên kết với thông tin duy nhất (ID) của thiết bị điện tử, từ bộ nhớ 413, có thể tạo ra khóa ghép cặp bằng cách sử dụng khóa chính, và có thể lưu trữ khóa ghép cặp được liên kết với thông tin duy nhất của thiết bị điện tử. Sau khi truyền thông báo trả lời ghép cặp thứ nhất, bộ xử lý thứ nhất 410 có thể tiếp nhận, từ thiết bị điện tử thứ hai 400b, khóa ghép cặp để đăng ký, trên thiết bị máy chủ 500, thiết bị điện tử thứ nhất 400a là thiết bị điện tử được liên kết với thiết bị điện tử thứ hai 400b. Khi khóa ghép cặp lưu trữ trong bộ nhớ 413 và khóa ghép cặp nhận được từ thiết bị điện tử thứ hai 400b là giống nhau, bộ xử lý thứ nhất 410 có thể duy trì lưu trữ khóa ghép cặp. Khi khóa ghép cặp lưu trữ trong bộ nhớ 413 và khóa ghép cặp nhận được từ thiết bị điện tử thứ hai 400b không giống nhau, bộ xử lý thứ nhất 410 có thể truyền, tới thiết bị điện tử thứ hai 400b, thông báo chỉ báo rằng các khóa ghép cặp là khác nhau, và có thể xóa khóa ghép cặp lưu trữ trong bộ nhớ 413.

Theo một phương án của sáng chế, khi thông báo yêu cầu ghép cặp thứ hai được truyền từ thiết bị điện tử thứ hai 400b được kết nối qua kết nối truyền thông tầm gần thứ nhất, bộ xử lý thứ nhất 410 tạo ra số ngẫu nhiên thứ nhất và truyền số ngẫu nhiên thứ nhất này tới thiết bị điện tử thứ hai 400b. Sau khi truyền số ngẫu nhiên thứ nhất tới thiết bị điện tử thứ hai 400b, khi số ngẫu nhiên thứ hai và khóa xác nhận thứ nhất được tiếp nhận từ thiết bị điện tử thứ hai 400b, bộ xử lý thứ nhất 410 có thể tạo ra khóa xác nhận thứ hai bằng cách sử dụng số ngẫu nhiên thứ nhất, số ngẫu nhiên thứ hai, và khóa ghép cặp. Bộ xử lý thứ nhất 410 có thể so sánh khóa xác nhận thứ nhất nhận được từ thiết bị điện tử thứ hai 400b và khóa xác nhận thứ hai, và khi khóa xác nhận thứ nhất và khóa xác nhận thứ hai là giống nhau, bộ xử lý thứ nhất 410 có thể truyền, tới thiết bị điện tử thứ hai 400b, thông báo trả lời ghép cặp thứ hai cùng với thông tin tạo ra khóa giao tiếp.

Theo một phương án của sáng chế, khi khóa xác nhận thứ nhất và khóa

xác nhận thứ hai là giống nhau, bộ xử lý thứ nhất 410 có thể tạo ra khóa giao tiếp bằng cách sử dụng thông tin tạo ra khóa giao tiếp, có thể mã hóa thông tin an toàn lưu trữ trong môđun an toàn 412 bằng cách sử dụng khóa giao tiếp, và có thể truyền thông tin an toàn đã mã hóa tới thiết bị điện tử thứ hai 400b.

Theo một phương án của sáng chế, bộ xử lý thứ nhất 410 có thể tạo ra thông tin tạo ra khóa giao tiếp là ít nhất một trong số thông tin nhãn thời gian (Timestamp) và thông tin số đếm của thiết bị điện tử thứ nhất 400a.

Theo một phương án của sáng chế, bộ xử lý thứ nhất 410 có thể quy định ngày hết hiệu lực của khóa giao tiếp bằng cách sử dụng thông tin nhãn thời gian (Timestamp) từ thông tin tạo ra khóa giao tiếp.

Theo các phương án khác nhau của sáng chế, môđun an toàn 412 có thể lưu trữ thông tin an toàn cần thiết để thực hiện dịch vụ nhờ môđun truyền thông tầm gần thứ hai (ví dụ, môđun NFC 228 theo Fig.2).

Theo một phương án của sáng chế, môđun an toàn 412 có thể có ít nhất một trong số chip phần tử an toàn gắn sẵn (eSE), chip thẻ mạch tích hợp vạn năng (UICC), chip UICC gắn sẵn (eUICC), và chip mô phỏng thẻ chủ (HCE).

Theo một phương án của sáng chế, môđun an toàn 412 có thể lưu trữ khóa ghép cặp để đăng ký, trên thiết bị máy chủ 500, thiết bị điện tử thứ nhất 400a là thiết bị điện tử được liên kết với thiết bị điện tử thứ hai 400b, được tiếp nhận từ thiết bị điện tử thứ hai 400b.

Theo một phương án của sáng chế, môđun an toàn 412 có thể được làm thích ứng để được cố định vào thiết bị điện tử thứ nhất 400a hoặc có thể tháo ra khỏi thiết bị điện tử thứ nhất 400a. Ví dụ, khi môđun an toàn 412 là chip eSE, môđun này có thể được làm thích ứng để được cố định vào thiết bị điện tử thứ nhất 400a, hoặc khi môđun an toàn 412 là chip UICC, môđun này có thể được làm thích ứng để có thể tháo ra khỏi thiết bị điện tử thứ nhất 400a.

Theo các phương án khác nhau của sáng chế, bộ nhớ 413 có thể lưu trữ thông tin duy nhất (ID) của thiết bị điện tử thứ nhất 400a và khóa ghép cặp sẽ được liên kết với nhau, hoặc có thể lưu trữ thông tin duy nhất (ID) của thiết bị điện tử thứ nhất 400a, một khóa chính, và khóa ghép cặp sẽ được liên kết với

nhau.

Theo một phương án của sáng chế, bộ nhớ 413 có thể lưu trữ khóa giao tiếp giống hệt khóa của thiết bị điện tử thứ hai 400b, và có thể lưu trữ ứng dụng (ví dụ, ứng dụng quản lý ghép cặp) có khả năng truyền thông tin an toàn đã mã hóa tới thiết bị điện tử thứ hai 400b bằng cách sử dụng khóa giao tiếp.

Theo các phương án khác nhau của sáng chế, thiết bị điện tử thứ hai 400b có thể có bộ xử lý thứ hai 420, môđun truyền thông tầm gần thứ nhất 421 (ví dụ, môđun BT 225 theo Fig.2), môđun truyền thông tầm gần thứ hai 422 (ví dụ, môđun NFC 228 theo Fig.2), và bộ nhớ 423.

Theo các phương án khác nhau của sáng chế, bộ xử lý thứ hai 420 (ví dụ, bộ xử lý 120 theo Fig.1 hoặc AP 201 theo Fig.2) có thể tiếp nhận thông tin an toàn, đã được mã hóa bằng cách sử dụng khóa giao tiếp, từ thiết bị điện tử thứ nhất 400a được kết nối nhờ môđun truyền thông tầm gần thứ nhất 421, và có thể truyền, tới thiết bị điện tử thứ ba 400c được kết nối nhờ môđun truyền thông tầm gần thứ hai 422, thông tin an toàn được giải mã nhờ khóa giao tiếp giống hệt khóa giao tiếp của thiết bị điện tử thứ nhất 400a.

Theo một phương án của sáng chế, bộ xử lý thứ hai 420 có thể truyền thông báo yêu cầu ghép cặp thứ nhất ở dạng yêu cầu ghép cặp thông thường, tới thiết bị điện tử thứ nhất 400a được kết nối qua kết nối truyền thông tầm gần thứ nhất. Khi thông tin duy nhất (ID) của thiết bị điện tử thứ nhất được tiếp nhận cùng với thông báo trả lời ghép cặp thứ nhất từ thiết bị điện tử thứ nhất 400a, bộ xử lý thứ hai 420 có thể truyền thông tin duy nhất (ID) của thiết bị điện tử thứ nhất tới thiết bị máy chủ 500 cùng với thông tin người dùng của thiết bị điện tử thứ hai (ví dụ, ID và mật khẩu được đăng ký trên máy chủ thứ nhất 510). Khi khóa ghép cặp để đăng ký thiết bị điện tử thứ nhất 400a là thiết bị điện tử được liên kết với thiết bị điện tử thứ hai 400b, được tiếp nhận từ thiết bị máy chủ 500, bộ xử lý thứ hai 420 có thể truyền khóa ghép cặp tới thiết bị điện tử thứ nhất 400a.

Theo một phương án của sáng chế, bộ xử lý thứ hai 420 có thể truyền thông báo yêu cầu ghép cặp thứ hai tới thiết bị điện tử thứ nhất 400a ở dạng yêu

cầu ghép cặp an toàn sau khi truyền khóa ghép cặp tới thiết bị điện tử thứ nhất 400a. Bộ xử lý thứ hai 420 có thể truyền, tới thiết bị máy chủ 500, số ngẫu nhiên thứ nhất được tiếp nhận từ thiết bị điện tử thứ nhất sau khi truyền thông báo yêu cầu ghép cặp thứ hai. Bộ xử lý thứ hai 420 có thể truyền, tới thiết bị điện tử thứ nhất 400a, số ngẫu nhiên thứ hai và khóa xác nhận thứ nhất, được tiếp nhận từ thiết bị máy chủ 500. Khi thông tin tạo ra khóa giao tiếp (ví dụ, thông tin nhãn thời gian hoặc thông tin số đếm) được tiếp nhận cùng với thông báo trả lời ghép cặp thứ hai từ thiết bị điện tử thứ nhất 400a, sau khi truyền số ngẫu nhiên thứ hai và khóa xác nhận thứ nhất, bộ xử lý thứ hai 420 có thể truyền thông tin tạo ra khóa giao tiếp tới thiết bị máy chủ 500. Khi khóa giao tiếp được tiếp nhận từ thiết bị máy chủ 500 sau khi truyền thông tin tạo ra khóa giao tiếp, bộ xử lý thứ hai 420 có thể giải mã, bằng cách sử dụng khóa giao tiếp, thông tin an toàn đã mã hóa được tiếp nhận từ thiết bị điện tử thứ nhất 400a. Bộ xử lý thứ hai 420 truyền thông tin an toàn, được tiếp nhận từ thiết bị điện tử thứ nhất 400a, tới thiết bị điện tử thứ ba 400c (ví dụ, bộ đọc NFC) được kết nối qua kết nối truyền thông tầm gần thứ hai, và hoàn thành việc xác nhận, và thực hiện dịch vụ bằng cách sử dụng thiết bị điện tử thứ ba 400c.

Theo các phương án khác nhau của sáng chế, bộ nhớ 423 có thể lưu trữ thông tin người dùng (ví dụ, ID và mật khẩu) của thiết bị điện tử thứ hai, được đăng ký trên thiết bị máy chủ 500.

Theo một phương án của sáng chế, bộ nhớ 423 có thể lưu trữ khóa giao tiếp giống hệt khóa của thiết bị điện tử thứ nhất 400a, và có thể lưu trữ ứng dụng (ví dụ, ứng dụng quản lý ghép cặp) có khả năng giải mã, bằng cách sử dụng khóa giao tiếp, thông tin an toàn đã mã hóa được tiếp nhận từ thiết bị điện tử thứ nhất 400a.

Theo các phương án khác nhau của sáng chế, thiết bị máy chủ 500 có thể có máy chủ thứ nhất 510 và máy chủ thứ hai 520. Theo một phương án của sáng chế, thiết bị máy chủ 500 có thể được tách rời thành máy chủ thứ nhất 510 và máy chủ thứ hai 520, hoặc máy chủ thứ nhất 510 và máy chủ thứ hai 520 có thể được tích hợp.

Theo các phương án khác nhau của sáng chế, máy chủ thứ nhất 510 có thể đăng ký thiết bị điện tử thứ nhất 400a là thiết bị điện tử được liên kết với thiết bị điện tử thứ hai 400b bằng cách sử dụng khóa ghép cặp, có thể tạo ra khóa giao tiếp để cho phép tiếp nhận thông tin an toàn của thiết bị điện tử thứ nhất, và có thể truyền khóa giao tiếp tới thiết bị điện tử thứ hai 400b.

Theo một phương án của sáng chế, máy chủ thứ nhất 510 có thể có bộ xử lý (không được thể hiện trên hình vẽ), và có thể thực hiện chức năng của một máy chủ quản lý nhắn tin.

Theo một phương án của sáng chế, máy chủ thứ nhất 510 có thể tiếp nhận, từ thiết bị điện tử thứ hai 400b, thông tin người dùng (ví dụ, ID và mật khẩu) của thiết bị điện tử thứ hai 400b và thông tin duy nhất (ID) của thiết bị điện tử thứ nhất 400a. Khi xác định được rằng thông tin người dùng của thiết bị điện tử thứ hai 400b là thông tin được đăng ký trên máy chủ thứ nhất 510, máy chủ thứ nhất 510 xác định rằng việc xác nhận đối với thiết bị điện tử thứ hai 400b là thành công, và có thể lưu trữ thông tin duy nhất (ID) của thiết bị điện tử thứ nhất 400a sẽ được liên kết với thông tin người dùng của thiết bị điện tử thứ hai 400b. Khi việc xác nhận đối với thiết bị điện tử thứ hai 400b là thành công, máy chủ thứ nhất 510 có thể truyền thông tin duy nhất (ID) của thiết bị điện tử thứ nhất 400a tới máy chủ thứ hai 520. Sau khi truyền thông tin duy nhất (ID) của thiết bị điện tử thứ nhất 400a, khi khóa ghép cặp được tiếp nhận từ máy chủ thứ hai 520, máy chủ thứ nhất 510 có thể lưu trữ khóa ghép cặp sẽ được liên kết với thông tin người dùng của thiết bị điện tử thứ hai 400b và thông tin duy nhất (ID) của thiết bị điện tử thứ nhất 400a, và có thể truyền khóa ghép cặp tới thiết bị điện tử thứ hai 400b.

Theo một phương án của sáng chế, sau khi truyền khóa ghép cặp, khi số ngẫu nhiên thứ nhất được tiếp nhận từ thiết bị điện tử thứ hai 400b, máy chủ thứ nhất 510 có thể tạo ra số ngẫu nhiên thứ hai, có thể tạo ra khóa xác nhận thứ nhất bằng cách sử dụng số ngẫu nhiên thứ nhất, số ngẫu nhiên thứ hai, và khóa ghép cặp, và có thể truyền số ngẫu nhiên thứ hai và khóa xác nhận thứ nhất tới thiết bị điện tử thứ hai 400b. Sau khi truyền số ngẫu nhiên thứ hai và khóa xác

nhận thứ nhất, khi thông tin tạo ra khóa giao tiếp được tiếp nhận từ thiết bị điện tử thứ hai 400b, máy chủ thứ nhất 510 có thể tạo ra khóa giao tiếp bằng cách sử dụng thông tin tạo ra khóa giao tiếp, và có thể truyền khóa giao tiếp tới thiết bị điện tử thứ hai 400b.

Theo các phương án khác nhau của sáng chế, máy chủ thứ hai 520 có thể tạo ra khóa ghép cặp bằng cách sử dụng một khóa chính tương ứng với thông tin duy nhất của thiết bị điện tử thứ nhất.

Theo một phương án của sáng chế, máy chủ thứ hai 520 có thể có bộ xử lý (không được thể hiện trên hình vẽ), và có thể thực hiện chức năng của một máy chủ quản lý khóa.

Theo một phương án của sáng chế, khi thông tin duy nhất (ID) của thiết bị điện tử thứ nhất 400a được tiếp nhận từ máy chủ thứ nhất 510, máy chủ thứ hai 520 có thể phát hiện, từ một cơ sở dữ liệu (DB), một khóa chính được lưu trữ để được liên kết với thiết bị điện tử thứ nhất 400a, và có thể truyền khóa ghép cặp được tạo ra bằng cách sử dụng khóa chính tới máy chủ thứ nhất 510.

Theo một phương án của sáng chế, môđun truyền thông tầm gần thứ nhất 411 có thể thực hiện truyền thông tầm gần với thiết bị điện tử thứ hai, môđun an toàn 412 có thể lưu trữ thông tin an toàn, và bộ xử lý thứ nhất 410 có thể được làm thích ứng để tiếp nhận, từ thiết bị điện tử thứ hai, khóa ghép cặp để đăng ký thiết bị điện tử là thiết bị điện tử được liên kết với thiết bị điện tử thứ hai, truyền thông tin tạo ra khóa giao tiếp tới thiết bị điện tử thứ hai khi việc xác nhận đối với thiết bị điện tử thứ hai được hoàn thành bằng cách sử dụng khóa ghép cặp, tạo ra khóa giao tiếp bằng cách sử dụng thông tin tạo ra khóa giao tiếp, và mã hóa thông tin an toàn và truyền thông tin an toàn đã mã hóa tới thiết bị điện tử thứ hai.

Theo các phương án khác nhau của sáng chế, bộ xử lý thứ nhất 410 có thể được làm thích ứng để truyền, tới thiết bị điện tử thứ hai, khi thông báo yêu cầu ghép cặp thứ nhất được tiếp nhận từ thiết bị điện tử thứ hai, thông báo trả lời ghép cặp thứ nhất cùng với thông tin duy nhất của thiết bị điện tử, và lưu trữ, khi khóa ghép cặp được tiếp nhận từ thiết bị điện tử thứ hai, khóa ghép cặp được

liên kết với thông tin duy nhất của thiết bị điện tử.

Theo các phương án khác nhau của sáng chế, bộ xử lý thứ nhất 410 có thể được làm thích ứng để tạo ra số ngẫu nhiên thứ nhất và truyền số ngẫu nhiên thứ nhất được tạo ra tới thiết bị điện tử thứ hai khi thông báo yêu cầu ghép cặp thứ hai được tiếp nhận từ thiết bị điện tử thứ hai, tạo ra, khi số ngẫu nhiên thứ hai và khóa xác nhận thứ nhất được tiếp nhận từ thiết bị điện tử thứ hai, khóa xác nhận thứ hai bằng cách sử dụng số ngẫu nhiên thứ nhất, số ngẫu nhiên thứ hai, và khóa ghép cặp, và truyền, tới thiết bị điện tử thứ hai, khi khóa xác nhận thứ nhất và khóa xác nhận thứ hai là giống nhau, thông báo trả lời ghép cặp thứ hai cùng với thông tin tạo ra khóa giao tiếp.

Theo các phương án khác nhau của sáng chế, bộ xử lý thứ nhất 410 có thể được làm thích ứng để tạo ra, khi khóa xác nhận thứ nhất và khóa xác nhận thứ hai là giống nhau, khóa giao tiếp bằng cách sử dụng thông tin tạo ra khóa giao tiếp.

Theo các phương án khác nhau của sáng chế, thông tin tạo ra khóa giao tiếp là ít nhất một trong số thông tin nhãn thời gian (Timestamp) và thông tin số đếm.

Theo các phương án khác nhau của sáng chế, môđun truyền thông tầm gần thứ nhất 421 có thể thực hiện truyền thông tầm gần với thiết bị điện tử thứ nhất, môđun truyền thông tầm gần thứ hai 422 có thể thực hiện truyền thông tầm gần với thiết bị điện tử thứ ba, và bộ xử lý 420 có thể được làm thích ứng để truyền, khi khóa ghép cặp, để đăng ký thiết bị điện tử thứ nhất là thiết bị điện tử được liên kết với thiết bị điện tử, được tiếp nhận từ thiết bị máy chủ, khóa ghép cặp tới thiết bị điện tử thứ nhất, và truyền, tới thiết bị máy chủ, thông tin tạo ra khóa giao tiếp nhận được từ thiết bị điện tử thứ nhất, giải mã thông tin an toàn đã mã hóa được tiếp nhận từ thiết bị điện tử thứ nhất, bằng cách sử dụng khóa giao tiếp nhận được từ thiết bị máy chủ, và truyền thông tin đã giải mã tới thiết bị điện tử thứ ba.

Timestamp là nhãn thời gian khi thiết bị điện tử thứ nhất xác nhận máy chủ thứ nhất, và là yếu tố được sử dụng khi máy chủ thứ nhất tạo ra khóa giao

tiếp. Timestamp thay đổi đối với từng giao tiếp và như vậy, khóa giao tiếp được tạo ra bằng cách sử dụng Timestamp được tạo ra khác nhau đối với từng thời điểm. Ngoài ra, Timestamp là tham số chuẩn được sử dụng khi máy chủ thứ nhất duy trì giao tiếp trong một khoảng thời gian nhất định, và biểu thị thời khoảng để sử dụng khóa giao tiếp.

Số đếm biểu thị số lần giao tiếp được kết nối với máy chủ thứ nhất cho đến lúc này trong thiết bị điện tử thứ nhất, và là yếu tố được sử dụng khi máy chủ thứ nhất tạo ra khóa giao tiếp. Số đếm liên quan tới kết nối giữa thiết bị điện tử thứ nhất và máy chủ thứ nhất thay đổi theo thời gian và như vậy, khóa giao tiếp được tạo ra khác nhau đối với từng thời điểm. Ngoài ra, máy chủ thứ nhất và thiết bị điện tử thứ nhất có giá trị số đếm bằng nhau và như vậy, khi máy chủ thứ nhất tiếp nhận một giá trị số đếm khác, có xác suất cao là xảy ra kết nối bất thường. Do đó, số đếm có thể phát hiện kết nối bất thường.

Theo các phương án khác nhau của sáng chế, bộ xử lý thứ hai 420 có thể được làm thích ứng để truyền, khi thông báo trả lời ghép cặp thứ nhất được tiếp nhận cùng với thông tin duy nhất của thiết bị điện tử thứ nhất, từ thiết bị điện tử thứ nhất, nhằm đáp lại thông báo yêu cầu ghép cặp thứ nhất, thông tin duy nhất của thiết bị điện tử thứ nhất cùng với thông tin người dùng của thiết bị điện tử tới thiết bị máy chủ, và tiếp nhận khóa ghép cặp từ thiết bị máy chủ.

Theo các phương án khác nhau của sáng chế, bộ xử lý thứ hai 420 có thể được làm thích ứng để truyền, khi số ngẫu nhiên thứ nhất được tiếp nhận từ thiết bị điện tử thứ nhất nhằm đáp lại việc truyền thông báo yêu cầu ghép cặp thứ hai, số ngẫu nhiên thứ nhất tới thiết bị máy chủ, và truyền số ngẫu nhiên thứ hai và khóa xác nhận thứ nhất nhận được từ thiết bị máy chủ tới thiết bị điện tử thứ nhất, và tiếp nhận thông tin tạo ra khóa giao tiếp từ thiết bị điện tử thứ nhất.

Theo các phương án khác nhau của sáng chế, thông tin tạo ra khóa giao tiếp là ít nhất một trong số thông tin nhãn thời gian (Timestamp) và thông tin số đếm.

Theo các phương án khác nhau của sáng chế, bộ xử lý của thiết bị máy chủ 500 có thể được làm thích ứng để tạo ra và lưu trữ khóa ghép cặp để đăng

ký thiết bị điện tử thứ nhất ở trạng thái được liên kết với thiết bị điện tử, bằng cách sử dụng thông tin duy nhất của thiết bị điện tử thứ nhất nhận được từ thiết bị điện tử, và truyền khóa ghép cặp tới thiết bị điện tử, và tạo ra khóa giao tiếp giống hệt khóa giao tiếp của thiết bị điện tử thứ nhất bằng cách sử dụng thông tin tạo ra khóa giao tiếp của thiết bị điện tử thứ nhất nhận được từ thiết bị điện tử, và truyền khóa giao tiếp tới thiết bị điện tử.

Theo các phương án khác nhau của sáng chế, bộ xử lý của thiết bị máy chủ 500 có thể được làm thích ứng để thực hiện, khi thông tin người dùng của thiết bị điện tử và thông tin duy nhất của thiết bị điện tử thứ nhất được tiếp nhận từ thiết bị điện tử, việc xác nhận đối với thiết bị điện tử bằng cách sử dụng thông tin người dùng của thiết bị điện tử, và tạo ra và lưu trữ khóa ghép cặp bằng cách sử dụng một khóa chính tương ứng với thông tin duy nhất của thiết bị điện tử thứ nhất, khi việc xác nhận đối với thiết bị điện tử được hoàn thành.

Theo các phương án khác nhau của sáng chế, bộ xử lý của thiết bị máy chủ 500 có thể được làm thích ứng để tạo ra, khi số ngẫu nhiên thứ nhất được tiếp nhận từ thiết bị điện tử, số ngẫu nhiên thứ hai, tạo ra khóa xác nhận thứ nhất bằng cách sử dụng số ngẫu nhiên thứ nhất, số ngẫu nhiên thứ hai, và khóa ghép cặp, và truyền số ngẫu nhiên thứ hai và khóa xác nhận thứ nhất tới thiết bị điện tử, và tiếp nhận thông tin tạo ra khóa giao tiếp của thiết bị điện tử thứ nhất từ thiết bị điện tử.

Theo các phương án khác nhau của sáng chế, thông tin tạo ra khóa giao tiếp có thể có ít nhất một trong số thông tin nhãn thời gian (Timestamp) và thông tin số đếm.

Fig.6A và Fig.6B là các lưu đồ thể hiện phương pháp đăng ký đối với kết nối an toàn theo các phương án khác nhau của sáng chế.

Theo Fig.6A và Fig.6B, phương pháp đăng ký đối với kết nối an toàn theo các phương án khác nhau của sáng chế được mô tả bằng ví dụ được thực hiện bởi thiết bị điện tử thứ nhất 400a, thiết bị điện tử thứ hai 400b, và thiết bị máy chủ 500 theo Fig.4 và Fig.5. Như được thể hiện trên Fig.6A và Fig.6B, ở bước 611, thiết bị điện tử thứ nhất 400a (ví dụ, bộ xử lý thứ nhất 410) và thiết bị điện

tử thứ hai 400b (ví dụ, bộ xử lý thứ hai 420) được kết nối nhờ kết nối truyền thông tầm gần thứ nhất (ví dụ, truyền thông BT).

Ở bước 612, thiết bị điện tử thứ hai 400b truyền thông báo yêu cầu ghép cặp thứ nhất, là yêu cầu ghép cặp thông thường, tới thiết bị điện tử thứ nhất 400a.

Ở bước 613, thiết bị điện tử thứ nhất 400a truyền, tới thiết bị điện tử thứ hai 400b, thông báo trả lời ghép cặp thứ nhất cùng với thông tin duy nhất (ví dụ, thông tin duy nhất của thông tin an toàn) của thiết bị điện tử thứ nhất.

Ở bước 614, khi thông tin duy nhất của thiết bị điện tử thứ nhất được tiếp nhận từ thiết bị điện tử thứ nhất 400a, thiết bị điện tử thứ hai 400b truyền, tới máy chủ thứ nhất 510, thông tin người dùng (ví dụ, ID và mật khẩu) của thiết bị điện tử thứ hai và thông tin duy nhất của thiết bị điện tử thứ nhất.

Ở bước 615, máy chủ thứ nhất 510 (ví dụ, bộ xử lý) thực hiện việc xác nhận đối với thiết bị điện tử thứ hai dựa trên việc thông tin người dùng của thiết bị điện tử thứ hai 400b có tồn tại trong số các mẩu thông tin người dùng được lưu trữ trong DB của máy chủ thứ nhất 510 hay không.

Ở bước 616, máy chủ thứ nhất 510 xác định rằng việc xác nhận không thành công khi thông tin người dùng của thiết bị điện tử thứ hai 400b không tồn tại trong số các mẩu thông tin người dùng được lưu trữ trong DB của máy chủ thứ nhất 510, và ở bước 617, truyền một thông báo thông tin lỗi tới thiết bị điện tử thứ hai 400b nhằm đáp lại việc xác nhận không thành công.

Ở bước 616, máy chủ thứ nhất 510 xác định rằng việc xác nhận là thành công khi thông tin người dùng của thiết bị điện tử thứ hai 400b tồn tại trong số các mẩu thông tin người dùng được lưu trữ trong DB của máy chủ thứ nhất 510, và ở bước 618, lưu trữ thông tin duy nhất của thiết bị điện tử thứ nhất sẽ được liên kết với thông tin người dùng của thiết bị điện tử thứ hai trong DB của máy chủ thứ nhất.

Ở bước 619, máy chủ thứ nhất 510 truyền thông tin duy nhất của thiết bị điện tử thứ nhất tới máy chủ thứ hai 520.

Ở bước 620, máy chủ thứ hai 520 phát hiện, từ DB của máy chủ thứ hai

520, một khóa chính đã lưu trữ tương ứng với thông tin duy nhất của thiết bị điện tử thứ nhất khi thông tin duy nhất của thiết bị điện tử thứ nhất được tiếp nhận từ máy chủ thứ nhất 510. Máy chủ thứ hai 520 tạo ra khóa ghép cặp (K_P) bằng cách sử dụng khóa chính phát hiện được ở bước 621, và truyền khóa ghép cặp (K_P) tới máy chủ thứ nhất 510 ở bước 622.

Ở bước 623, khi khóa ghép cặp (K_P) được tiếp nhận từ máy chủ thứ hai 520, máy chủ thứ nhất 510 lưu trữ, trong DB của máy chủ thứ nhất, khóa ghép cặp (K_P) sẽ được liên kết với thông tin người dùng của thiết bị điện tử thứ hai và thông tin duy nhất của thiết bị điện tử thứ nhất, nhờ đó đăng ký thiết bị điện tử thứ nhất 400a là thiết bị điện tử được liên kết với thiết bị điện tử thứ hai 400b bằng cách sử dụng khóa ghép cặp (K_P).

Ở bước 624, máy chủ thứ nhất 510 truyền khóa ghép cặp (K_P) tới thiết bị điện tử thứ hai 400b.

Ở bước 625, khi khóa ghép cặp (K_P) để đăng ký thiết bị điện tử thứ nhất 400a là thiết bị điện tử được liên kết với thiết bị điện tử thứ hai 400b được tiếp nhận từ máy chủ thứ nhất 510, thiết bị điện tử thứ hai 400b truyền khóa ghép cặp (K_P) tới thiết bị điện tử thứ nhất 400a.

Ở bước 626, khi khóa ghép cặp (K_P) để đăng ký thiết bị điện tử thứ nhất 400a là thiết bị điện tử liên kết với thiết bị điện tử thứ hai 400b được tiếp nhận từ thiết bị điện tử thứ hai 400b, thiết bị điện tử thứ nhất 400a lưu trữ khóa ghép cặp (K_P) được liên kết với thông tin duy nhất của thiết bị điện tử thứ nhất.

Fig.7A và Fig.7B là các lưu đồ thể hiện phương pháp kết nối an toàn theo các phương án khác nhau của sáng chế.

Theo Fig.7A và Fig.7B, phương pháp kết nối an toàn, theo các phương án khác nhau của sáng chế, được mô tả bằng ví dụ được thực hiện bởi thiết bị điện tử thứ nhất 400a, thiết bị điện tử thứ hai 400b, và thiết bị máy chủ 500 theo Fig.4 và Fig.5. Phương pháp kết nối an toàn theo Fig.7A và Fig.7B, theo các phương án khác nhau của sáng chế, có thể được thực hiện sau khi thực hiện phương pháp đăng ký kết nối an toàn theo Fig.6A và Fig.6B theo các phương án khác nhau của sáng chế. Như được thể hiện trên Fig.7A và Fig.7B, ở bước 711,

thiết bị điện tử thứ nhất 400a (ví dụ, bộ xử lý thứ nhất 410) và thiết bị điện tử thứ hai 400b (ví dụ, bộ xử lý thứ hai 420) có thể được kết nối nhờ kết nối truyền thông tầm gần thứ nhất (ví dụ, truyền thông BT).

Ở bước 712, khi thiết bị điện tử thứ hai 400b truyền thông tin người dùng của thiết bị điện tử thứ hai tới máy chủ thứ nhất 510 qua Web và xác định rằng việc xác nhận là thành công, thiết bị điện tử thứ hai 400b có thể được kết nối với máy chủ thứ nhất 510.

Ở bước 713, sau khi đăng ký theo Fig.6A và Fig.6B, thiết bị điện tử thứ hai 400b có thể truyền thông báo yêu cầu ghép cặp thứ hai, là yêu cầu ghép cặp an toàn, tới thiết bị điện tử thứ nhất 400a.

Ở bước 714, khi thông báo yêu cầu ghép cặp thứ hai được tiếp nhận từ thiết bị điện tử thứ hai 400b, thiết bị điện tử thứ nhất 400a tạo ra số ngẫu nhiên thứ nhất ở bước 714, và truyền số ngẫu nhiên thứ nhất tới thiết bị điện tử thứ hai 400b ở bước 715.

Ở bước 716, khi số ngẫu nhiên thứ nhất được tiếp nhận từ thiết bị điện tử thứ nhất 400a, thiết bị điện tử thứ hai 400b truyền số ngẫu nhiên thứ nhất tới máy chủ thứ nhất 510 (ví dụ, bộ xử lý).

Ở bước 717, khi số ngẫu nhiên thứ nhất được tiếp nhận từ thiết bị điện tử thứ hai 400b, máy chủ thứ nhất 510 tạo ra số ngẫu nhiên thứ hai.

Ở bước 718, máy chủ thứ nhất 510 tạo ra khóa xác nhận thứ nhất (Res_Key) bằng cách sử dụng ít nhất một trong số: số ngẫu nhiên thứ nhất, số ngẫu nhiên thứ hai, và khóa ghép cặp (K_P).

Ở bước 719, máy chủ thứ nhất 510 truyền số ngẫu nhiên thứ hai và khóa xác nhận thứ nhất (Res_Key) tới thiết bị điện tử thứ hai 400b.

Ở bước 720, khi số ngẫu nhiên thứ hai và khóa xác nhận thứ nhất (Res_key) được tiếp nhận từ máy chủ thứ nhất 510, thiết bị điện tử thứ hai 400b truyền số ngẫu nhiên thứ hai và khóa xác nhận thứ nhất (Res_Key) tới thiết bị điện tử thứ nhất 400a.

Ở bước 721, khi số ngẫu nhiên thứ hai và khóa xác nhận thứ nhất (Res_Key) được tiếp nhận từ thiết bị điện tử thứ hai 400b, thiết bị điện tử thứ

nhất 400a tạo ra khóa xác nhận thứ hai (Res_Key) bằng cách sử dụng ít nhất một trong số: số ngẫu nhiên thứ nhất, số ngẫu nhiên thứ hai, và khóa ghép cặp (K_P).

Ở bước 722, thiết bị điện tử thứ nhất 400a so sánh khóa xác nhận thứ nhất nhận được từ thiết bị điện tử thứ hai 400b và khóa xác nhận thứ hai được tạo ra. Khi khóa xác nhận thứ nhất và khóa xác nhận thứ hai là khác nhau ở bước 722, thiết bị điện tử thứ nhất 400a truyền, tới thiết bị điện tử thứ hai 400b, thông báo lỗi chỉ báo rằng các khóa xác nhận là khác nhau ở bước 723. Khi khóa xác nhận thứ nhất và khóa xác nhận thứ hai là giống nhau ở bước 722, thiết bị điện tử thứ nhất 400a truyền thông báo trả lời ghép cặp thứ hai cùng với thông tin tạo ra khóa giao tiếp (ví dụ, thông tin nhãn thời gian (Timestamp) và thông tin số đếm) tới thiết bị điện tử thứ hai 400b ở bước 724.

Ở bước 725, thiết bị điện tử thứ nhất 400a tạo ra khóa giao tiếp (K_S) bằng cách sử dụng thông tin tạo ra khóa giao tiếp (ví dụ, thông tin nhãn thời gian (Timestamp) và thông tin số đếm).

Ở bước 726, khi thông tin tạo ra khóa giao tiếp và thông báo trả lời ghép cặp thứ hai được tiếp nhận từ thiết bị điện tử thứ nhất 400a, thiết bị điện tử thứ hai 400b truyền thông tin tạo ra khóa giao tiếp tới máy chủ thứ nhất 510.

Ở bước 727, khi thông tin tạo ra khóa giao tiếp được tiếp nhận từ thiết bị điện tử thứ hai 400b, máy chủ thứ nhất 510 tạo ra khóa giao tiếp (K_S) bằng cách sử dụng thông tin tạo ra khóa giao tiếp.

Ở bước 728, máy chủ thứ nhất 510 truyền khóa giao tiếp (K_S) tới thiết bị điện tử thứ hai 400b.

Ở bước 729, thiết bị điện tử thứ nhất 400a mã hóa thông tin an toàn lưu trữ trong môđun an toàn 412 của thiết bị điện tử thứ nhất 400a bằng cách sử dụng khóa giao tiếp (K_S) giống hệt khóa của thiết bị điện tử thứ hai 400b, và truyền thông tin an toàn đã mã hóa tới thiết bị điện tử thứ hai 400b. Khi thông tin an toàn đã mã hóa được tiếp nhận từ thiết bị điện tử thứ nhất 400a ở bước 729, thiết bị điện tử thứ hai 400b giải mã thông tin an toàn bằng cách sử dụng khóa giao tiếp.

Ở bước 730, khi thiết bị điện tử thứ hai 400b truyền thông tin an toàn

nhận được từ thiết bị điện tử thứ nhất 400a tới thiết bị điện tử thứ ba 400c (ví dụ, bộ đọc NFC) và xác định rằng việc xác nhận được hoàn thành, thiết bị điện tử thứ hai 400b có thể tiến hành dịch vụ (ví dụ, dịch vụ thanh toán NFC) với thiết bị điện tử thứ ba 400c.

Theo các phương án khác nhau của sáng chế, phương pháp kết nối an toàn của thiết bị điện tử được đề xuất. Phương pháp này có các bước: tiếp nhận khóa ghép cặp để đăng ký thiết bị điện tử khi thiết bị điện tử được liên kết với thiết bị điện tử thứ hai từ thiết bị điện tử thứ hai được kết nối qua kết nối truyền thông tầm gần thứ nhất, truyền thông tin tạo ra khóa giao tiếp tới thiết bị điện tử thứ hai khi việc xác nhận đối với thiết bị điện tử thứ hai được hoàn thành bằng cách sử dụng khóa ghép cặp, và tạo ra khóa giao tiếp bằng cách sử dụng thông tin tạo ra khóa giao tiếp, mã hóa thông tin an toàn nhờ khóa giao tiếp, và truyền thông tin đã mã hóa tới thiết bị điện tử thứ hai.

Theo các phương án khác nhau của sáng chế, hoạt động tiếp nhận khóa ghép cặp bao gồm: truyền, tới thiết bị điện tử thứ hai, khi thông báo yêu cầu ghép cặp thứ nhất được tiếp nhận từ thiết bị điện tử thứ hai, thông báo trả lời ghép cặp thứ nhất cùng với thông tin duy nhất của thiết bị điện tử, và lưu trữ, khi khóa ghép cặp được tiếp nhận từ thiết bị điện tử thứ hai, khóa ghép cặp được liên kết với thông tin duy nhất của thiết bị điện tử.

Theo các phương án khác nhau của sáng chế, hoạt động truyền thông tin tạo ra khóa giao tiếp bao gồm: tạo ra, khi thông báo yêu cầu ghép cặp thứ hai được tiếp nhận từ thiết bị điện tử thứ hai, số ngẫu nhiên thứ nhất và truyền số ngẫu nhiên thứ nhất này tới thiết bị điện tử thứ hai, tạo ra, khi số ngẫu nhiên thứ hai và khóa xác nhận thứ nhất được tiếp nhận từ thiết bị điện tử thứ hai, khóa xác nhận thứ hai bằng cách sử dụng số ngẫu nhiên thứ nhất, số ngẫu nhiên thứ hai, và khóa ghép cặp, và truyền, tới thiết bị điện tử thứ hai, khi khóa xác nhận thứ nhất và khóa xác nhận thứ hai là giống nhau, thông báo trả lời ghép cặp thứ hai cùng với thông tin tạo ra khóa giao tiếp.

Theo các phương án khác nhau của sáng chế, khi khóa xác nhận thứ nhất và khóa xác nhận thứ hai là giống nhau, phương pháp còn có bước tạo ra khóa

giao tiếp bằng cách sử dụng thông tin tạo ra khóa giao tiếp.

Theo các phương án khác nhau của sáng chế, thông tin tạo ra khóa giao tiếp là ít nhất một trong số thông tin nhãn thời gian (Timestamp) và thông tin số đếm.

Theo các phương án khác nhau của sáng chế, sáng chế đề xuất phương pháp kết nối an toàn của thiết bị điện tử. Phương pháp này có các bước: truyền, khi khóa ghép cặp để đăng ký thiết bị điện tử thứ nhất là thiết bị điện tử được liên kết với thiết bị điện tử được tiếp nhận từ thiết bị máy chủ, khóa ghép cặp tới thiết bị điện tử thứ nhất được kết nối qua kết nối truyền thông tầm gần thứ nhất, truyền, tới thiết bị máy chủ, thông tin tạo ra khóa giao tiếp nhận được từ thiết bị điện tử thứ nhất, và giải mã, khi khóa giao tiếp được tiếp nhận từ thiết bị máy chủ, thông tin an toàn đã mã hóa được tiếp nhận từ thiết bị điện tử thứ nhất, bằng cách sử dụng khóa giao tiếp, và truyền thông tin đã giải mã tới thiết bị điện tử thứ ba được kết nối qua kết nối truyền thông tầm gần thứ hai.

Theo các phương án khác nhau của sáng chế, hoạt động truyền tới thiết bị điện tử thứ nhất bao gồm: truyền thông báo yêu cầu ghép cặp thứ nhất, truyền, tới thiết bị máy chủ, thông tin duy nhất của thiết bị điện tử thứ nhất cùng với thông tin người dùng của thiết bị điện tử khi thông báo trả lời ghép cặp thứ nhất được tiếp nhận cùng với thông tin duy nhất của thiết bị điện tử thứ nhất, từ thiết bị điện tử thứ nhất, nhằm đáp lại thông báo yêu cầu ghép cặp thứ nhất, và tiếp nhận khóa ghép cặp từ thiết bị máy chủ.

Theo các phương án khác nhau của sáng chế, hoạt động truyền tới thiết bị máy chủ bao gồm: truyền thông báo yêu cầu ghép cặp thứ hai, truyền, khi số ngẫu nhiên thứ nhất được tiếp nhận từ thiết bị điện tử thứ nhất nhằm đáp lại việc truyền thông báo yêu cầu ghép cặp thứ hai, số ngẫu nhiên thứ nhất tới thiết bị máy chủ, truyền, khi số ngẫu nhiên thứ hai và khóa xác nhận thứ nhất được tiếp nhận từ thiết bị máy chủ, số ngẫu nhiên thứ hai và khóa xác nhận thứ nhất tới thiết bị điện tử thứ nhất, và tiếp nhận thông tin tạo ra khóa giao tiếp từ thiết bị điện tử thứ nhất.

Theo các phương án khác nhau của sáng chế, thông tin tạo ra khóa giao

tiếp là ít nhất một trong số thông tin nhãn thời gian (Timestamp) và thông tin số đếm.

Theo các phương án khác nhau, sáng chế đề xuất phương pháp kết nối an toàn của thiết bị máy chủ. Phương pháp này có các bước: tạo ra và lưu trữ, khi thông tin duy nhất của thiết bị điện tử thứ nhất được tiếp nhận từ thiết bị điện tử, khóa ghép cặp để đăng ký thiết bị điện tử thứ nhất là thiết bị điện tử được liên kết với thiết bị điện tử, bằng cách sử dụng thông tin duy nhất của thiết bị điện tử thứ nhất, và truyền khóa ghép cặp tới thiết bị điện tử, và tạo ra, khi thông tin tạo ra khóa giao tiếp của thiết bị điện tử thứ nhất được tiếp nhận từ thiết bị điện tử, khóa giao tiếp giống hệt khóa giao tiếp của thiết bị điện tử thứ nhất bằng cách sử dụng thông tin tạo ra khóa giao tiếp, và truyền khóa giao tiếp tới thiết bị điện tử.

Theo các phương án khác nhau của sáng chế, hoạt động truyền khóa ghép cặp tới thiết bị điện tử bao gồm: thực hiện, khi thông tin người dùng của thiết bị điện tử và thông tin duy nhất của thiết bị điện tử thứ nhất được tiếp nhận từ thiết bị điện tử, việc xác nhận đối với thiết bị điện tử bằng cách sử dụng thông tin người dùng của thiết bị điện tử, và tạo ra và lưu trữ, khi việc xác nhận đối với thiết bị điện tử được hoàn thành, khóa ghép cặp bằng cách sử dụng một khóa chính tương ứng với thông tin duy nhất của thiết bị điện tử thứ nhất.

Theo các phương án khác nhau của sáng chế, hoạt động truyền khóa giao tiếp tới thiết bị điện tử bao gồm: tạo ra, khi số ngẫu nhiên thứ nhất được tiếp nhận từ thiết bị điện tử, số ngẫu nhiên thứ hai, tạo ra khóa xác nhận thứ nhất bằng cách sử dụng số ngẫu nhiên thứ nhất, số ngẫu nhiên thứ hai, và khóa ghép cặp, truyền số ngẫu nhiên thứ hai và khóa xác nhận thứ nhất tới thiết bị điện tử, và tiếp nhận thông tin tạo ra khóa giao tiếp của thiết bị điện tử thứ nhất từ thiết bị điện tử.

Theo các phương án khác nhau của sáng chế, thông tin tạo ra khóa giao tiếp là ít nhất một trong số thông tin Timestamp và thông tin số đếm.

Mặc dù sáng chế đã được thể hiện và mô tả có dựa vào các phương án khác nhau của nó, người có hiểu biết trung bình trong lĩnh vực kỹ thuật này cần phải hiểu rằng các thay đổi khác nhau về hình thức và chi tiết có thể được tạo ra

mà không nằm ngoài ~~tinh~~ thần và phạm vi của sáng chế như được xác định bằng các điểm yêu cầu bảo hộ kèm theo và các phương án tương đương của chúng.

Yêu cầu bảo hộ

1. Thiết bị điện tử thứ nhất (400a) bao gồm:

môđun truyền thông tầm gần thứ nhất (411) được làm thích ứng để thực hiện truyền thông tầm gần với thiết bị điện tử thứ hai (400b);

môđun an toàn (412) được làm thích ứng để lưu trữ thông tin an toàn; và

bộ xử lý (410) được làm thích ứng để:

khi tin nhắn yêu cầu ghép cặp thứ nhất được tiếp nhận từ thiết bị điện tử thứ hai (400b), điều khiển môđun truyền thông tầm gần thứ nhất (411) để truyền, tới thiết bị điện tử thứ hai (400b), tin nhắn trả lời ghép cặp thứ nhất cùng với thông tin duy nhất của thiết bị điện tử thứ nhất (400a),

thu được và lưu trữ, từ thiết bị máy chủ (500) nhờ thiết bị điện tử thứ hai (400b), khóa ghép cặp để đăng ký thiết bị điện tử thứ nhất (400a) khi đang được liên kết với thiết bị điện tử thứ hai (400b), khi việc xác thực với thiết bị điện tử thứ hai (400b) được hoàn thành dựa trên khóa ghép cặp và tin nhắn yêu cầu ghép cặp thứ hai để ghép cặp an toàn được tiếp nhận từ thiết bị điện tử thứ hai (400b), điều khiển môđun truyền thông tầm gần thứ nhất (411) để truyền thông tin tạo ra khóa giao tiếp tới thiết bị máy chủ (500) nhờ thiết bị điện tử thứ hai (400b),

tạo ra khóa giao tiếp dựa trên thông tin tạo ra khóa giao tiếp,

mã hóa thông tin an toàn dựa trên khóa giao tiếp, và

điều khiển môđun truyền thông tầm gần thứ nhất (411) để truyền thông tin an toàn đã mã hóa tới thiết bị điện tử thứ hai (400b),

trong đó khóa ghép cặp được tạo ra dựa trên thông tin duy nhất của thiết bị điện tử thứ nhất (400a), và

trong đó thông tin duy nhất của thiết bị điện tử thứ nhất (400a) là thông tin duy nhất của môđun an toàn (412).

2. Thiết bị điện tử thứ nhất (400a) theo điểm 1, trong đó bộ xử lý (410) còn được làm thích ứng để:

tạo ra số ngẫu nhiên thứ nhất và truyền số ngẫu nhiên thứ nhất đã tạo ra tới thiết bị điện tử thứ hai (400b) khi tin nhắn yêu cầu ghép cặp thứ hai được tiếp

nhận từ thiết bị điện tử thứ hai (400b),

tạo ra, khi số ngẫu nhiên thứ hai và khóa xác thực thứ nhất được tiếp nhận từ thiết bị điện tử thứ hai (400b), khóa xác thực thứ hai dựa trên số ngẫu nhiên thứ nhất, số ngẫu nhiên thứ hai, và khóa ghép cặp, và

truyền, tới thiết bị máy chủ (500) nhờ thiết bị điện tử thứ hai (400b), khi khóa xác thực thứ nhất và khóa xác thực thứ hai là giống nhau, tin nhắn trả lời ghép cặp thứ hai cùng với thông tin tạo ra khóa giao tiếp.

3. Thiết bị điện tử thứ nhất (400a) theo điểm 2, trong đó bộ xử lý (410) còn được làm thích ứng để:

tạo ra, khi khóa xác thực thứ nhất và khóa xác thực thứ hai là giống nhau, khóa giao tiếp dựa trên thông tin tạo ra khóa giao tiếp.

4. Thiết bị điện tử thứ hai (400b) bao gồm:

môđun truyền thông tầm gần thứ nhất (421) được làm thích ứng để thực hiện truyền thông tầm gần với thiết bị điện tử thứ nhất (400a);

môđun truyền thông tầm gần thứ hai (422) được làm thích ứng để thực hiện truyền thông tầm gần với thiết bị điện tử thứ ba (400c); và

bộ xử lý (420) được làm thích ứng để:

tiếp nhận, bởi môđun truyền thông tầm gần thứ nhất (421), tin nhắn trả lời ghép cặp thứ nhất cùng với thông tin duy nhất của thiết bị điện tử thứ nhất nhằm đáp lại việc truyền tin nhắn yêu cầu ghép cặp thứ nhất tới thiết bị điện tử thứ nhất (400a);

nhằm đáp lại việc truyền thông tin duy nhất tới thiết bị máy chủ (500), thu được, từ thiết bị máy chủ (500), khóa ghép cặp để đăng ký thiết bị điện tử thứ nhất khi đang được liên kết với thiết bị điện tử thứ hai (400b);

điều khiển môđun truyền thông tầm gần thứ nhất (421) để truyền, khi khóa ghép cặp được tiếp nhận từ thiết bị máy chủ (500), khóa ghép cặp tới thiết bị điện tử thứ nhất (400a),

khi việc xác thực đối với thiết bị điện tử thứ hai(400b) được hoàn thành dựa trên khóa ghép cặp, thu được thông tin tạo ra khóa giao tiếp đã tiếp nhận, bởi môđun truyền thông tầm gần thứ nhất (421), từ thiết bị điện tử thứ nhất

(400a) nhằm đáp lại việc truyền tin nhắn yêu cầu ghép cặp thứ hai,

khi thu được thông tin tạo ra khóa giao tiếp, điều khiển môđun truyền thông tầm gần thứ hai (422) để truyền, tới thiết bị máy chủ (500), thông tin tạo ra khóa giao tiếp,

thu được, từ thiết bị máy chủ (500), khóa giao tiếp đã tạo ra dựa trên thông tin tạo ra khóa giao tiếp đã truyền,

giải mã thông tin an toàn đã mã hóa được tiếp nhận từ thiết bị điện tử thứ nhất (400a) dựa trên khóa giao tiếp đã tiếp nhận từ thiết bị máy chủ (500), và

điều khiển môđun truyền thông tầm gần thứ hai (422) để truyền thông tin an toàn đã giải mã tới thiết bị điện tử thứ ba (400c),

trong đó khóa ghép cặp được tạo ra dựa trên thông tin duy nhất của thiết bị điện tử thứ nhất (400a), và

trong đó thông tin duy nhất của thiết bị điện tử thứ nhất (400a) là thông tin duy nhất của môđun an toàn (412) của thiết bị điện tử thứ nhất (400a).

5. Thiết bị điện tử thứ hai (400b) theo điểm 4, trong đó bộ xử lý (420) còn được làm thích ứng để:

truyền, khi tin nhắn trả lời ghép cặp thứ nhất được tiếp nhận cùng với thông tin duy nhất của thiết bị điện tử thứ nhất (400a) từ thiết bị điện tử thứ nhất (400a), thông tin duy nhất của thiết bị điện tử thứ nhất (400a) cùng với thông tin người dùng của thiết bị điện tử thứ hai (400b) tới thiết bị máy chủ (500).

6. Thiết bị điện tử thứ hai (400b) theo điểm 4 hoặc 5, trong đó bộ xử lý (420) còn được làm thích ứng để:

truyền, khi số ngẫu nhiên thứ nhất được tiếp nhận từ thiết bị điện tử thứ nhất (400a) nhằm đáp lại việc truyền tin nhắn yêu cầu ghép cặp thứ hai, số ngẫu nhiên thứ nhất tới thiết bị máy chủ (500), và

truyền số ngẫu nhiên thứ hai và khóa xác thực thứ nhất đã tiếp nhận từ thiết bị máy chủ (500), tới thiết bị điện tử thứ nhất (400a).

7. Thiết bị điện tử thứ hai (400b) theo điểm 4, trong đó thông tin tạo ra khóa giao tiếp bao gồm ít nhất một trong số thông tin nhãn thời gian hoặc thông tin số đếm.

8. Phương pháp kết nối an toàn của thiết bị điện tử thứ nhất (400a), phương pháp này bao gồm các bước:

điều khiển (613) môđun truyền thông tầm gần thứ nhất (411) của thiết bị điện tử thứ nhất (400a) để truyền, tới thiết bị điện tử thứ hai (400b), khi tin nhắn yêu cầu ghép cặp thứ nhất được tiếp nhận từ thiết bị điện tử thứ hai (400b), tin nhắn trả lời ghép cặp thứ nhất cùng với thông tin duy nhất của thiết bị điện tử thứ nhất (400a);

thu được (625) và lưu trữ, khóa ghép cặp để đăng ký thiết bị điện tử thứ nhất (400a) khi đang được liên kết với thiết bị điện tử thứ hai (400b) trong thiết bị máy chủ (500), từ thiết bị máy chủ (500) nhờ thiết bị điện tử thứ hai (400b) được kết nối nhờ truyền thông tầm gần thứ nhất;

khi việc xác thực với thiết bị điện tử thứ hai (400b) được hoàn thành dựa trên khóa ghép cặp và tin nhắn yêu cầu ghép cặp thứ hai để ghép cặp an toàn được tiếp nhận từ thiết bị điện tử thứ hai (400b), điều khiển (712, 713, 724) môđun truyền thông tầm gần thứ nhất(411) để truyền thông tin tạo ra khóa giao tiếp tới thiết bị máy chủ (500) nhờ thiết bị điện tử thứ hai (400b);

tạo ra (725) khóa giao tiếp dựa trên thông tin tạo ra khóa giao tiếp;

mã hóa thông tin an toàn nhờ khóa giao tiếp; và

điều khiển (729) môđun truyền thông tầm gần thứ nhất (411) để truyền thông tin an toàn đã mã hóa tới thiết bị điện tử thứ hai (400b),

trong đó khóa ghép cặp được tạo ra dựa trên thông tin duy nhất của thiết bị điện tử thứ nhất (400a), và

trong đó thông tin duy nhất của thiết bị điện tử thứ nhất (400a) là thông tin duy nhất của môđun an toàn (412) của thiết bị điện tử thứ nhất (400a).

9. Phương pháp theo điểm 8, trong đó bước truyền thông tin tạo ra khóa giao tiếp bao gồm:

tạo ra (714) số ngẫu nhiên thứ nhất và truyền số ngẫu nhiên thứ nhất tới thiết bị điện tử thứ hai (400b), khi tin nhắn yêu cầu ghép cặp thứ hai được tiếp nhận từ thiết bị điện tử thứ hai (400b);

tạo ra (721), khi số ngẫu nhiên thứ hai và khóa xác thực thứ nhất được

tiếp nhận từ thiết bị điện tử thứ hai (400b), khóa xác thực thứ hai dựa trên số ngẫu nhiên thứ nhất, số ngẫu nhiên thứ hai, và khóa ghép cặp; và

truyền (724), tới thiết bị máy chủ (500) nhờ thiết bị điện tử thứ hai (400b), khi khóa xác thực thứ nhất và khóa xác thực thứ hai là giống nhau, tin nhắn trả lời ghép cặp thứ hai cùng với thông tin tạo ra khóa giao tiếp.

10. Phương pháp theo điểm 9, trong đó, khi khóa xác thực thứ nhất và khóa xác thực thứ hai là giống nhau, phương pháp này còn có bước:

tạo ra khóa giao tiếp dựa trên thông tin tạo ra khóa giao tiếp.

11. Phương pháp của thiết bị điện tử thứ hai (400b), phương pháp này bao gồm các bước:

tiếp nhận (613), bởi môđun truyền thông tầm gần thứ nhất (421) của thiết bị điện tử thứ hai (400b), tin nhắn trả lời ghép cặp thứ nhất cùng với thông tin duy nhất của thiết bị điện tử thứ nhất (400a) từ thiết bị điện tử thứ nhất (400a) nhằm đáp lại việc truyền tin nhắn yêu cầu ghép cặp thứ nhất tới thiết bị điện tử thứ nhất (400a);

nhằm đáp lại việc truyền thông tin duy nhất tới thiết bị máy chủ (500), thu được (624), từ thiết bị máy chủ (500), khóa ghép cặp để đăng ký thiết bị điện tử thứ nhất khi đang được liên kết với thiết bị điện tử thứ hai (400b);

điều khiển (625) môđun truyền thông tầm gần thứ nhất (421) để truyền, khi khóa ghép cặp được tiếp nhận từ thiết bị máy chủ (500), khóa ghép cặp tới thiết bị điện tử thứ nhất (400a) được kết nối nhờ truyền thông tầm gần thứ nhất;

khi việc xác thực đối với thiết bị điện tử (400b) được hoàn thành dựa trên khóa ghép cặp, thu được (724) thông tin tạo ra khóa giao tiếp đã tiếp nhận, bởi môđun truyền thông tầm gần thứ nhất (421), từ thiết bị điện tử thứ nhất (400a) nhằm đáp lại việc truyền tin nhắn yêu cầu ghép cặp thứ hai;

khi thu được thông tin tạo ra khóa giao tiếp, điều khiển môđun truyền thông tầm gần thứ hai (422) để truyền thông tin tạo ra khóa giao tiếp tới thiết bị máy chủ (500);

thu được (728), từ thiết bị máy chủ (500), khóa giao tiếp đã tạo ra dựa trên thông tin tạo ra khóa giao tiếp đã truyền,

giải mã thông tin an toàn đã mã hóa được tiếp nhận từ thiết bị điện tử thứ nhất (400a), dựa trên khóa giao tiếp đã tiếp nhận từ thiết bị máy chủ (500); và

điều khiển (730) môđun truyền thông tầm gần thứ hai (422) để truyền thông tin đã giải mã tới thiết bị điện tử thứ ba (400c) được kết nối nhờ truyền thông tầm gần thứ hai,

trong đó khóa ghép cặp được tạo ra dựa trên thông tin duy nhất của thiết bị điện tử thứ nhất (400a), và trong đó thông tin duy nhất của thiết bị điện tử thứ nhất (400a) là thông tin duy nhất của môđun an toàn (412) của thiết bị điện tử thứ nhất (400a).

12. Phương pháp theo điểm 11, trong đó bước truyền tới thiết bị điện tử thứ nhất (400a) bao gồm:

truyền (614), tới thiết bị máy chủ, khi tin nhắn trả lời ghép cặp thứ nhất được tiếp nhận cùng với thông tin duy nhất của thiết bị điện tử thứ nhất (400a) từ thiết bị điện tử thứ nhất (400a), thông tin duy nhất của thiết bị điện tử thứ nhất (400a) cùng với thông tin người dùng của thiết bị điện tử thứ hai (400b).

13. Phương pháp theo điểm 11 hoặc 12, trong đó bước truyền tới thiết bị máy chủ (500) bao gồm:

truyền (716), khi số ngẫu nhiên thứ nhất được tiếp nhận từ thiết bị điện tử thứ nhất (400a) nhằm đáp lại việc truyền tin nhắn yêu cầu ghép cặp thứ hai, số ngẫu nhiên thứ nhất tới thiết bị máy chủ (500); và

truyền (719), khi số ngẫu nhiên thứ hai và khóa xác thực thứ nhất được tiếp nhận từ thiết bị máy chủ (500), số ngẫu nhiên thứ hai và khóa xác thực thứ nhất tới thiết bị điện tử thứ nhất (400a).

Fig.1

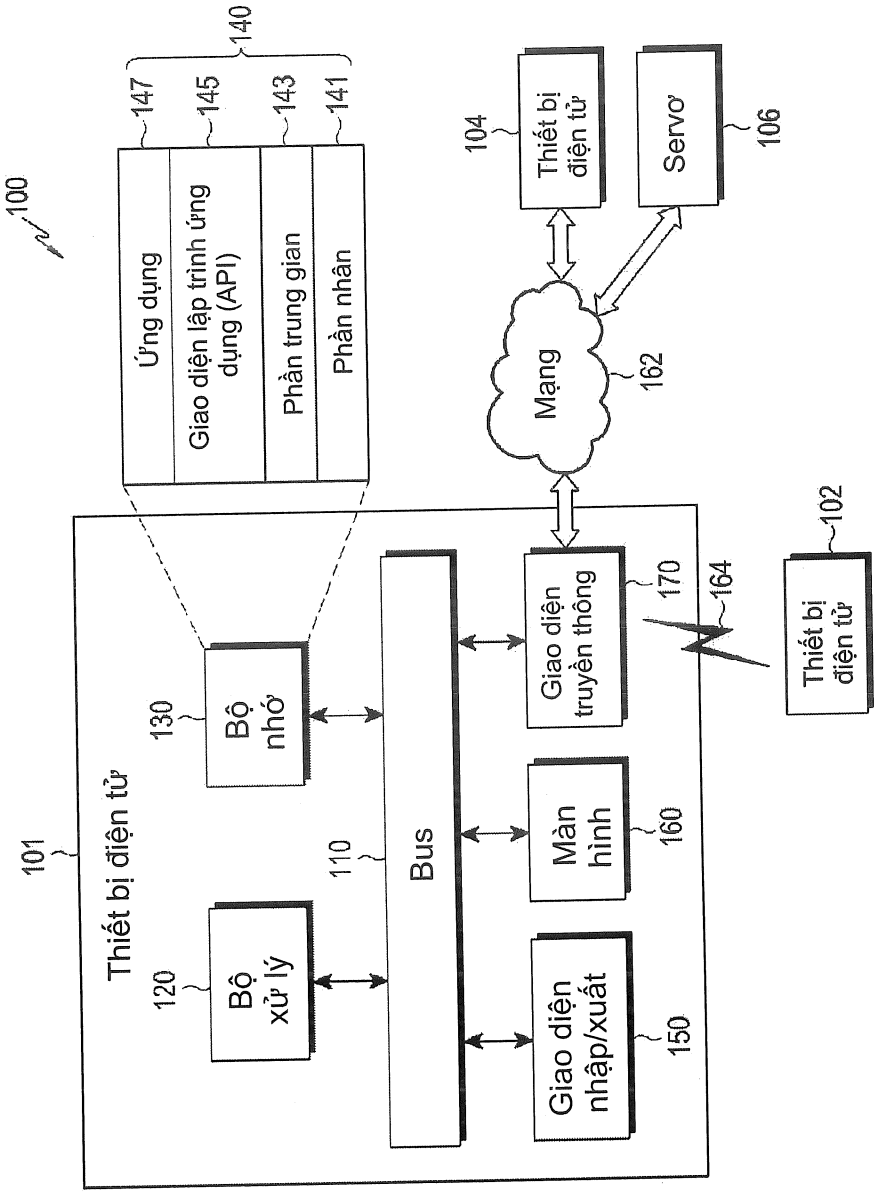

100
140
147
145
143
141
Ứng dụng
Giao diện lập trình ứng dụng (API)
Phần trung gian
Phần nhân
104
Thiết bị điện tử
Servơ
106
Mạng
162
102
Thiết bị điện tử
101
Thiết bị điện tử
130
Bộ nhớ
110
Bus
Giao diện truyền thông
170
164
120
Bộ xử lý
Màn hình
160
Giao diện nhập/xuất
150

Fig.2

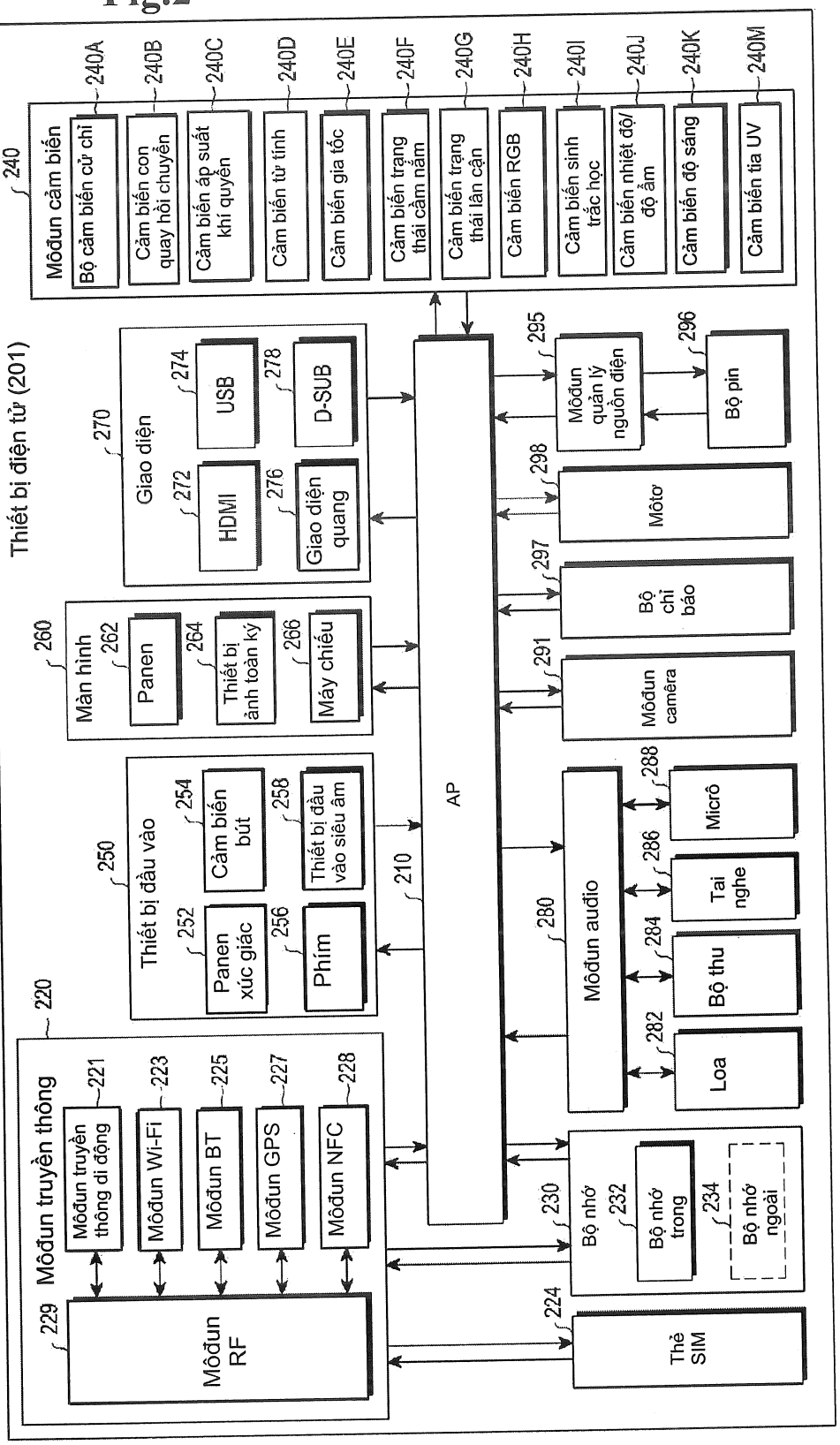

Thiết bị điện tử (201)
AP
210
Môđun cảm biến
240
Bộ cảm biến cử chỉ
240A
Cảm biến con quay hồi chuyển
240B
Cảm biến áp suất khí quyển
240C
Cảm biến từ tính
240D
Cảm biến gia tốc
240E
Cảm biến trạng thái cầm nắm
240F
Cảm biến trạng thái lân cận
240G
Cảm biến RGB
240H
Cảm biến sinh trắc học
240I
Cảm biến nhiệt độ/ độ ẩm
240J
Cảm biến độ sáng
240K
Cảm biến tia UV
240M
Giao diện
270
USB
274
D-SUB
278
HDMI
272
Giao diện quang
276
Màn hình
260
Panen
262
Thiết bị ảnh toàn ký
264
Máy chiếu
266
Thiết bị đầu vào
250
Cảm biến bút
254
Thiết bị đầu vào siêu âm
258
Panen xúc giác
252
Phím
256
Môđun truyền thông
220
Môđun truyền thông di động
221
Môđun Wi-Fi
223
Môđun BT
225
Môđun GPS
227
Môđun NFC
228
Môđun RF
229
Môđun quản lý nguồn điện
295
Bộ pin
296
Môtơ
298
Bộ chỉ báo
297
Môđun camêra
291
Môđun audio
280
Micrô
288
Tai nghe
286
Bộ thu
284
Loa
282
Bộ nhớ
230
Bộ nhớ trong
232
Bộ nhớ ngoài
234
Thẻ SIM
224

Fig.3

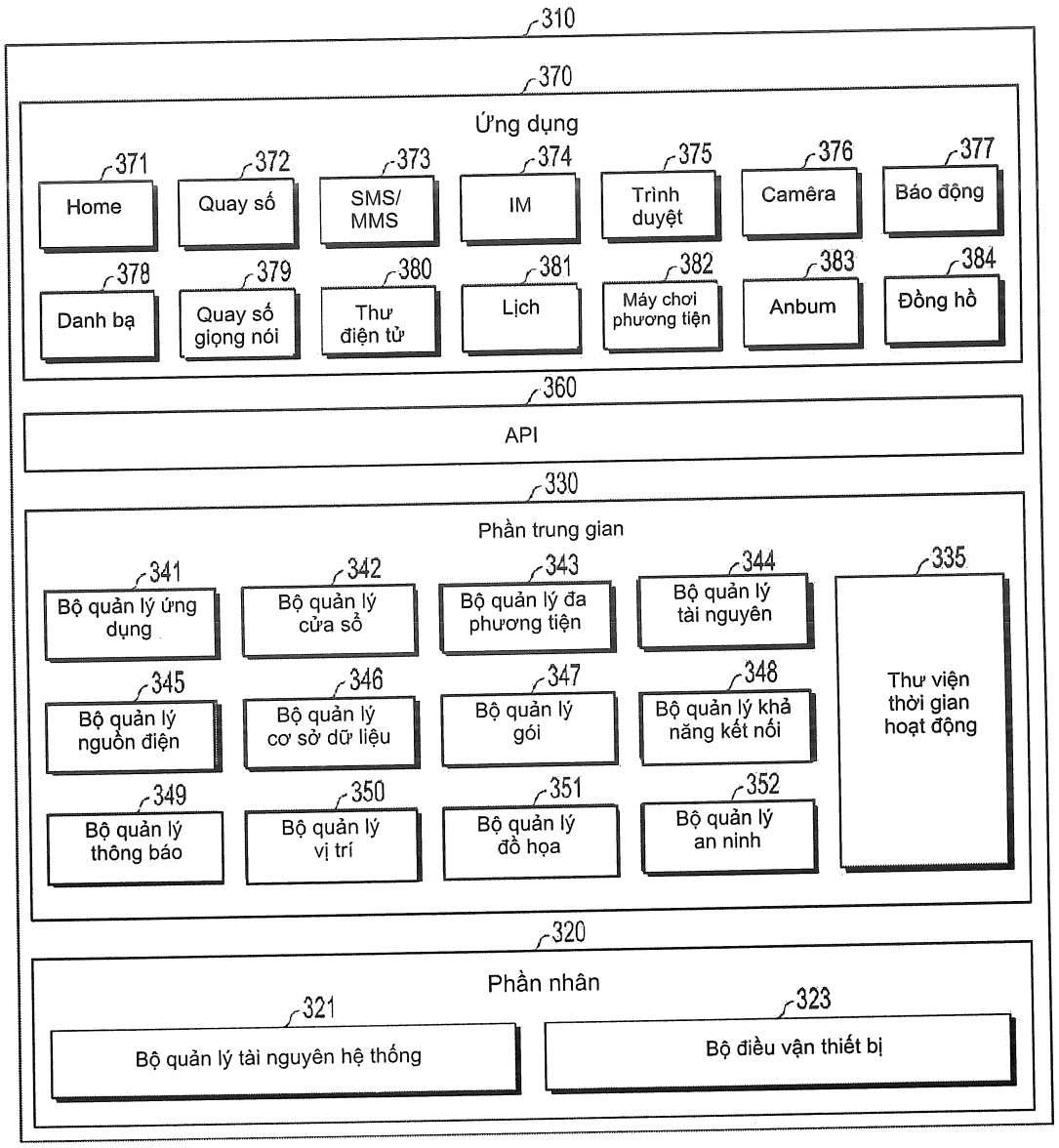

310
370
Ứng dụng
371
Home
372
Quay số
373
SMS/ MMS
374
IM
375
Trình duyệt
376
Camêra
377
Báo động
378
Danh bạ
379
Quay số giọng nói
380
Thư điện tử
381
Lịch
382
Máy chơi phương tiện
383
Anbum
384
Đồng hồ
360
API
330
Phần trung gian
341
Bộ quản lý ứng dụng
342
Bộ quản lý cửa sổ
343
Bộ quản lý đa phương tiện
344
Bộ quản lý tài nguyên
335
Thư viện thời gian hoạt động
345
Bộ quản lý nguồn điện
346
Bộ quản lý cơ sở dữ liệu
347
Bộ quản lý gói
348
Bộ quản lý khả năng kết nối
349
Bộ quản lý thông báo
350
Bộ quản lý vị trí
351
Bộ quản lý đồ họa
352
Bộ quản lý an ninh
320
Phần nhân
321
Bộ quản lý tài nguyên hệ thống
323
Bộ điều vận thiết bị

Fig.4

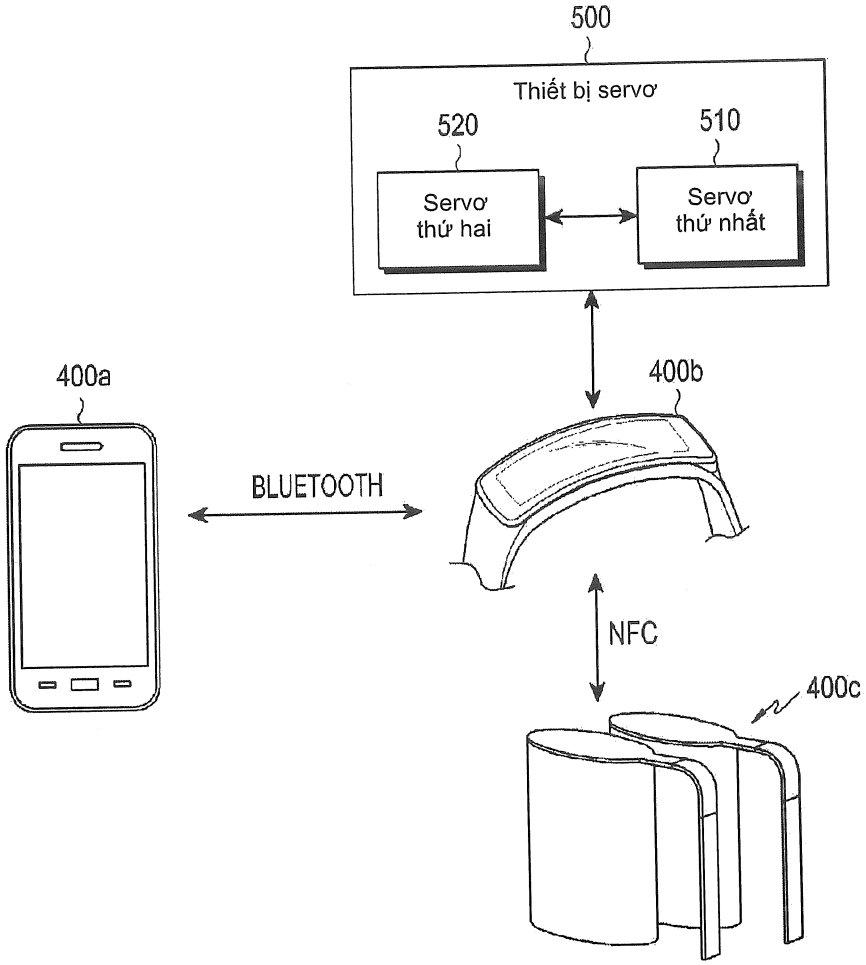

500
Thiết bị servơ
520
510
Servơ thứ hai
Servơ thứ nhất
400a
400b
BLUETOOTH
NFC
400c

Fig.5

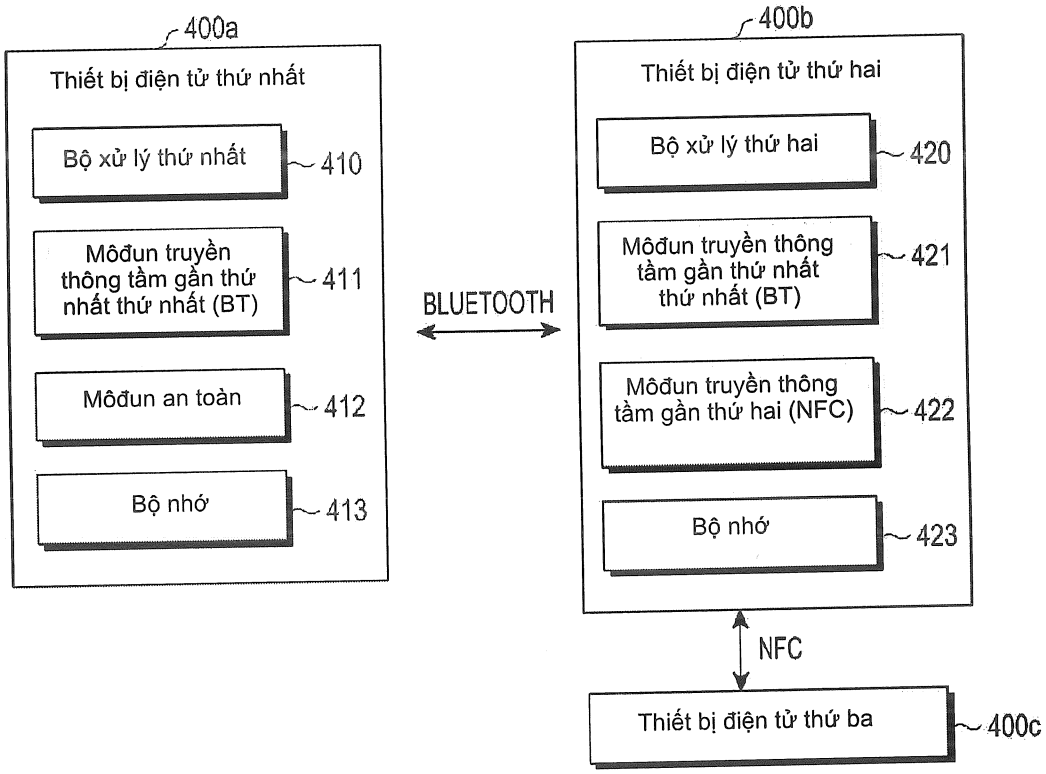

400a
Thiết bị điện tử thứ nhất
Bộ xử lý thứ nhất
410
Môđun truyền thông tầm gần thứ nhất thứ nhất (BT)
411
Môđun an toàn
412
Bộ nhớ
413
BLUETOOTH
400b
Thiết bị điện tử thứ hai
Bộ xử lý thứ hai
420
Môđun truyền thông tầm gần thứ nhất thứ nhất (BT)
421
Môđun truyền thông tầm gần thứ hai (NFC)
422
Bộ nhớ
423
NFC
Thiết bị điện tử thứ ba
400c

Fig.6A

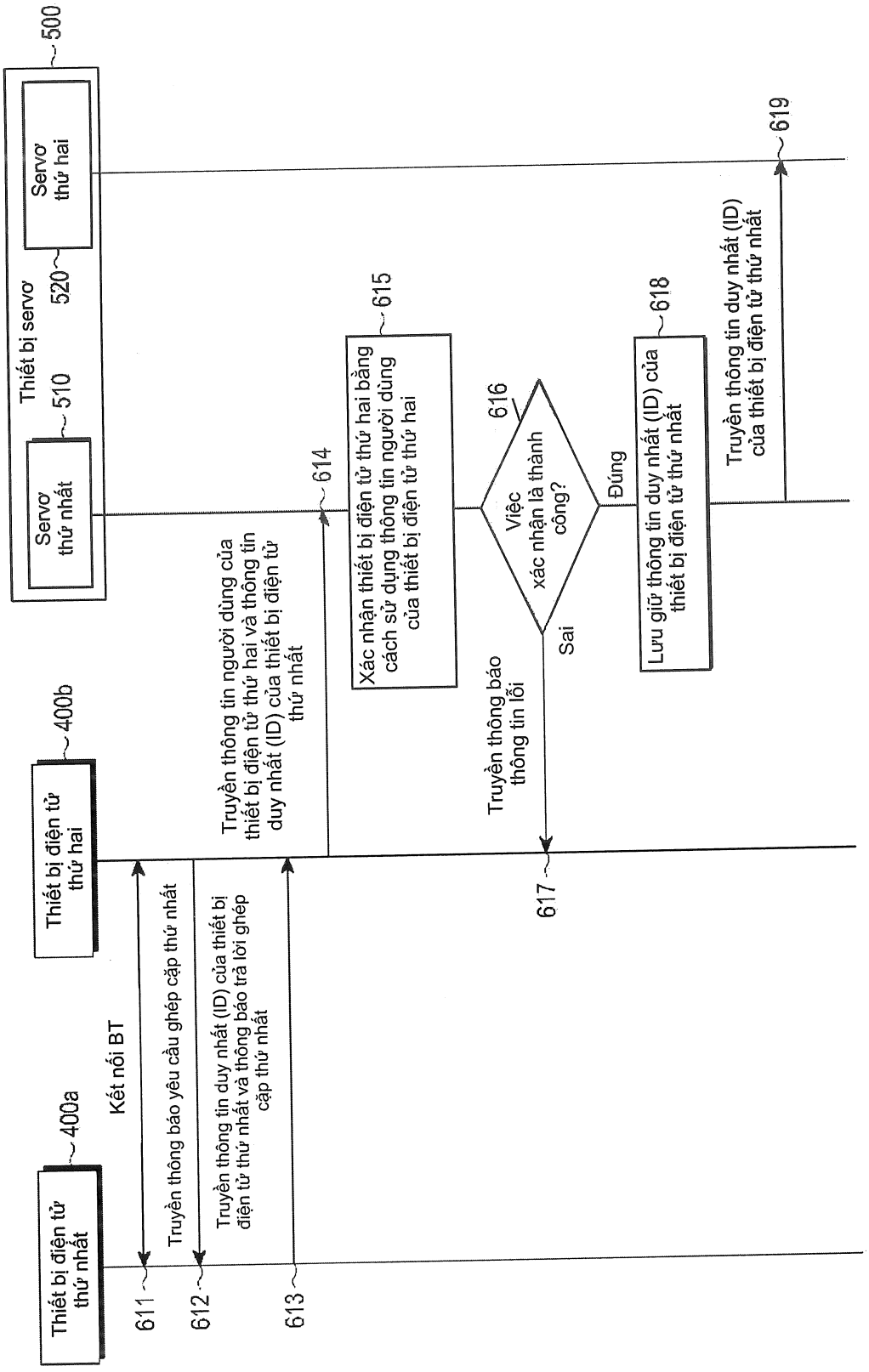

500
Thiết bị servo
Servơ thứ hai
520
Servơ thứ nhất
510
400b
Thiết bị điện tử thứ hai
400a
Thiết bị điện tử thứ nhất
Kết nối BT
Truyền thông báo yêu cầu ghép cặp thứ nhất
Truyền thông tin duy nhất (ID) của thiết bị điện tử thứ nhất và thông báo trả lời ghép cặp thứ nhất
Truyền thông tin người dùng của thiết bị điện tử thứ hai và thông tin duy nhất (ID) của thiết bị điện tử thứ nhất
Xác nhận thiết bị điện tử thứ hai bằng cách sử dụng thông tin người dùng của thiết bị điện tử thứ hai
Việc xác nhận là thành công?
Đúng
Sai
Truyền thông báo thông tin lỗi
Lưu giữ thông tin duy nhất (ID) của thiết bị điện tử thứ nhất
Truyền thông tin duy nhất (ID) của thiết bị điện tử thứ nhất
611
612
613
614
615
616
617
618
619

Fig.6B

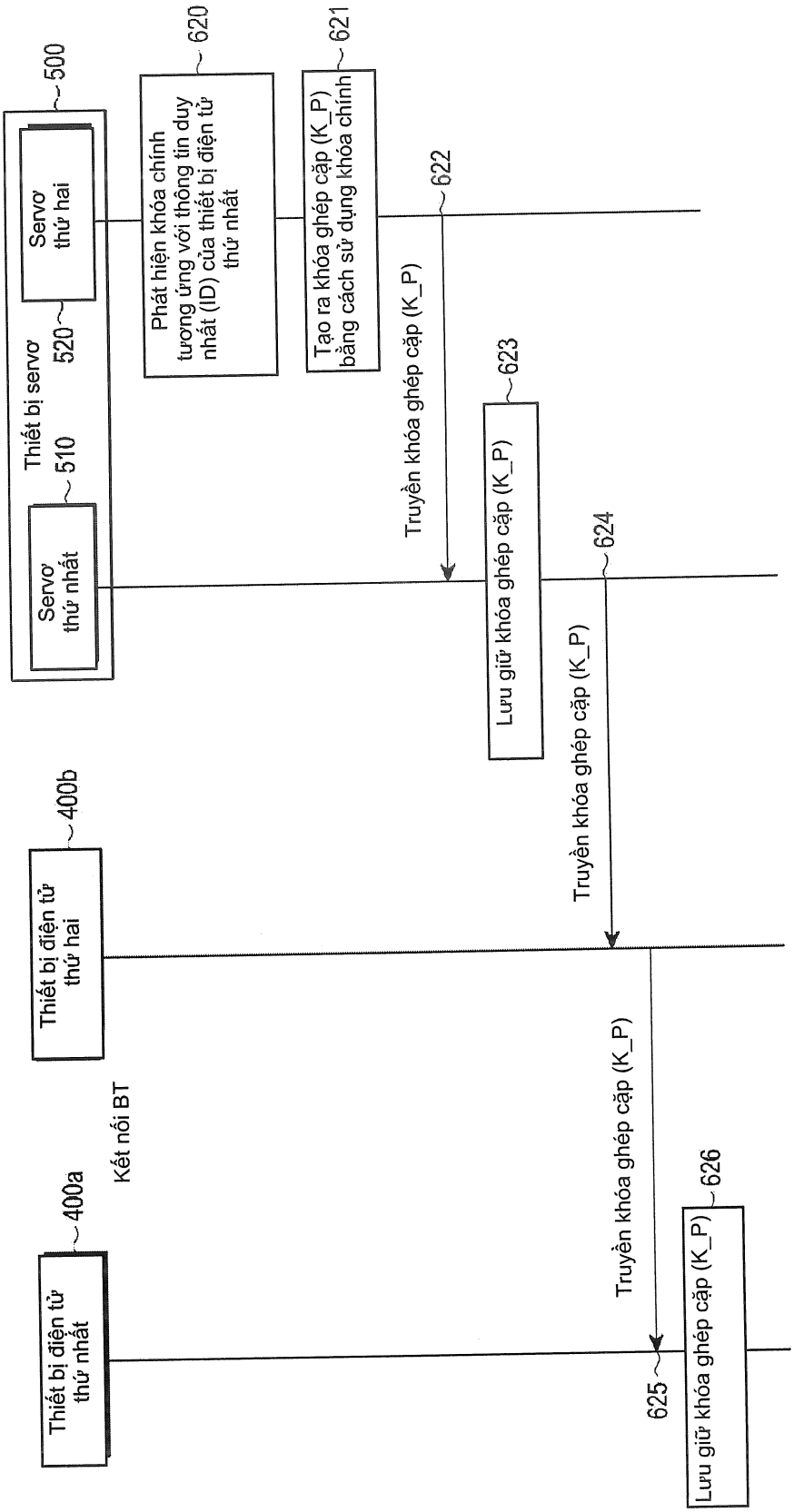

500
Thiết bị servơ
Servơ thứ hai
520
Servơ thứ nhất
510
620
Phát hiện khóa chính tương ứng với thông tin duy nhất (ID) của thiết bị điện tử thứ nhất
621
Tạo ra khóa ghép cặp (K_P) bằng cách sử dụng khóa chính
622
Truyền khóa ghép cặp (K_P)
623
Lưu giữ khóa ghép cặp (K_P)
624
Truyền khóa ghép cặp (K_P)
400b
Thiết bị điện tử thứ hai
Kết nối BT
400a
Thiết bị điện tử thứ nhất
Truyền khóa ghép cặp (K_P)
625
626
Lưu giữ khóa ghép cặp (K_P)

Fig.7A

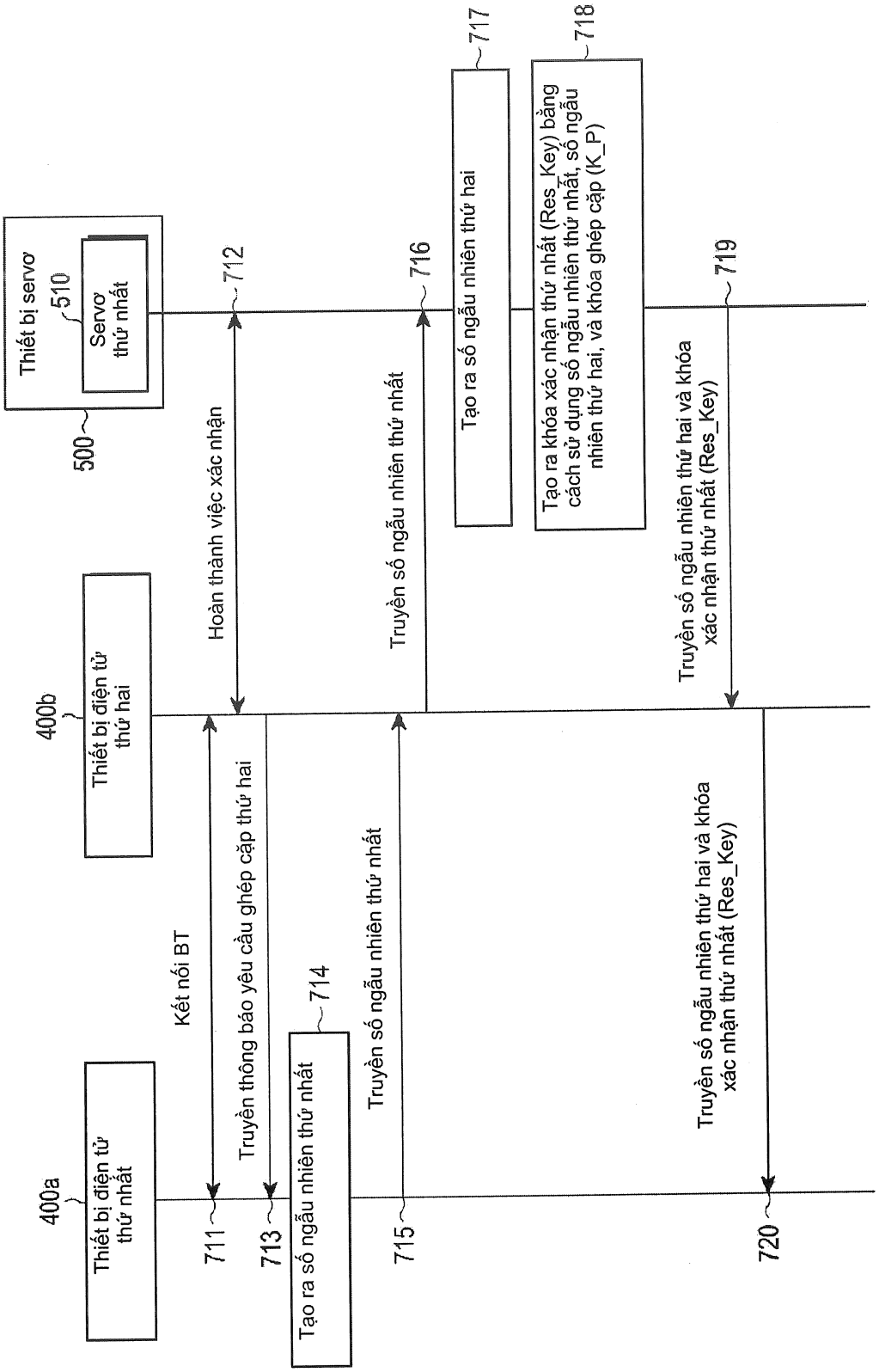
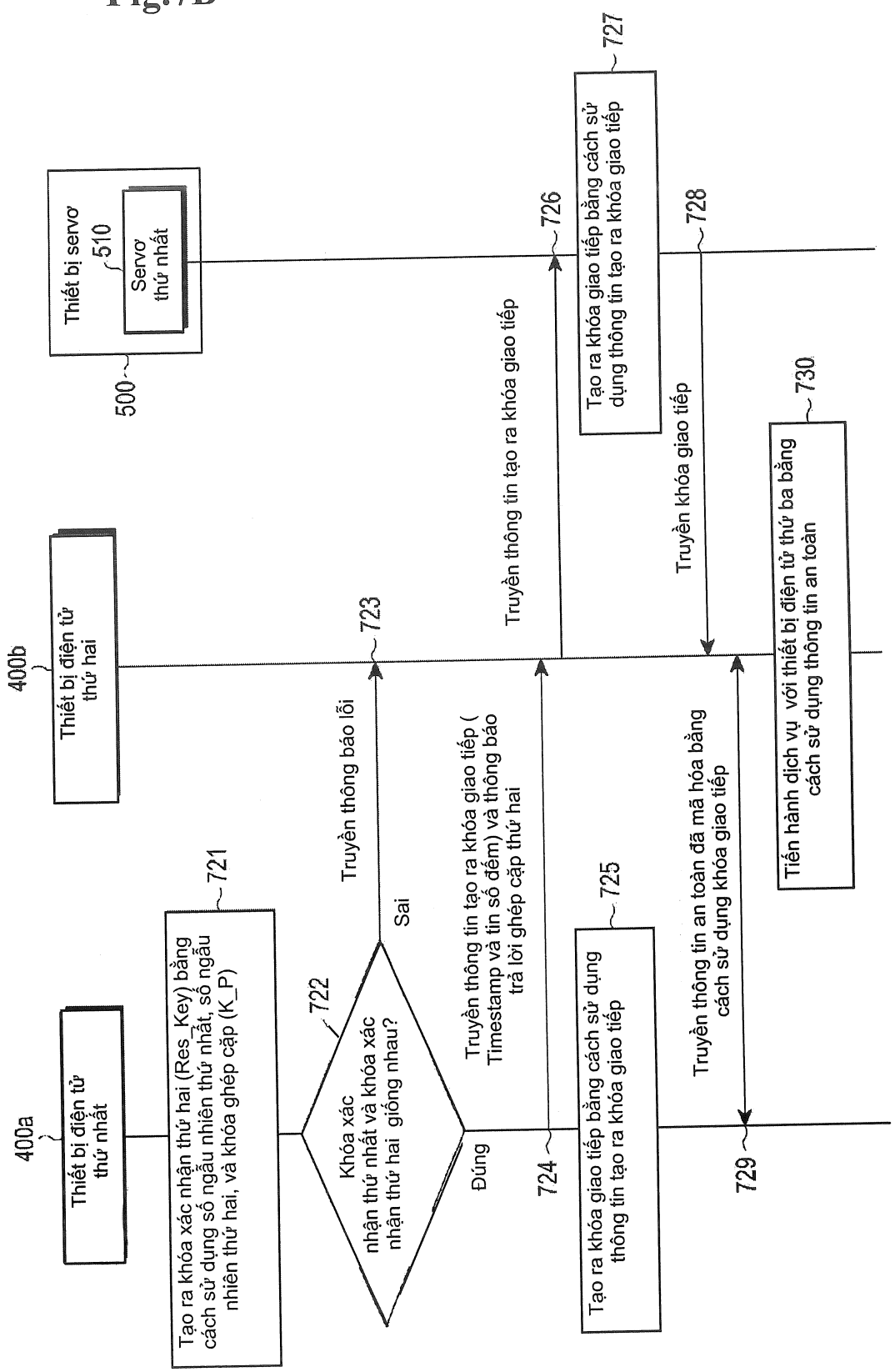

Thiết bị servo
510
Servo thứ nhất
500
712
716
717
718
719
Hoàn thành việc xác nhận
Truyền số ngẫu nhiên thứ nhất
Tạo ra số ngẫu nhiên thứ hai
Tạo ra khóa xác nhận thứ nhất (Res_Key) bằng cách sử dụng số ngẫu nhiên thứ nhất, số ngẫu nhiên thứ hai, và khóa ghép cặp (K_P)
Truyền số ngẫu nhiên thứ hai và khóa xác nhận thứ nhất (Res_Key)
400b
Thiết bị điện tử thứ hai
Kết nối BT
Truyền thông báo yêu cầu ghép cặp thứ hai
Truyền số ngẫu nhiên thứ nhất
Truyền số ngẫu nhiên thứ hai và khóa xác nhận thứ nhất (Res_Key)
400a
Thiết bị điện tử thứ nhất
711
713
714
715
720
Tạo ra số ngẫu nhiên thứ nhất

Fig.7B


Thiết bị servơ
510
Servơ thứ nhất
500
400b
Thiết bị điện tử thứ hai
400a
Thiết bị điện tử thứ nhất
721
Tạo ra khóa xác nhận thứ hai (Res_Key) bằng cách sử dụng số ngẫu nhiên thứ nhất, số ngẫu nhiên thứ hai, và khóa ghép cặp (K_P)
722
Khóa xác nhận thứ nhất và khóa xác nhận thứ hai giống nhau?
Sai
Đúng
723
Truyền thông báo lỗi
724
Truyền thông tin tạo ra khóa giao tiếp (Timestamp và tin số đếm) và thông báo trả lời ghép cặp thứ hai
725
Tạo ra khóa giao tiếp bằng cách sử dụng thông tin tạo ra khóa giao tiếp
726
Truyền thông tin tạo ra khóa giao tiếp
727
Tạo ra khóa giao tiếp bằng cách sử dụng thông tin tạo ra khóa giao tiếp
728
Truyền khóa giao tiếp
729
Truyền thông tin an toàn đã mã hóa bằng cách sử dụng khóa giao tiếp
730
Tiến hành dịch vụ với thiết bị điện tử thứ ba bằng cách sử dụng thông tin an toàn