(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) **1-0051179**

(51)[2021.01] **H04L 29/06**

(13) **B**

(21) 1-2022-05725
(22) 02/11/2020
(86) PCT/CN2020/125973 02/11/2020
(87) WO2021/159765 19/08/2021
(30) 202010088205.5 12/02/2020 CN
(45) 25/09/2025 450
(43) 25/11/2022 416A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, P. R. China
(72) LUO, Meiling (CN); FANG, Xiwen (CN); YANG, Zongjun (CN); ZHOU, Yilei (CN).
(74) Công ty Luật TNHH T&G (TGVN)

(54) PHƯƠNG PHÁP CHIA SẺ DỮ LIỆU TÀI KHOẢN, THIẾT BỊ ĐIỆN TỬ, HỆ THỐNG CHIP VÀ PHƯƠNG TIỆN LƯU TRỮ ĐỌC ĐƯỢC BỞI MÁY TÍNH

(21) 1-2022-05725

(57) Sáng chế đề cập đến phương pháp chia sẻ dữ liệu tài khoản và thiết bị điện tử, và liên quan đến lĩnh vực về các công nghệ truyền thông và lĩnh vực về các công nghệ trí tuệ nhân tạo (Artificial Intelligence, viết tắt là AI), để bảo vệ bảo mật thông tin người dùng và thực hiện một cách thông minh việc chia sẻ tự động của dữ liệu tài khoản. Giải pháp thứ nhất bao gồm: sau khi thiết bị thứ nhất đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất, thiết bị thứ nhất có thể thu thao tác thứ nhất được thực hiện bởi người dùng trên ứng dụng thứ nhất. Thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất, hoặc tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất. Thiết bị thứ nhất có thể hiển thị, đáp lại thao tác thứ nhất, giao diện thứ nhất bao gồm một hoặc nhiều tùy chọn thiết bị. Mỗi tùy chọn thiết bị tương ứng với một thiết bị không dây được tìm thấy bởi thiết bị thứ nhất. Thiết bị thứ nhất có thể gửi, đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất trên giao diện thứ nhất, thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới thiết bị thứ hai tương ứng với tùy chọn thiết bị thứ nhất. Sáng chế cũng đề cập đến hệ thống chip và phương tiện lưu trữ đọc được bởi máy tính.

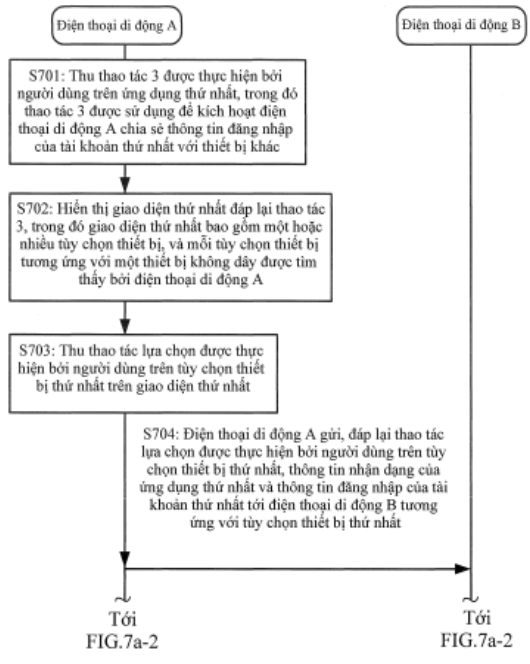

FIG. 7A-1

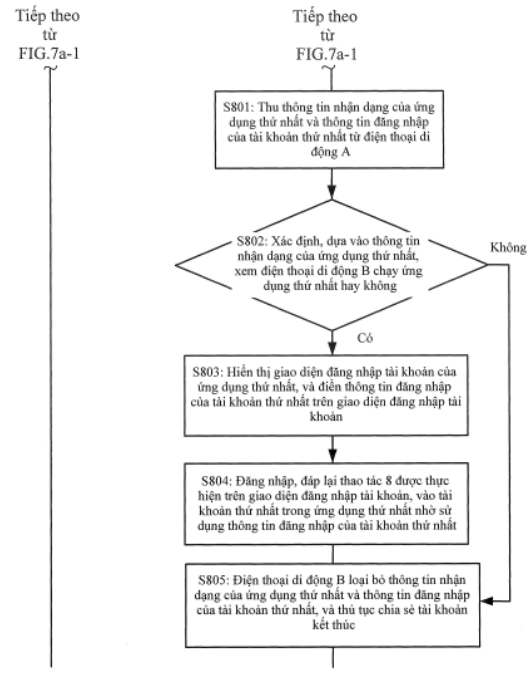

FIG. 7A-2

Lĩnh vực kỹ thuật được đề cập

Các phương án của sáng chế đề cập đến lĩnh vực về các công nghệ truyền thông và lĩnh vực về các công nghệ trí tuệ nhân tạo (Artificial Intelligence, viết tắt là AI), và cụ thể là, đến phương pháp chia sẻ dữ liệu tài khoản và thiết bị điện tử.

Tình trạng kỹ thuật của sáng chế

Với sự phát triển về các công nghệ điện tử và sự cải thiện về tính năng thiết bị điện tử, nhiều ứng dụng hơn có thể được cài đặt trong thiết bị điện tử (chẳng hạn như điện thoại di động, máy thu hình, hoặc máy tính bảng). Sau khi bắt đầu ứng dụng và hiển thị giao diện đăng nhập của ứng dụng (ví dụ, ứng dụng a), thiết bị điện tử có thể thu tài khoản và mật khẩu đăng nhập của tài khoản mà được nhập bởi người dùng trên giao diện đăng nhập. Sau đó, thiết bị điện tử có thể khởi tạo yêu cầu đăng nhập tới máy chủ dựa vào tài khoản và mật khẩu đăng nhập, để đăng nhập vào tài khoản. Ví dụ, ứng dụng a có thể là ứng dụng mua sắm, ứng dụng nhắn tin nhanh, hoặc ứng dụng viđeo.

Sau khi đăng nhập tới một tài khoản trong ứng dụng a trong thiết bị điện tử 1 (ví dụ, điện thoại di động A), người dùng có thể muốn đăng nhập vào tài khoản trong ứng dụng a trong thiết bị điện tử 2 (ví dụ, điện thoại di động B hoặc máy thu hình). Trong trường hợp này, sau khi thiết bị điện tử 2 hiển thị giao diện đăng nhập của ứng dụng a, người dùng cần nhập tài khoản chính xác và mật khẩu đăng nhập lại để đăng nhập vào tài khoản trong thiết bị điện tử 2.

Tuy nhiên, bởi vì nhiều ứng dụng được cài đặt trong thiết bị điện tử, nên khó để người dùng ghi nhớ chính xác tài khoản và mật khẩu đăng nhập của mỗi ứng dụng. Ngoài ra, một số thiết bị điện tử (ví dụ, các máy thu hình) bị giới hạn bởi các dạng vật lý của các thiết bị điện tử, và do đó tài khoản và mật khẩu đăng nhập không thể được nhập một cách thuận lợi. Do đó, giải pháp để chia sẻ tự động tài khoản và mật khẩu đăng nhập được yêu cầu.

Bản chất kỹ thuật của sáng chế

Các phương án của sáng chế đề cập đến phương pháp chia sẻ dữ liệu tài khoản

và thiết bị điện tử, để bảo vệ bảo mật thông tin người dùng và thực hiện một cách thông minh việc chia sẻ tự động của dữ liệu tài khoản.

Theo khía cạnh thứ nhất, sáng chế đề xuất phương pháp chia sẻ dữ liệu tài khoản. Phương pháp có thể được áp dụng cho thiết bị thứ nhất, và ứng dụng thứ nhất được cài đặt trong thiết bị thứ nhất. Sau khi đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất, thiết bị thứ nhất có thể thu thao tác thứ nhất được thực hiện bởi người dùng trên ứng dụng thứ nhất. Thao tác thứ nhất được sử dụng để kích hoạt thiết bị thứ nhất chia sẻ thông tin đăng nhập của tài khoản thứ nhất với thiết bị khác. Thiết bị thứ nhất có thể hiển thị, đáp lại thao tác thứ nhất, giao diện thứ nhất bao gồm một hoặc nhiều tùy chọn thiết bị. Mỗi tùy chọn thiết bị trên giao diện thứ nhất tương ứng với một thiết bị không dây được tìm thấy bởi thiết bị thứ nhất. Thiết bị thứ nhất có thể gửi, đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất trên giao diện thứ nhất, thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới thiết bị thứ hai tương ứng với tùy chọn thiết bị thứ nhất. Thông tin nhận dạng của ứng dụng thứ nhất bao gồm tên gói của ứng dụng thứ nhất, và tên gói của ứng dụng thứ nhất được sử dụng để nhận dạng ứng dụng thứ nhất. Theo cách này, thiết bị thứ hai có thể xác định, dựa vào tên gói của ứng dụng thứ nhất, rằng thông tin đăng nhập của tài khoản thứ nhất là thông tin đăng nhập của một tài khoản của ứng dụng thứ nhất.

Theo kịch bản ứng dụng thứ nhất của sáng chế, thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất. Theo kịch bản ứng dụng, thiết bị thứ nhất đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất.

Theo kịch bản ứng dụng thứ hai của sáng chế, thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất, nhưng thông tin đăng nhập của tài khoản thứ nhất không bao gồm mật khẩu đăng nhập của tài khoản thứ nhất. Theo kịch bản ứng dụng, thiết bị thứ nhất đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mã xác thực. Tài khoản thứ nhất có thể là số điện thoại, địa chỉ thư điện tử, hoặc tương tự.

Theo phương pháp được đề xuất trong sáng chế, máy khách và máy chủ của ứng dụng bất kỳ (ví dụ, ứng dụng thứ nhất) không cần được phát triển thêm, và thiết bị thứ nhất

có thể chia sẻ thông tin đăng nhập của ứng dụng thứ nhất với thiết bị khác (ví dụ, thiết bị thứ hai) đáp lại thao tác thứ nhất được thực hiện bởi người dùng trên ứng dụng (ví dụ, ứng dụng thứ nhất). Nói cách khác, theo phương pháp, thiết bị điện tử có thể chia sẻ một cách thích hợp thông tin đăng nhập của ứng dụng được lựa chọn bởi người dùng với thiết bị khác. Điều này có thể nâng cao độ bảo mật thông tin trong thiết bị điện tử.

Ngoài ra, thiết bị thứ nhất có thể chia sẻ trực tiếp thông tin đăng nhập của tài khoản thứ nhất với thiết bị thứ hai, và thông tin đăng nhập của tài khoản thứ nhất không cần được truyền nhờ sử dụng máy chủ. Điều này có thể ngăn ngừa thông tin đăng nhập của tài khoản thứ nhất khỏi bị đánh cắp ở phía máy chủ, và có thể bảo vệ bảo mật thông tin người dùng.

Tóm lại, theo phương pháp trong sáng chế, thiết bị điện tử có thể chia sẻ tài khoản và mật khẩu đăng nhập của ứng dụng bất kỳ trong thiết bị điện tử với thiết bị khác mà không phải triển thêm máy khách và máy chủ của ứng dụng, và bảo mật thông tin người dùng có thể được bảo vệ. Nói cách khác, phương pháp trong sáng chế có thể bảo vệ bảo mật thông tin người dùng và thực hiện một cách thông minh việc chia sẻ tự động của dữ liệu tài khoản.

Dựa vào khía cạnh thứ nhất, theo cách thiết kế khả thi, thao tác thứ nhất có thể là thao tác được thiết đặt trước được thực hiện trên biểu tượng của ứng dụng thứ nhất. Trước khi thiết bị thứ nhất thu thao tác thứ nhất được thực hiện bởi người dùng trên ứng dụng thứ nhất, thiết bị thứ nhất có thể hiển thị màn hình chính của thiết bị thứ nhất. Màn hình chính bao gồm biểu tượng của ứng dụng thứ nhất. Thiết bị thứ nhất có thể thu thao tác được thiết đặt trước (nghĩa là, thao tác thứ nhất) được thực hiện trên biểu tượng của ứng dụng thứ nhất trên màn hình chính. Ví dụ, thao tác thứ nhất có thể là thao tác bất kỳ chẳng hạn như thao tác nhấn đúp hoặc thao tác chạm và giữ được thực hiện bởi người dùng trên biểu tượng của ứng dụng thứ nhất.

Theo cách khác, thao tác thứ nhất là thao tác nhấn được thực hiện trên sự điều khiển được thiết đặt trước trong ứng dụng thứ nhất. Trước khi thiết bị thứ nhất thu thao tác thứ nhất được thực hiện bởi người dùng trên ứng dụng thứ nhất, thiết bị thứ nhất có thể hiển thị trang được thiết đặt trước của ứng dụng thứ nhất. Trang được thiết đặt trước bao gồm sự điều khiển được thiết đặt trước. Sự điều khiển được thiết đặt trước được sử dụng

để kích hoạt thiết bị thứ nhất chia sẻ thông tin đăng nhập với thiết bị khác. Ví dụ, thao tác thứ nhất có thể là thao tác nhấn được thực hiện bởi người dùng trên sự điều khiển được thiết đặt trước trên trang được thiết đặt trước của ứng dụng thứ nhất.

Có thể hiểu rằng người dùng có thể nhập một cách lựa chọn thao tác thứ nhất trên ứng dụng bất kỳ trong thiết bị thứ nhất, để kích hoạt thiết bị thứ nhất chia sẻ một cách thích hợp thông tin đăng nhập của ứng dụng được lựa chọn bởi người dùng với thiết bị khác.

Dựa vào khía cạnh thứ nhất, theo cách thiết kế khả thi khác, dựa vào kịch bản ứng dụng thứ nhất nêu trên, thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất.

Theo kịch bản ứng dụng thứ nhất, trước khi thiết bị thứ nhất thu thao tác thứ nhất được thực hiện bởi người dùng trên ứng dụng thứ nhất, thiết bị thứ nhất có thể thu dữ liệu tài khoản (bao gồm tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất) được nhập bởi người dùng trên giao diện đăng nhập tài khoản của ứng dụng thứ nhất, và thiết bị thứ nhất có thể đăng nhập, đáp lại thao tác đăng nhập được thực hiện bởi người dùng trên giao diện đăng nhập tài khoản, vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất.

Dựa vào khía cạnh thứ nhất, theo cách thiết kế khả thi khác, dựa vào kịch bản ứng dụng thứ hai nêu trên, thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất nhưng không bao gồm mật khẩu đăng nhập của tài khoản thứ nhất. Ví dụ, tài khoản thứ nhất bao gồm ít nhất số điện thoại hoặc địa chỉ thư điện tử của thiết bị thứ nhất.

Theo kịch bản ứng dụng thứ hai, trước khi thiết bị thứ nhất thu thao tác thứ nhất được thực hiện bởi người dùng trên ứng dụng thứ nhất, thiết bị thứ nhất có thể thu tài khoản thứ nhất và mã xác thực thứ nhất mà được nhập bởi người dùng trên giao diện đăng nhập tài khoản của ứng dụng thứ nhất; và thiết bị thứ nhất có thể đăng nhập, đáp lại thao tác đăng nhập được thực hiện bởi người dùng trên giao diện đăng nhập tài khoản, vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mã xác thực thứ nhất.

Dựa vào khía cạnh thứ nhất, theo cách thiết kế khả thi khác, dựa vào kịch bản ứng dụng thứ hai nêu trên, sau khi thiết bị thứ nhất chia sẻ tài khoản thứ nhất với thiết bị

thứ hai, thiết bị thứ hai vẫn không thể trực tiếp đăng nhập vào tài khoản thứ nhất. Trong trường hợp này, thiết bị thứ hai có thể yêu cầu máy chủ của ứng dụng thứ nhất gửi mã xác thực (ví dụ, mã xác thực thứ hai) tới tài khoản thứ nhất. Theo cách này, thiết bị thứ nhất có thể thu mã xác thực thứ hai từ máy chủ. Mã xác thực thứ hai có thể là khác với mã xác thực thứ nhất. Sau đó, thiết bị thứ nhất có thể gửi mã xác thực thứ hai tới thiết bị thứ hai. Sau khi thu mã xác thực thứ hai, thiết bị thứ hai có thể đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mã xác thực thứ hai.

Dựa vào khía cạnh thứ nhất, theo cách thiết kế khả thi khác, sau khi thiết bị thứ nhất đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất, người dùng có thể xác định xem có lưu thông tin đăng nhập của tài khoản thứ nhất hay không. Nói cách khác, người dùng có thể xác định xem có lưu thông tin đăng nhập của tài khoản thứ nhất hay không, sao cho thiết bị thứ nhất chia sẻ thông tin đăng nhập với thiết bị khác đáp lại thao tác thứ nhất.

Cụ thể là, Sau khi đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất, thiết bị thứ nhất có thể còn hiển thị giao diện thứ hai. Giao diện thứ hai được tạo cấu hình để yêu cầu người dùng xác nhận xem có lưu thông tin đăng nhập của tài khoản thứ nhất hay không. Thiết bị thứ nhất có thể lưu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất đáp lại thao tác thứ hai được thực hiện bởi người dùng trên giao diện thứ hai. Theo cách thiết kế này, thiết bị thứ nhất có thể lưu thông tin đăng nhập của tài khoản thứ nhất dựa vào sự lựa chọn của người dùng và thiện chí của người dùng. Điều này có thể nâng cao hiệu suất của sự tương tác giữa thiết bị thứ nhất và người dùng, và nâng cao trải nghiệm người dùng.

Dựa vào khía cạnh thứ nhất, theo cách thiết kế khả thi khác, thiết bị thứ nhất có thể không lưu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất đáp lại thao tác thứ sáu được thực hiện bởi người dùng trên giao diện thứ hai, và thiết bị thứ nhất có thể hiển thị giao diện thứ nhất, màn hình chính, hoặc trang được thiết đặt trước của ứng dụng thứ nhất.

Theo cách thiết kế này, thiết bị thứ nhất có thể lưu thông tin đăng nhập của tài khoản thứ nhất dựa vào sự lựa chọn của người dùng và thiện chí của người dùng. Điều này có thể nâng cao hiệu suất của sự tương tác giữa thiết bị thứ nhất và người dùng, và nâng

cao trải nghiệm người dùng.

Dựa vào khía cạnh thứ nhất, theo cách thiết kế khả thi khác, trước khi gửi thông tin đăng nhập của tài khoản thứ nhất tới thiết bị thứ hai, thiết bị thứ nhất có thể yêu cầu người dùng xác nhận xem có chia sẻ thông tin đăng nhập của tài khoản thứ nhất với thiết bị thứ hai hay không. Điều này có thể ngăn ngừa thông tin đăng nhập của tài khoản thứ nhất không bị chia sẻ với thiết bị khác do thao tác lỗi của người dùng, và do đó có thể ngăn ngừa thiết bị khác thu nhận thông tin đăng nhập của tài khoản thứ nhất do thao tác lỗi của người dùng. Theo cách này, bảo mật thông tin người dùng có thể được bảo vệ.

Cụ thể là, thiết bị thứ nhất gửi, đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất trên giao diện thứ nhất, thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới thiết bị thứ hai tương ứng với tùy chọn thiết bị thứ nhất có thể bao gồm: thiết bị thứ nhất hiển thị thông tin gợi ý thứ nhất đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất. Thông tin gợi ý thứ nhất được sử dụng để yêu cầu người dùng xác nhận xem có chia sẻ thông tin đăng nhập của tài khoản thứ nhất với thiết bị thứ hai hay không. Thiết bị thứ nhất gửi thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới thiết bị thứ hai đáp lại thao tác thứ ba được thực hiện bởi người dùng trên thông tin gợi ý thứ nhất.

Dựa vào khía cạnh thứ nhất, theo cách thiết kế khả thi khác, để nâng cao bảo mật của thông tin đăng nhập của tài khoản thứ nhất và ngăn ngừa thông tin đăng nhập của tài khoản thứ nhất khỏi bị đánh cắp trong suốt thời gian chia sẻ, thiết bị thứ nhất có thể thương lượng khóa phiên với thiết bị thứ hai. Thiết bị thứ nhất có thể mã hóa, nhờ sử dụng khóa phiên, dữ liệu được chia sẻ với thiết bị thứ hai.

Cụ thể là, thiết bị thứ nhất gửi, đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất trên giao diện thứ nhất, thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới thiết bị thứ hai tương ứng với tùy chọn thiết bị thứ nhất có thể bao gồm: thiết bị thứ nhất thương lượng khóa phiên với thiết bị thứ hai đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất. Thiết bị thứ nhất mã hóa thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất nhờ sử dụng khóa phiên, để thu nhận dữ liệu

được mã hóa, và gửi dữ liệu được mã hóa tới thiết bị thứ hai.

Dựa vào khía cạnh thứ nhất, theo cách thiết kế khả thi khác, thông tin nhận dạng của ứng dụng thứ nhất có thể còn bao gồm khóa công khai chữ ký của ứng dụng thứ nhất, tên gói của ứng dụng thứ nhất được sử dụng để biểu diễn ứng dụng thứ nhất, và khóa công khai chữ ký của ứng dụng thứ nhất được sử dụng để xác thực xem tên gói của ứng dụng thứ nhất bị giả mạo hay không. Có thể hiểu rằng, nếu tên gói của ứng dụng thứ nhất bị giả mạo, thiết bị thứ hai không đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng thông tin đăng nhập của tài khoản thứ nhất.

Dựa vào khía cạnh thứ nhất, theo cách thiết kế khả thi khác, trước khi thiết bị thứ nhất gửi thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới thiết bị thứ hai, thiết bị thứ nhất có thể đã thiết lập sự kết nối không dây tới thiết bị thứ hai, hoặc có thể không thiết lập sự kết nối không dây tới thiết bị thứ hai.

Đối với hai trường hợp, thiết bị thứ nhất gửi, đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất trên giao diện thứ nhất, thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới thiết bị thứ hai có thể bao gồm: Nếu thiết bị thứ nhất đã thiết lập sự kết nối không dây tới thiết bị thứ hai, thiết bị thứ nhất gửi thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới thiết bị thứ hai qua sự kết nối không dây đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất. Nếu thiết bị thứ nhất không thiết lập sự kết nối không dây tới thiết bị thứ hai, thiết bị thứ nhất có thể yêu cầu thiết lập sự kết nối không dây tới thiết bị thứ hai đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất, và gửi thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới thiết bị thứ hai qua sự kết nối không dây sau khi thiết lập sự kết nối không dây.

Dựa vào khía cạnh thứ nhất, theo thiết kế khả thi khác, để bảo vệ bảo mật thông tin người dùng, thiết bị thứ nhất có thể thực hiện việc xác thực danh tính người dùng đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất. Nếu việc xác thực danh tính người dùng thành công, thiết bị thứ nhất có thể gửi thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới thiết bị thứ hai.

Theo khía cạnh thứ hai, sáng chế đề xuất phương pháp chia sẻ dữ liệu tài khoản. Phương pháp được áp dụng cho thiết bị thứ hai. Thiết bị thứ hai có thể thu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất của ứng dụng thứ nhất từ thiết bị thứ nhất. Thiết bị thứ hai hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất, và điền thông tin đăng nhập của tài khoản thứ nhất trên giao diện đăng nhập tài khoản. Thiết bị thứ hai có thể đăng nhập, đáp lại thao tác thứ tư được thực hiện bởi người dùng trên giao diện đăng nhập tài khoản, vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng thông tin đăng nhập của tài khoản thứ nhất.

Theo kịch bản ứng dụng thứ nhất của sáng chế, thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất. Theo kịch bản ứng dụng thứ hai của sáng chế, thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất, nhưng thông tin đăng nhập của tài khoản thứ nhất không bao gồm mật khẩu đăng nhập của tài khoản thứ nhất. Thông tin nhận dạng của ứng dụng thứ nhất có thể bao gồm tên gói của ứng dụng thứ nhất, và tên gói của ứng dụng thứ nhất được sử dụng để nhận dạng ứng dụng thứ nhất.

Theo phương pháp được đề xuất trong sáng chế, máy khách và máy chủ của ứng dụng (ví dụ, ứng dụng thứ nhất) không cần được phát triển thêm, và thiết bị thứ hai có thể thu thông tin đăng nhập của tài khoản thứ nhất mà được chia sẻ bởi thiết bị thứ nhất, và đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng thông tin đăng nhập của tài khoản thứ nhất. Theo phương pháp, thiết bị điện tử có thể chia sẻ một cách thích hợp thông tin đăng nhập của ứng dụng được lựa chọn bởi người dùng với thiết bị khác. Điều này có thể nâng cao độ bảo mật thông tin trong thiết bị điện tử.

Ngoài ra, thiết bị thứ hai có thể thu thông tin đăng nhập của tài khoản thứ nhất từ thiết bị thứ nhất, và thông tin đăng nhập của tài khoản thứ nhất không cần được truyền nhờ sử dụng máy chủ. Điều này có thể ngăn ngừa thông tin đăng nhập của tài khoản thứ nhất khỏi bị đánh cắp ở phía máy chủ, và có thể bảo vệ bảo mật thông tin người dùng.

Tóm lại, theo phương pháp trong sáng chế, thiết bị điện tử có thể chia sẻ tài khoản và mật khẩu đăng nhập của ứng dụng bất kỳ trong thiết bị điện tử với thiết bị khác mà không phải triển thêm máy khách và máy chủ của ứng dụng, và bảo mật thông tin người dùng có thể được bảo vệ. Nói cách khác, phương pháp trong sáng chế có thể bảo vệ bảo

mật thông tin người dùng và thực hiện một cách thông minh việc chia sẻ tự động của dữ liệu tài khoản.

Dựa vào khía cạnh thứ hai, theo cách thiết kế khả thi, sau khi thiết bị thứ hai thu thông tin đăng nhập của tài khoản thứ nhất, người dùng có thể xác định xem có đăng nhập vào tài khoản thứ nhất nhờ sử dụng thông tin đăng nhập hay không. Cụ thể là, sau khi thiết bị thứ hai thu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất từ thiết bị thứ nhất, và trước khi thiết bị thứ hai hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất, thiết bị thứ hai có thể hiển thị giao diện thứ ba. Giao diện thứ ba được tạo cấu hình để yêu cầu người dùng xác nhận xem có đăng nhập vào tài khoản thứ nhất hay không nhờ sử dụng thông tin đăng nhập. Thiết bị thứ hai có thể hiển thị giao diện đăng nhập tài khoản đáp lại thao tác thứ năm được thực hiện bởi người dùng trên giao diện thứ ba.

Theo cách thiết kế này, thiết bị thứ hai có thể đăng nhập vào tài khoản thứ nhất dựa vào sự lựa chọn của người dùng và thiện chí của người dùng nhờ sử dụng thông tin đăng nhập. Điều này có thể nâng cao hiệu suất của sự tương tác giữa thiết bị thứ hai và người dùng, và nâng cao trải nghiệm người dùng.

Dựa vào khía cạnh thứ hai, theo cách thiết kế khả thi khác, dựa vào kịch bản ứng dụng thứ hai nêu trên, thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất nhưng không bao gồm mật khẩu đăng nhập của tài khoản thứ nhất. Trong trường hợp này, thiết bị thứ hai có thể yêu cầu máy chủ của ứng dụng thứ nhất gửi mã xác thực (ví dụ, mã xác thực thứ hai) tới tài khoản thứ nhất. Thiết bị thứ hai có thể đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mã xác thực thứ hai.

Cụ thể là, thiết bị thứ hai đăng nhập, đáp lại thao tác thứ tư được thực hiện bởi người dùng trên giao diện đăng nhập tài khoản, vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng thông tin đăng nhập của tài khoản thứ nhất có thể bao gồm: thiết bị thứ hai có thể gửi yêu cầu thu nhận mã xác thực tới máy chủ của ứng dụng thứ nhất đáp lại thao tác thu nhận mã xác thực được nhập bởi người dùng trên giao diện đăng nhập tài khoản. Yêu cầu thu nhận mã xác thực bao gồm tài khoản thứ nhất và được sử dụng để yêu cầu máy chủ gửi mã xác thực tới tài khoản thứ nhất. Sau đó, thiết bị thứ hai có thể thu mã xác thực thứ hai từ thiết bị thứ nhất. Mã xác thực thứ hai là mã mà thiết bị thứ hai yêu cầu

máy chủ gửi tới tài khoản thứ nhất. Cuối cùng, thiết bị thứ hai có thể điền mã xác thực thứ hai trên giao diện đăng nhập tài khoản, và đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mã xác thực thứ hai. Thao tác thứ tư bao gồm thao tác thu nhận mã xác thực.

Dựa vào khía cạnh thứ hai, theo cách thiết kế khả thi khác, trước khi thiết bị thứ hai hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất, thiết bị thứ hai có thể xác định, dựa vào thông tin nhận dạng của ứng dụng thứ nhất, xem thiết bị thứ hai đang chạy ứng dụng thứ nhất hay không. Nếu thiết bị thứ hai đang chạy ứng dụng thứ nhất, thiết bị thứ hai có thể hiển thị giao diện đăng nhập tài khoản. Nếu thiết bị thứ hai không chạy ứng dụng thứ nhất, thiết bị thứ hai có thể loại bỏ thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất.

Ví dụ, thiết bị thứ hai đang chạy ứng dụng thứ nhất bao gồm bất kỳ một trong số các trường hợp sau: thiết bị thứ hai đang chạy ứng dụng thứ nhất trong nền trước; thiết bị thứ hai đang chạy ứng dụng thứ nhất trong nền sau; thiết bị thứ hai đang chạy trình duyệt trong nền trước, và trình duyệt hiển thị trang web của ứng dụng thứ nhất; hoặc thiết bị thứ hai đang chạy trình duyệt trong nền sau, và trình duyệt hiển thị trang web của ứng dụng thứ nhất.

Dựa vào khía cạnh thứ hai, theo cách thiết kế khả thi khác, miễn là ứng dụng thứ nhất được cài đặt trong thiết bị thứ hai, ngay cả khi thiết bị thứ hai không chạy ứng dụng thứ nhất, sau khi thiết bị thứ hai thu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất từ thiết bị thứ nhất, thiết bị thứ hai có thể tự động bắt đầu ứng dụng thứ nhất, và hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất.

Dựa vào khía cạnh thứ hai, theo cách thiết kế khả thi khác, để bảo vệ bảo mật thông tin người dùng, thiết bị thứ hai có thể thương lượng khóa phiên với thiết bị thứ nhất; thiết bị thứ hai có thể thu dữ liệu được mã hóa từ thiết bị thứ nhất, trong đó dữ liệu được mã hóa được thu nhận bằng cách mã hóa thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất nhờ sử dụng khóa phiên; và thiết bị thứ hai có thể giải mã dữ liệu được mã hóa nhờ sử dụng khóa phiên, để thu nhận thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất.

Dựa vào khía cạnh thứ hai, theo cách thiết kế khả thi khác, thông tin nhận dạng

của ứng dụng thứ nhất còn bao gồm khóa công khai chữ ký của ứng dụng thứ nhất. Khóa công khai chữ ký của ứng dụng thứ nhất được sử dụng để xác định xem tên gói của ứng dụng thứ nhất bị giả mạo hay không. Thiết bị thứ hai hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất bao gồm: thiết bị thứ hai xác định, dựa vào khóa công khai chữ ký của ứng dụng thứ nhất, rằng tên gói của ứng dụng thứ nhất trong thông tin nhận dạng của ứng dụng thứ nhất không bị giả mạo, và thiết bị thứ hai hiển thị giao diện đăng nhập tài khoản.

Có thể hiểu rằng, nếu tên gói của ứng dụng thứ nhất bị giả mạo, ngay cả khi thiết bị thứ hai điền thông tin đăng nhập của tài khoản thứ nhất trên giao diện đăng nhập tài khoản của ứng dụng tương ứng với tên gói bị giả mạo, thiết bị thứ hai vẫn không thể đăng nhập vào ứng dụng thứ nhất hoặc ứng dụng tương ứng với tên gói bị giả mạo. Nói cách khác, sau khi thiết bị thứ hai thu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất, các thao tác gồm "hiển thị giao diện đăng nhập tài khoản", "điền thông tin đăng nhập trên giao diện đăng nhập tài khoản", và "đăng nhập vào tài khoản thứ nhất nhờ sử dụng thông tin đăng nhập" mà được thực hiện bởi thiết bị thứ hai đều là không hợp lệ. Do đó, trước khi hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất, thiết bị thứ hai xác định xem tên gói của ứng dụng thứ nhất bị giả mạo hay không. Điều này có thể ngăn ngừa thiết bị thứ hai thực hiện các thao tác không hợp lệ nêu trên.

Theo khía cạnh thứ ba, sáng chế đề xuất phương pháp chia sẻ dữ liệu tài khoản. Theo phương pháp, thiết bị thứ nhất đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng mã xác thực thứ nhất, và thiết bị thứ nhất có thể thu thao tác thứ nhất được thực hiện bởi người dùng thứ nhất trên ứng dụng thứ nhất. Thao tác thứ nhất được sử dụng để kích hoạt thiết bị thứ nhất chia sẻ tài khoản thứ nhất với thiết bị khác. Thiết bị thứ nhất có thể hiển thị giao diện thứ nhất đáp lại thao tác thứ nhất. Giao diện thứ nhất bao gồm một hoặc nhiều tùy chọn thiết bị, và mỗi tùy chọn thiết bị tương ứng với một thiết bị không dây được tìm thấy bởi thiết bị thứ nhất. Thiết bị thứ nhất có thể gửi, đáp lại thao tác lựa chọn được thực hiện bởi người dùng thứ nhất trên tùy chọn thiết bị thứ nhất trên giao diện thứ nhất, thông tin nhận dạng của ứng dụng thứ nhất và tài khoản thứ nhất tới thiết bị thứ hai tương ứng với tùy chọn thiết bị thứ nhất. Thông tin nhận dạng của ứng dụng thứ nhất được sử dụng để nhận dạng ứng dụng thứ nhất. Thiết bị thứ hai có thể thu thông tin

nhận dạng của ứng dụng thứ nhất và tài khoản thứ nhất từ thiết bị thứ nhất. Sau đó, thiết bị thứ hai hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất, và điền tài khoản thứ nhất trên giao diện đăng nhập tài khoản. Thiết bị thứ hai có thể gửi yêu cầu thu nhận mã xác thực tới máy chủ của ứng dụng thứ nhất đáp lại thao tác thu nhận mã xác thực được nhập bởi người dùng thứ hai trên giao diện đăng nhập tài khoản. Yêu cầu thu nhận mã xác thực bao gồm tài khoản thứ nhất và được sử dụng để yêu cầu máy chủ gửi mã xác thực tới tài khoản thứ nhất. Máy chủ có thể thu yêu cầu thu nhận mã xác thực từ thiết bị thứ hai, và gửi mã xác thực thứ hai của tài khoản thứ nhất tới thiết bị thứ nhất. Thiết bị thứ nhất có thể thu mã xác thực thứ hai từ máy chủ, và gửi mã xác thực thứ hai tới thiết bị thứ hai. Thiết bị thứ hai có thể thu mã xác thực thứ hai từ thiết bị thứ nhất, điền mã xác thực thứ hai trên giao diện đăng nhập tài khoản, và đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mã xác thực thứ hai.

Người dùng thứ nhất và người dùng thứ hai có thể giống nhau hoặc có thể khác nhau. Sau khi đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mã xác thực, thiết bị thứ nhất có thể chia sẻ thông tin nhận dạng của ứng dụng thứ nhất và tài khoản thứ nhất với thiết bị thứ hai đáp lại thao tác thứ nhất được thực hiện bởi người dùng trên ứng dụng thứ nhất. Thiết bị thứ hai có thể tự động yêu cầu máy chủ dựa vào tài khoản thứ nhất để cấp phát mã xác thực. Máy chủ có thể gửi mã xác thực thứ hai tới thiết bị thứ nhất, và thiết bị thứ nhất có thể chuyển tiếp mã xác thực thứ hai tới thiết bị thứ hai, sao cho thiết bị thứ nhất đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất dựa vào tài khoản thứ nhất và mã xác thực thứ hai.

Theo phương pháp được đề xuất trong sáng chế, máy khách và máy chủ của ứng dụng bất kỳ (ví dụ, ứng dụng thứ nhất) không cần được phát triển thêm, và thiết bị thứ nhất có thể chia sẻ thông tin đăng nhập của ứng dụng thứ nhất với thiết bị khác (ví dụ, thiết bị thứ hai) đáp lại thao tác thứ nhất được thực hiện bởi người dùng trên ứng dụng (ví dụ, ứng dụng thứ nhất). Nói cách khác, theo phương pháp, thiết bị điện tử có thể chia sẻ một cách thích hợp thông tin đăng nhập của ứng dụng được lựa chọn bởi người dùng với thiết bị khác. Điều này có thể nâng cao độ bảo mật thông tin trong thiết bị điện tử.

Ngoài ra, thiết bị thứ nhất có thể chia sẻ trực tiếp tài khoản thứ nhất và mã xác thực thứ hai với thiết bị thứ hai, và tài khoản thứ nhất và mã xác thực thứ hai không cần

được truyền nhờ sử dụng máy chủ. Điều này có thể ngăn ngừa tài khoản thứ nhất và mã xác thực thứ hai khỏi bị đánh cắp ở phía máy chủ, và có thể bảo vệ bảo mật thông tin người dùng.

Tóm lại, theo phương pháp trong sáng chế, thiết bị điện tử có thể chia sẻ tài khoản và mật khẩu đăng nhập của ứng dụng bất kỳ trong thiết bị điện tử với thiết bị khác mà không phải triển thêm máy khách và máy chủ của ứng dụng, và bảo mật thông tin người dùng có thể được bảo vệ.

Dựa vào khía cạnh thứ ba, theo cách thiết kế khả thi, thông tin nhận dạng của ứng dụng thứ nhất bao gồm tên gói của ứng dụng thứ nhất. Theo cách khác, thông tin nhận dạng của ứng dụng thứ nhất bao gồm tên gói của ứng dụng thứ nhất và khóa công khai chữ ký của ứng dụng thứ nhất. Khóa công khai chữ ký được sử dụng để xác thực xem tên gói của ứng dụng thứ nhất bị giả mạo hay không. Tên gói của ứng dụng thứ nhất được sử dụng để nhận dạng ứng dụng thứ nhất.

Do đó, trước khi thiết bị thứ hai hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất, phương pháp còn bao gồm: thiết bị thứ hai xác định, dựa vào khóa công khai chữ ký, rằng tên gói của ứng dụng thứ nhất không bị giả mạo. Nói cách khác, thiết bị thứ hai hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất chỉ khi tên gói của ứng dụng thứ nhất không bị giả mạo.

Theo khía cạnh thứ tư, sáng chế đề xuất thiết bị điện tử. Thiết bị điện tử là thiết bị thứ nhất, và thiết bị thứ nhất bao gồm môđun truyền thông không dây, bộ nhớ, màn hình, và một hoặc nhiều bộ xử lý. Môđun truyền thông không dây, bộ nhớ, và màn hình được ghép nối với bộ xử lý.

Bộ nhớ được tạo cấu hình để lưu trữ mã chương trình máy tính, mã chương trình máy tính bao gồm các lệnh máy tính, và khi các lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị thứ nhất được phép thực hiện các thao tác sau: thu thao tác thứ nhất được thực hiện bởi người dùng trên ứng dụng thứ nhất, trong đó thiết bị thứ nhất đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất, và thao tác thứ nhất được sử dụng để kích hoạt thiết bị thứ nhất chia sẻ thông tin đăng nhập của tài khoản thứ nhất với thiết bị khác; hiển thị, đáp lại thao tác thứ nhất, giao diện thứ nhất bao gồm một hoặc nhiều tùy chọn thiết bị, trong đó mỗi tùy chọn thiết bị tương ứng với một thiết bị không dây được tìm thấy bởi thiết

bị thứ nhất; và gửi, đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất trên giao diện thứ nhất, thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới thiết bị thứ hai tương ứng với tùy chọn thiết bị thứ nhất. Thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất, hoặc thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất. Thông tin nhận dạng của ứng dụng thứ nhất bao gồm tên gói của ứng dụng thứ nhất, và tên gói của ứng dụng thứ nhất được sử dụng để nhận dạng ứng dụng thứ nhất.

Dựa vào khía cạnh thứ tư, theo cách thiết kế khả thi, khi các lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị thứ nhất còn được phép thực hiện bước sau: trước khi thu thao tác thứ nhất được thực hiện bởi người dùng trên ứng dụng thứ nhất, hiển thị màn hình chính của thiết bị thứ nhất. Màn hình chính bao gồm biểu tượng của ứng dụng thứ nhất, và thao tác thứ nhất là thao tác được thiết đặt trước được thực hiện bởi người dùng trên biểu tượng của ứng dụng thứ nhất được hiển thị trên màn hình chính.

Theo cách khác, khi các lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị thứ nhất còn được phép thực hiện bước sau: trước khi thu thao tác thứ nhất được thực hiện bởi người dùng trên ứng dụng thứ nhất, hiển thị trang được thiết đặt trước của ứng dụng thứ nhất. Trang được thiết đặt trước bao gồm sự điều khiển được thiết đặt trước, và sự điều khiển được thiết đặt trước được sử dụng để kích hoạt thiết bị thứ nhất chia sẻ thông tin đăng nhập với thiết bị khác.

Dựa vào khía cạnh thứ tư, theo cách thiết kế khả thi khác, thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất. Khi các lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị thứ nhất còn được phép thực hiện các bước sau: trước khi thu thao tác thứ nhất được thực hiện bởi người dùng trên ứng dụng thứ nhất, thu tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất mà được nhập bởi người dùng trên giao diện đăng nhập tài khoản của ứng dụng thứ nhất; và đăng nhập, đáp lại thao tác đăng nhập được thực hiện bởi người dùng trên giao diện đăng nhập tài khoản, vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất.

Dựa vào khía cạnh thứ tư, theo cách thiết kế khả thi khác, thông tin đăng nhập

của tài khoản thứ nhất bao gồm tài khoản thứ nhất nhưng không bao gồm mật khẩu đăng nhập của tài khoản thứ nhất, và tài khoản thứ nhất bao gồm ít nhất số điện thoại hoặc địa chỉ thư điện tử của thiết bị thứ nhất.

Khi các lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị thứ nhất còn được phép thực hiện các bước sau: trước khi thu thao tác thứ nhất được thực hiện bởi người dùng trên ứng dụng thứ nhất, thu tài khoản thứ nhất và mã xác thực thứ nhất mà được nhập bởi người dùng trên giao diện đăng nhập tài khoản của ứng dụng thứ nhất; và đăng nhập, đáp lại thao tác đăng nhập được thực hiện bởi người dùng trên giao diện đăng nhập tài khoản, vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mã xác thực thứ nhất.

Dựa vào khía cạnh thứ tư, theo cách thiết kế khả thi khác, khi các lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị thứ nhất còn được phép thực hiện các bước sau: sau khi gửi thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới thiết bị thứ hai, thu mã xác thực thứ hai từ máy chủ của ứng dụng thứ nhất, trong đó mã xác thực thứ hai là mã mà thiết bị thứ hai yêu cầu máy chủ gửi tới tài khoản thứ nhất; và gửi mã xác thực thứ hai tới thiết bị thứ hai, trong đó mã xác thực thứ hai được sử dụng bởi thiết bị thứ hai để đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất.

Dựa vào khía cạnh thứ tư, theo cách thiết kế khả thi khác, khi các lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị thứ nhất còn được phép thực hiện các bước sau: sau khi đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất, hiển thị giao diện thứ hai, trong đó giao diện thứ hai được tạo cấu hình để yêu cầu người dùng xác nhận xem có lưu thông tin đăng nhập của tài khoản thứ nhất hay không; và lưu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất đáp lại thao tác thứ hai được thực hiện bởi người dùng trên giao diện thứ hai.

Dựa vào khía cạnh thứ tư, theo cách thiết kế khả thi khác, khi các lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị thứ nhất còn được phép thực hiện các bước sau: bỏ qua lưu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất đáp lại thao tác thứ sáu được thực hiện bởi người dùng trên giao diện thứ hai, và hiển thị giao diện thứ nhất.

Dựa vào khía cạnh thứ tư, theo cách thiết kế khả thi khác, khi các lệnh máy tính

được thực hiện bởi bộ xử lý, thiết bị thứ nhất còn được phép thực hiện các bước sau: hiển thị thông tin gợi ý thứ nhất đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất, trong đó thông tin gợi ý thứ nhất được sử dụng để yêu cầu người dùng xác nhận xem có chia sẻ thông tin đăng nhập của tài khoản thứ nhất với thiết bị thứ hai hay không; và gửi thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới thiết bị thứ hai đáp lại thao tác thứ ba được thực hiện bởi người dùng trên thông tin gợi ý thứ nhất.

Dựa vào khía cạnh thứ tư, theo cách thiết kế khả thi khác, khi các lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị thứ nhất còn được phép thực hiện các bước sau: thương lượng khóa phiên với thiết bị thứ hai đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất; và mã hóa thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất nhờ sử dụng khóa phiên, để thu nhận dữ liệu được mã hóa, và gửi dữ liệu được mã hóa tới thiết bị thứ hai.

Dựa vào khía cạnh thứ tư, theo cách thiết kế khả thi khác, thông tin nhận dạng của ứng dụng thứ nhất còn bao gồm khóa công khai chữ ký của ứng dụng thứ nhất, và khóa công khai chữ ký của ứng dụng thứ nhất được sử dụng để xác thực xem tên gói của ứng dụng thứ nhất bị giả mạo hay không.

Dựa vào khía cạnh thứ tư, theo cách thiết kế khả thi khác, khi các lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị thứ nhất còn được phép thực hiện các bước sau: thương lượng khóa phiên với thiết bị thứ hai đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất; và mã hóa thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất nhờ sử dụng khóa phiên, để thu nhận dữ liệu được mã hóa, và gửi dữ liệu được mã hóa tới thiết bị thứ hai.

Theo khía cạnh thứ năm, sáng chế đề xuất thiết bị điện tử. Thiết bị điện tử là thiết bị thứ hai, và thiết bị thứ hai bao gồm môđun truyền thông không dây, bộ nhớ, màn hình, và một hoặc nhiều bộ xử lý. Môđun truyền thông không dây, bộ nhớ, và màn hình được ghép nối với bộ xử lý.

Bộ nhớ được tạo cấu hình để lưu trữ mã chương trình máy tính, mã chương trình máy tính bao gồm các lệnh máy tính, và khi các lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị thứ hai được phép thực hiện các thao tác sau: thu thông tin nhận dạng của ứng

dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất của ứng dụng thứ nhất từ thiết bị thứ nhất; hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất, và điền thông tin đăng nhập của tài khoản thứ nhất trên giao diện đăng nhập tài khoản; và đăng nhập, đáp lại thao tác thứ tư được thực hiện bởi người dùng trên giao diện đăng nhập tài khoản, vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng thông tin đăng nhập của tài khoản thứ nhất. Thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất, hoặc thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất. Thông tin nhận dạng của ứng dụng thứ nhất bao gồm tên gói của ứng dụng thứ nhất, và tên gói của ứng dụng thứ nhất được sử dụng để nhận dạng ứng dụng thứ nhất.

Dựa vào khía cạnh thứ năm, theo cách thiết kế khả thi, khi các lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị thứ hai còn được phép thực hiện các bước sau: sau khi thu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất, và trước khi hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất, hiển thị giao diện thứ ba, trong đó giao diện thứ ba được tạo cấu hình để yêu cầu người dùng xác nhận xem có đăng nhập vào tài khoản thứ nhất hay không nhờ sử dụng thông tin đăng nhập; và hiển thị giao diện đăng nhập tài khoản đáp lại thao tác thứ năm được thực hiện bởi người dùng trên giao diện thứ ba.

Dựa vào khía cạnh thứ năm, theo cách thiết kế khả thi khác, thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất nhưng không bao gồm mật khẩu đăng nhập của tài khoản thứ nhất.

Khi các lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị thứ hai còn được phép thực hiện các bước sau: gửi yêu cầu thu nhận mã xác thực tới máy chủ của ứng dụng thứ nhất đáp lại thao tác thu nhận mã xác thực được nhập bởi người dùng trên giao diện đăng nhập tài khoản, trong đó yêu cầu thu nhận mã xác thực bao gồm tài khoản thứ nhất và được sử dụng để yêu cầu máy chủ gửi mã xác thực tới tài khoản thứ nhất; thu mã xác thực thứ hai từ thiết bị thứ nhất, trong đó mã xác thực thứ hai là mã mà thiết bị thứ hai yêu cầu máy chủ gửi tới tài khoản thứ nhất; và điền mã xác thực thứ hai trên giao diện đăng nhập tài khoản, và đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mã xác thực thứ hai. Thao tác thứ tư bao gồm thao tác thu nhận mã

xác thực.

Dựa vào khía cạnh thứ năm, theo cách thiết kế khả thi khác, khi các lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị thứ hai còn được phép thực hiện bước sau: nếu thiết bị thứ hai xác định, dựa vào thông tin nhận dạng của ứng dụng thứ nhất, rằng thiết bị thứ hai đang chạy ứng dụng thứ nhất, hiển thị giao diện đăng nhập tài khoản.

Thiết bị thứ hai đang chạy ứng dụng thứ nhất bao gồm bất kỳ một trong số các trường hợp sau: thiết bị thứ hai đang chạy ứng dụng thứ nhất trong nền trước; thiết bị thứ hai đang chạy ứng dụng thứ nhất trong nền sau; thiết bị thứ hai đang chạy trình duyệt trong nền trước, và trình duyệt hiển thị trang web của ứng dụng thứ nhất; hoặc thiết bị thứ hai đang chạy trình duyệt trong nền sau, và trình duyệt hiển thị trang web của ứng dụng thứ nhất.

Dựa vào khía cạnh thứ năm, theo cách thiết kế khả thi khác, khi các lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị thứ hai còn được phép thực hiện các bước sau: thương lượng khóa phiên với thiết bị thứ nhất; thu dữ liệu được mã hóa từ thiết bị thứ nhất, trong đó dữ liệu được mã hóa được thu nhận bằng cách mã hóa thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất nhờ sử dụng khóa phiên; và giải mã dữ liệu được mã hóa nhờ sử dụng khóa phiên, để thu nhận thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất.

Dựa vào khía cạnh thứ năm, theo cách thiết kế khả thi khác, thông tin nhận dạng của ứng dụng thứ nhất còn bao gồm khóa công khai chữ ký của ứng dụng thứ nhất, và khóa công khai chữ ký của ứng dụng thứ nhất được sử dụng để xác thực xem tên gói của ứng dụng thứ nhất bị giả mạo hay không. Khi các lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị thứ hai còn được phép thực hiện các bước sau: xác định, dựa vào khóa công khai chữ ký của ứng dụng thứ nhất, xem tên gói của ứng dụng thứ nhất trong thông tin nhận dạng của ứng dụng thứ nhất bị giả mạo hay không; và nếu tên gói của ứng dụng thứ nhất không bị giả mạo, hiển thị giao diện đăng nhập tài khoản.

Dựa vào khía cạnh thứ năm, theo cách thiết kế khả thi khác, khi các lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị thứ hai còn được phép thực hiện các bước sau: thương lượng khóa phiên với thiết bị thứ nhất; thu dữ liệu được mã hóa từ thiết bị thứ nhất, trong đó dữ liệu được mã hóa được thu nhận bằng cách mã hóa thông tin nhận dạng của

ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất nhờ sử dụng khóa phiên; và giải mã dữ liệu được mã hóa nhờ sử dụng khóa phiên, để thu nhận thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất.

Theo khía cạnh thứ sáu, sáng chế đề xuất hệ thống chip. Hệ thống chip có thể được áp dụng cho thiết bị điện tử bao gồm môđun truyền thông không dây, bộ nhớ, và màn hình. Hệ thống chip bao gồm một hoặc nhiều mạch giao diện và một hoặc nhiều bộ xử lý. Mạch giao diện và bộ xử lý được kết nối qua đường dây. Mạch giao diện được tạo cấu hình để: thu tín hiệu từ bộ nhớ, và gửi tín hiệu tới bộ xử lý. Tín hiệu bao gồm các lệnh máy tính được lưu trữ trong bộ nhớ. Khi bộ xử lý thực hiện các lệnh máy tính, thiết bị điện tử thực hiện phương pháp theo bất kỳ một trong số khía cạnh thứ nhất, khía cạnh thứ hai, và khía cạnh thứ ba và các cách thiết kế khả thi của nó.

Theo khía cạnh thứ bảy, sáng chế đề xuất phương tiện lưu trữ đọc được bởi máy tính. Phương tiện lưu trữ đọc được bởi máy tính bao gồm các lệnh máy tính. Khi các lệnh máy tính được chạy trên thiết bị điện tử, thiết bị điện tử được phép thực hiện phương pháp theo bất kỳ một trong số khía cạnh thứ nhất, khía cạnh thứ hai, và khía cạnh thứ ba và các cách thiết kế khả thi của nó.

Theo khía cạnh thứ tám, sáng chế đề xuất sản phẩm chương trình máy tính. Khi sản phẩm chương trình máy tính chạy trên máy tính, máy tính được phép thực hiện phương pháp theo bất kỳ một trong số khía cạnh thứ nhất, khía cạnh thứ hai, và khía cạnh thứ ba và các cách thiết kế khả thi của nó.

Có thể hiểu rằng, đối với các hiệu quả có lợi mà có thể là đạt được bởi thiết bị điện tử theo bất kỳ một trong số khía cạnh thứ tư và khía cạnh thứ năm và các cách thiết kế khả thi của nó, hệ thống chip theo khía cạnh thứ sáu, phương tiện lưu trữ đọc được bởi máy tính theo khía cạnh thứ bảy, và sản phẩm chương trình máy tính theo khía cạnh thứ tám, tham chiếu tới các hiệu quả có lợi trong bất kỳ một trong số khía cạnh thứ nhất, khía cạnh thứ hai, và khía cạnh thứ ba và các cách thiết kế khả thi của nó. Chi tiết không được mô tả lại ở đây.

Mô tả vắn tắt các hình vẽ

Fig.1 là hình vẽ giản lược của kiến trúc hệ thống mà phương pháp chia sẻ dữ

liệu tài khoản được áp dụng cho theo phương án của sáng chế;

Fig.2 là hình vẽ giản lược của cấu trúc phần cứng của thiết bị điện tử theo phương án của sáng chế;

Fig.3A và Fig.3C là lưu đồ của phương pháp chia sẻ dữ liệu tài khoản theo phương án của sáng chế;

Fig.4(a) đến Fig.4(c) là các hình vẽ giản lược của trường hợp về giao diện hiển thị của điện thoại di động theo phương án của sáng chế;

Fig.5 là hình vẽ giản lược của trường hợp về giao diện hiển thị khác của điện thoại di động theo phương án của sáng chế;

Fig.6A là hình vẽ giản lược của trường hợp về trường hợp thứ hai theo phương án của sáng chế;

Fig.6B là lưu đồ của phương pháp chia sẻ dữ liệu tài khoản khác theo phương án của sáng chế;

Fig.7A-1 và Fig.7A-2 là lưu đồ của phương pháp chia sẻ dữ liệu tài khoản khác theo phương án của sáng chế;

Fig.7B là hình vẽ giản lược của trường hợp về giao diện hiển thị khác của điện thoại di động theo phương án của sáng chế;

Fig.7C là hình vẽ giản lược của trường hợp về giao diện hiển thị khác của điện thoại di động theo phương án của sáng chế;

Fig.7D là hình vẽ giản lược của trường hợp về giao diện hiển thị khác của điện thoại di động theo phương án của sáng chế;

Fig.7E là hình vẽ giản lược của trường hợp về giao diện hiển thị khác của điện thoại di động theo phương án của sáng chế;

Fig.8 là hình vẽ giản lược của trường hợp về giao diện hiển thị khác của điện thoại di động theo phương án của sáng chế;

Fig.9 là hình vẽ giản lược của trường hợp về giao diện hiển thị khác của điện thoại di động theo phương án của sáng chế;

Fig.10(a) đến Fig.10(c) là các hình vẽ giản lược của trường hợp về giao diện hiển thị khác của điện thoại di động theo phương án của sáng chế;

Fig.11A và Fig.11B là lưu đồ của phương pháp chia sẻ dữ liệu tài khoản khác theo phương án của sáng chế;

Fig.12A và Fig.12B là lưu đồ của phương pháp chia sẻ dữ liệu tài khoản khác theo phương án của sáng chế;

Fig.13 là hình vẽ giản lược của cấu trúc của thiết bị điện tử theo phương án của sáng chế; và

Fig.14 là hình vẽ giản lược của cấu trúc của hệ thống chip theo phương án của sáng chế.

Mô tả chi tiết sáng chế

Các thuật ngữ "thứ nhất" và "thứ hai" dưới đây chỉ nhằm mục đích mô tả, và sẽ không được hiểu là sự chỉ báo hoặc hàm ý về tầm quan trọng tương đối hoặc sự chỉ báo ngầm về chất lượng của các đặc điểm kỹ thuật được chỉ báo. Do đó, dấu hiệu giới hạn ở "thứ nhất" hoặc "thứ hai" có thể một cách rõ ràng hoặc ẩn ý bao gồm một hoặc nhiều đặc điểm như vậy. Trong các phần mô tả của các phương án, ngoại trừ được định rõ theo cách khác, "nhiều" có nghĩa là hai hoặc lớn hơn hai.

Hiện nay, giải pháp để chia sẻ tự động tài khoản và mật khẩu đăng nhập có thể thực hiện việc chia sẻ tự động của dữ liệu tài khoản của ứng dụng (ví dụ, ứng dụng a) giữa hai thiết bị điện tử (ví dụ, thiết bị điện tử 1 và thiết bị điện tử 2). Theo giải pháp này, môđun lưu trữ mật khẩu đăng nhập của thiết bị điện tử 1 (ví dụ, điện thoại di động) có thể lưu các tài khoản và các mật khẩu đăng nhập của tất cả các ứng dụng (bao gồm ứng dụng a) trong thiết bị điện tử 1, môđun nhân bản dữ liệu có thể nhân bản, tại một thời điểm, các tài khoản và các mật khẩu đăng nhập của tất cả ứng dụng mà được lưu trong môđun lưu trữ mật khẩu đăng nhập, và môđun kết nối thiết bị có thể truyền, tới thiết bị điện tử 2 (ví dụ, máy thu hình), các tài khoản và các mật khẩu đăng nhập của tất cả ứng dụng mà được thu nhận qua việc nhân bản. Theo cách này, thiết bị điện tử 2 có thể tự động đăng nhập vào tài khoản của ứng dụng a nhờ sử dụng tài khoản và mật khẩu đăng nhập của ứng dụng a.

Theo giải pháp nêu trên, thiết bị điện tử 1 không thể chia sẻ một cách có lựa

chọn tài khoản và mật khẩu đăng nhập của ứng dụng a với thiết bị điện tử 2. Ngoài ra, thiết bị điện tử 2 có thể là thiết bị công cộng nằm trong phạm vi cụ thể, và nhân bản các tài khoản và các mật khẩu đăng nhập của tất cả các ứng dụng trong thiết bị điện tử 1 tới thiết bị điện tử 2 có thể gây ra sự rò rỉ của nhiều tài khoản và các mật khẩu đăng nhập của người dùng.

Để giải quyết vấn đề tồn tại trong giải pháp nêu trên, giải pháp khác có thể thực hiện việc chia sẻ của tài khoản và mật khẩu đăng nhập giữa các thiết bị qua việc quét mã trong ứng dụng. Cụ thể là, thiết bị điện tử 2 mà chưa được đăng nhập vào tài khoản có thể hiển thị giao diện quét của ứng dụng a, và giao diện quét bao gồm mã hai chiều của ứng dụng a. Thiết bị điện tử 1 mà đã đăng nhập vào tài khoản quét mã hai chiều, và có thể gửi thông tin đăng nhập tới thiết bị điện tử 2. Thiết bị điện tử 2 có thể đăng nhập vào tài khoản nhờ sử dụng thông tin đăng nhập.

Tuy nhiên, chỉ một số ứng dụng hiện hỗ trợ chức năng chia sẻ tài khoản và mật khẩu đăng nhập qua việc quét mã trong ứng dụng, và một số ứng dụng không hỗ trợ chức năng. Để cho phép mỗi ứng dụng hỗ trợ chức năng, các máy khách và các máy chủ của số lượng lớn các ứng dụng cần được phát triển thêm, mà là khó khăn và tốn kém.

Các phương án của sáng chế đề xuất phương pháp chia sẻ dữ liệu tài khoản. Theo phương pháp, thiết bị điện tử có thể chia sẻ tài khoản và mật khẩu đăng nhập của ứng dụng bất kỳ trong thiết bị điện tử với thiết bị khác mà không phải triển thêm máy khách và máy chủ của ứng dụng, và bảo mật thông tin người dùng có thể được bảo vệ.

Fig.1 là hình vẽ giản lược của kiến trúc hệ thống mà phương pháp chia sẻ dữ liệu tài khoản được áp dụng cho theo phương án của sáng chế. Như được thể hiện trên Fig.1, hệ thống có thể bao gồm thiết bị thứ nhất 110 và thiết bị thứ hai 120. Thiết bị thứ nhất 110 có thể thiết lập sự kết nối không dây tới thiết bị thứ hai 120. Sự kết nối không dây có thể là bất kỳ một trong số kết nối mạng không dây (wireless fidelity, viết tắt là Wi-Fi), kết nối Bluetooth, công nghệ truyền thông trường gần (near field communication, viết tắt là NFC), hoặc tương tự. Kết nối Wi-Fi có thể bao gồm Wi-Fi trực tiếp, nghĩa là, Wi-Fi kết nối ngang hàng (peer-to-peer, viết tắt là P2P).

Ứng dụng thứ nhất được cài đặt trong thiết bị thứ nhất 110. Ngoài ra, thiết bị thứ nhất 110 đã đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất. Có thể hiểu rằng

thiết bị thứ nhất 110 có thể đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mật khẩu đăng nhập. Tất nhiên, ứng dụng thứ nhất có thể cũng được cài đặt trong thiết bị thứ hai 120. Theo cách khác, thiết bị thứ hai 120 có thể mở trang web của ứng dụng thứ nhất trong trình duyệt của thiết bị thứ hai 120.

Theo phương án này của sáng chế, thiết bị thứ nhất 110 có thể chia sẻ tài khoản thứ nhất và mật khẩu đăng nhập của ứng dụng thứ nhất với thiết bị thứ hai 120 qua sự kết nối không dây. Sau khi thu tài khoản thứ nhất và mật khẩu đăng nhập mà được chia sẻ bởi thiết bị thứ nhất 110, thiết bị thứ hai 120 có thể đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất hoặc trang web của ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mật khẩu đăng nhập.

Ví dụ, ứng dụng thứ nhất có thể là ứng dụng bất kỳ mà có chức năng đăng ký và đăng nhập tài khoản, chẳng hạn như ứng dụng mua sắm, ứng dụng nhắn tin nhanh, hoặc ứng dụng viđeo.

Ví dụ, thiết bị điện tử (ví dụ, thiết bị thứ nhất hoặc thiết bị thứ hai) theo phương án này của sáng chế có thể là điện thoại di động, máy tính bảng, máy thu hình thông minh, máy tính cá nhân (personal computer, viết tắt là PC), máy tính để bàn, máy tính xách tay (laptop), máy tính cầm tay (handheld computer), máy tính bảng (notebook), máy tính cá nhân siêu di động (ultra-mobile personal computer, viết tắt là UMPC), máy tính cầm tay thu nhỏ (netbook), hoặc thiết bị chẳng hạn như điện thoại di động (cellular phone), thiết bị hỗ trợ số cá nhân (personal digital assistant, viết tắt là PDA), hoặc thiết bị thực tế tăng cường (augmented reality, viết tắt là AR)/thực tế ảo (virtual reality, viết tắt là VR). Dạng cụ thể của thiết bị điện tử không giới hạn cụ thể ở phương án này của sáng chế.

Cần lưu ý rằng thiết bị thứ nhất 110 và thiết bị thứ hai 120 có thể là các thiết bị thuộc các loại khác nhau. Ví dụ, thiết bị thứ nhất 110 là điện thoại di động, và thiết bị thứ hai 120 là máy tính bảng. Theo cách khác, thiết bị thứ nhất 110 và thiết bị thứ hai 120 có thể là các thiết bị cùng loại. Ví dụ, cả thiết bị thứ nhất 110 và thiết bị thứ hai 120 đều là các điện thoại di động. Điều này không giới hạn ở phương án này của sáng chế.

Theo phương án này của sáng chế, ví dụ trong đó thiết bị thứ nhất 110 và thiết bị thứ hai 120 được thể hiện trên Fig.1 là các điện thoại di động được sử dụng để mô tả cấu trúc của thiết bị điện tử được đề xuất theo phương án này của sáng chế. Như được thể hiện

trên Fig.2, thiết bị điện tử 200 (ví dụ, điện thoại di động) có thể bao gồm bộ xử lý 210, giao diện bộ nhớ ngoài 220, bộ nhớ trong 221, giao diện bus nối tiếp toàn cầu (universal serial bus, viết tắt là USB) 230, môđun quản lý nạp 240, môđun quản lý công suất 241, pin 242, anten 1, anten 2, môđun truyền thông di động 250, môđun truyền thông không dây 260, môđun auđio 270, loa 270A, bộ thu 270B, micrô 270C, giắc cắm tai nghe 270D, môđun bộ cảm biến 280, nút nhấn 290, động cơ 291, bộ chỉ báo 292, camera 293, màn hình 294, môđun nhận dạng thuê bao (subscriber identity module, viết tắt là SIM) giao diện thẻ 295, và tương tự.

Môđun bộ cảm biến 280 có thể bao gồm bộ cảm biến áp suất, bộ cảm biến con quay hồi chuyển, bộ cảm biến áp suất khí quyển, bộ cảm biến từ, bộ cảm biến gia tốc, bộ cảm biến phạm vi, bộ cảm biến tiệm cận quang học, bộ cảm biến dấu vân tay, bộ cảm biến nhiệt độ, bộ cảm biến chạm, bộ cảm biến ánh sáng xung quanh, bộ cảm biến dẫn xương, và tương tự.

Có thể hiểu rằng cấu trúc được thể hiện theo phương án này không cấu thành giới hạn cụ thể về thiết bị điện tử 200. Theo một số phương án khác, thiết bị điện tử 200 có thể bao gồm nhiều hơn hoặc ít hơn các thành phần so với các thành phần được thể hiện trên hình vẽ, hoặc kết hợp một số thành phần, hoặc tách một số thành phần, hoặc có các sự bố trí thành phần khác nhau. Các thành phần được thể hiện trên hình vẽ có thể được thực hiện bởi phần cứng, phần mềm, hoặc sự kết hợp của phần mềm và phần cứng.

Bộ xử lý 210 có thể bao gồm một hoặc nhiều bộ phận xử lý. Ví dụ, bộ xử lý 210 có thể bao gồm bộ xử lý ứng dụng (application processor, viết tắt là AP), bộ xử lý môđem, bộ phận xử lý đồ họa (graphics processing unit, viết tắt là GPU), bộ xử lý tín hiệu hình ảnh (image signal processor, viết tắt là ISP), bộ điều khiển, bộ nhớ, bộ mã hóa-giải mã viđeo, bộ xử lý tín hiệu số (digital signal processor, viết tắt là DSP), bộ xử lý dải gốc, và/hoặc bộ phận xử lý mạng nơron (neural-network processing unit, viết tắt là NPU). Các bộ phận xử lý khác nhau có thể là các thành phần độc lập, hoặc có thể được tích hợp thành một hoặc nhiều bộ xử lý.

Bộ điều khiển có thể là trung tâm thần kinh và trung tâm lệnh của thiết bị điện tử 200. Bộ điều khiển có thể tạo ra tín hiệu điều khiển thao tác dựa vào mã thao tác lệnh và tín hiệu chuỗi thời gian, để hoàn thiện sự điều khiển của việc tìm nạp lệnh và thực hiện

lệnh.

Bộ nhớ có thể còn được bố trí trong bộ xử lý 210, và được tạo cấu hình để lưu trữ các lệnh và dữ liệu. Theo một số phương án, bộ nhớ trong bộ xử lý 210 là bộ nhớ đệm (cache). Bộ nhớ có thể lưu trữ các lệnh hoặc dữ liệu chỉ được sử dụng hoặc được sử dụng theo chu kỳ bởi bộ xử lý 210. Nếu bộ xử lý 210 cần sử dụng lại các lệnh hoặc dữ liệu, bộ xử lý có thể trực tiếp truy xuất các lệnh hoặc dữ liệu từ bộ nhớ. Điều này tránh khỏi việc truy cập lặp lại và làm giảm thời gian chờ của bộ xử lý 210, nhờ đó nâng cao hiệu quả hệ thống.

Theo một số phương án, bộ xử lý 210 có thể bao gồm một hoặc nhiều giao diện. Giao diện có thể bao gồm giao diện mạch tích hợp liên kết (inter-integrated circuit, viết tắt là I2C), giao diện âm thanh mạch tích hợp liên kết (inter-integrated circuit sound, viết tắt là I2S), giao diện điều biến mã xung (pulse code modulation, viết tắt là PCM), giao diện bộ thu/bộ truyền không đồng bộ toàn cầu (universal asynchronous receiver/transmitter, UART), giao diện bộ xử lý công nghiệp di động (mobile industry processor interface, viết tắt là MIPI), giao diện đầu vào/đầu ra đa năng (general-purpose input/output, viết tắt là GPIO), giao diện môđun nhận dạng thuê bao (subscriber identity module, viết tắt là SIM), giao diện bus nối tiếp toàn cầu (universal serial bus, viết tắt là USB), và/hoặc tương tự.

Có thể hiểu rằng mối tương quan kết nối giao diện giữa các môđun được thể hiện theo phương án này chỉ là ví dụ cho việc mô tả, và không cấu thành giới hạn về cấu trúc của thiết bị điện tử 200. Theo một số phương án khác, thiết bị điện tử 200 theo cách khác có thể sử dụng cách thức kết nối giao diện khác với cách thức theo phương án nêu trên hoặc sự kết hợp của nhiều cách thức kết nối giao diện.

Môđun quản lý nạp 240 được tạo cấu hình để thu đầu vào nạp từ bộ nạp. Bộ nạp có thể là bộ nạp không dây hoặc bộ nạp nối dây. Khi nạp pin 242, môđun quản lý nạp 240 có thể còn cấp nguồn tới thiết bị điện tử nhờ sử dụng môđun quản lý công suất 241.

Môđun quản lý công suất 241 được tạo cấu hình để kết nối tới pin 242, môđun quản lý nạp 240, và bộ xử lý 210. Môđun quản lý công suất 241 thu đầu vào của pin 242 và/hoặc đầu vào của môđun quản lý nạp 240, và cấp nguồn tới bộ xử lý 210, bộ nhớ trong 221, bộ nhớ ngoài, màn hình 294, camera 293, môđun truyền thông không dây 260, và tương tự. Theo một số phương án, môđun quản lý công suất 241 và môđun quản lý nạp

240 theo cách khác có thể được bố trí trong cùng thành phần.

Chức năng truyền thông không dây của thiết bị điện tử 200 có thể được thực hiện qua anten 1, anten 2, môđun truyền thông di động 250, môđun truyền thông không dây 260, bộ xử lý môđem, bộ xử lý dải gốc, và tương tự. Theo một số phương án, trong thiết bị điện tử 200, anten 1 và môđun truyền thông di động 250 được ghép nối, và anten 2 và môđun truyền thông không dây 260 được ghép nối, sao cho thiết bị điện tử 200 có thể truyền thông với mạng và thiết bị khác nhờ sử dụng công nghệ truyền thông không dây. Ví dụ, theo phương án này của sáng chế, thiết bị điện tử 200 có thể gửi tài khoản thứ nhất và mật khẩu đăng nhập tới thiết bị khác nhờ sử dụng công nghệ truyền thông không dây.

Anten 1 và anten 2 được tạo cấu hình để truyền và thu các tín hiệu sóng điện từ. Mỗi anten trong thiết bị điện tử 200 có thể được tạo cấu hình để bao phủ một hoặc nhiều dải truyền thông. Các anten khác nhau có thể là còn được đa hợp, để tăng sự sử dụng anten. Ví dụ, anten 1 có thể được đa hợp như anten hỗn hợp trong mạng vùng cục bộ không dây. Theo một số phương án khác, anten có thể được sử dụng theo sự kết hợp với chuyển mạch điều hưởng.

Môđun truyền thông di động 250 có thể cung cấp giải pháp, được áp dụng cho thiết bị điện tử 200, tới truyền thông không dây bao gồm 2G, 3G, 4G, 5G, hoặc tương tự. Môđun truyền thông di động 250 có thể bao gồm ít nhất một bộ lọc, chuyển mạch, bộ khuếch đại công cuất, bộ khuếch đại nhiễu thấp (low noise amplifier, viết tắt là LNA), và tương tự. Môđun truyền thông di động 250 có thể thu sóng điện từ qua anten 1, thực hiện việc xử lý chẳng hạn như lọc hoặc khuếch đại trên sóng điện từ được thu, và truyền sóng điện từ được xử lý tới bộ xử lý môđem cho việc giải điều biến.

Môđun truyền thông di động 250 có thể còn khuếch đại tín hiệu được điều biến bởi bộ xử lý môđem, và chuyển đổi tín hiệu được khuếch đại thành sóng điện từ qua anten 1 cho việc phát xạ. Theo một số phương án, ít nhất một số các môđun chức năng trong môđun truyền thông di động 250 có thể được bố trí trong bộ xử lý 210. Theo một số phương án, ít nhất một số các môđun chức năng trong môđun truyền thông di động 250 có thể được bố trí trong thiết bị giống như ít nhất một số môđun trong bộ xử lý 210.

Môđun truyền thông không dây 260 có thể cung cấp giải pháp, mà được áp dụng cho thiết bị điện tử 200, cho truyền thông không dây bao gồm mạng vùng cục bộ không

dây (wireless local area network, viết tắt là WLAN) (ví dụ, mạng kết nối không dây (wireless fidelity, viết tắt là Wi-Fi)), Bluetooth (Bluetooth, BT), hệ thống vệ tinh định vị toàn cầu (global navigation satellite system, viết tắt là GNSS), điều biến tần số (frequency modulation, viết tắt là FM), công nghệ truyền thông trường gần (near field communication, viết tắt là NFC), công nghệ hồng ngoại (infrared, viết tắt là IR), hoặc tương tự. Ví dụ, theo phương án này của sáng chế, thiết bị điện tử 200 (ví dụ, thiết bị thứ nhất 110) có thể truy cập mạng Wi-Fi nhờ sử dụng môđun truyền thông không dây 260.

Môđun truyền thông không dây 260 có thể là một hoặc nhiều thành phần tích hợp ít nhất một môđun xử lý truyền thông. Môđun truyền thông không dây 260 thu sóng điện từ qua anten 2, thực hiện điều biến tần số và xử lý lọc trên tín hiệu sóng điện từ, và gửi tín hiệu được xử lý tới bộ xử lý 210. Môđun truyền thông không dây 260 có thể còn thu tín hiệu cần được gửi từ bộ xử lý 210, thực hiện điều biến tần số và khuếch đại trên tín hiệu, và chuyển đổi tín hiệu được xử lý thành sóng điện từ qua anten 2 cho việc phát xạ.

Thiết bị điện tử 200 có thể thực hiện chức năng màn hình qua GPU, màn hình 294, bộ xử lý ứng dụng, và tương tự. GPU là bộ vi xử lý dùng cho việc xử lý hình ảnh, và được kết nối với màn hình 294 và bộ xử lý ứng dụng. GPU được tạo cấu hình để: thực hiện phép tính toán học và hình học, và thực hiện việc kết xuất đồ họa. Bộ xử lý 210 có thể bao gồm một hoặc nhiều GPU mà thực hiện các lệnh chương trình để tạo ra hoặc thay đổi thông tin hiển thị.

Màn hình 294 được tạo cấu hình để hiển thị hình ảnh, viđeo, và tương tự. Màn hình 294 bao gồm panen màn hình. Ví dụ, theo phương án này của sáng chế, màn hình 294 có thể được tạo cấu hình để hiển thị giao diện ứng dụng của app thứ nhất, chẳng hạn như giao diện chia sẻ thiết bị, giao diện tìm kiếm thiết bị, hoặc giao diện quét mã hai chiều.

Thiết bị điện tử 200 có thể thực hiện chức năng chụp ảnh qua ISP, camera 293, bộ mã hóa-giải mã viđeo, GPU, màn hình 294, bộ xử lý ứng dụng, và tương tự. ISP được tạo cấu hình để xử lý dữ liệu được phản hồi bởi camera 293. Camera 293 được tạo cấu hình để chụp hình ảnh tĩnh hoặc viđeo. Theo một số phương án, thiết bị điện tử 200 có thể bao gồm một hoặc N camera 293, trong đó N là số nguyên dương lớn hơn 1.

Giao diện bộ nhớ ngoài 220 có thể được tạo cấu hình để kết nối với thẻ nhớ ngoài, ví dụ, thẻ vi SD, để mở rộng dung lượng lưu trữ của thiết bị điện tử 200. Thẻ nhớ

ngoài truyền thông với bộ xử lý 210 qua giao diện bộ nhớ ngoài 220, để thực hiện chức năng lưu trữ dữ liệu. Ví dụ, các tệp tin chẳng hạn như âm nhạc và viđeo được lưu trữ trong thẻ nhớ ngoài.

Bộ nhớ trong 221 có thể được tạo cấu hình để lưu trữ mã chương trình thực hiện được bởi máy tính. Mã chương trình thực hiện được bao gồm các lệnh. Bộ xử lý 210 chạy các lệnh được lưu trữ trong bộ nhớ trong 221, để thực hiện các ứng dụng chức năng khác nhau của thiết bị điện tử 200 và xử lý dữ liệu. Ví dụ, theo phương án này của sáng chế, bộ xử lý 210 có thể thực hiện các lệnh được lưu trữ trong bộ nhớ trong 221, và bộ nhớ trong 221 có thể bao gồm vùng lưu trữ chương trình và vùng lưu trữ dữ liệu.

Vùng lưu trữ chương trình có thể lưu trữ hệ điều hành, chương trình ứng dụng được yêu cầu bởi ít nhất một chức năng (ví dụ, chức năng chơi âm thanh hoặc chức năng chơi hình ảnh), và tương tự. vùng lưu trữ dữ liệu có thể lưu trữ dữ liệu (chẳng hạn như dữ liệu auđio và danh bạ điện thoại) được tạo ra khi thiết bị điện tử 200 được sử dụng, và tương tự. Ngoài ra, bộ nhớ trong 221 có thể bao gồm bộ nhớ truy cập ngẫu nhiên tốc độ cao, hoặc có thể bao gồm bộ nhớ bất khả biến, ví dụ, ít nhất một thiết bị lưu trữ đĩa từ, bộ nhớ tia chớp, hoặc bộ lưu trữ tia chớp toàn cầu (universal flash storage, viết tắt là UFS).

Thiết bị điện tử 200 có thể thực hiện chức năng auđio chẳng hạn như chơi và ghi âm nhạc qua môđun auđio 270, loa 270A, bộ thu 270B, micrô 270C, giắc cắm tai nghe 270D, bộ xử lý ứng dụng, và tương tự.

Nút nhấn 290 bao gồm nút nhấn nguồn, nút nhấn âm lượng, và tương tự. Nút nhấn 290 có thể là nút nhấn cơ học, hoặc có thể là nút nhấn chạm. Động cơ 291 có thể tạo ra nhắc rung. Động cơ 291 có thể được tạo cấu hình để cung cấp nhắc rung cuộc gọi đến hoặc phản hồi rung chạm. Bộ chỉ báo 292 có thể là ánh sáng bộ chỉ báo, và có thể được tạo cấu hình để chỉ báo trạng thái nạp và thay đổi nguồn, hoặc có thể được tạo cấu hình để chỉ báo tin nhắn, cuộc gọi nhỡ, thông báo, hoặc tương tự. Giao diện thẻ SIM 295 được tạo cấu hình để kết nối với thẻ SIM. Thẻ SIM có thể được đưa vào giao diện thẻ SIM 295 hoặc lấy ra từ giao diện thẻ SIM 295, để thực hiện sự tiếp xúc với hoặc tách ra từ thiết bị điện tử 200. Thiết bị điện tử 200 có thể bao gồm một hoặc N giao diện thẻ SIM, trong đó N là số nguyên dương lớn hơn 1. Giao diện thẻ SIM 295 có thể hỗ trợ thẻ SIM cỡ rất nhỏ (nano), thẻ SIM cỡ nhỏ (micro), thẻ SIM, và tương tự.

Ví dụ, theo phương án này của sáng chế, ví dụ trong đó thiết bị thứ nhất 110 là điện thoại di động A và thiết bị thứ hai 120 là điện thoại di động B trên Fig.1 được sử dụng để mô tả phương pháp theo phương án này của sáng chế. Ứng dụng thứ nhất được cài đặt trong điện thoại di động A. Ví dụ, ứng dụng thứ nhất có thể là ứng dụng mua sắm, ứng dụng viđeo, ứng dụng nhắn tin nhanh, hoặc ứng dụng bất kỳ khác mà có chức năng đăng ký và đăng nhập tài khoản, ví dụ, ứng dụng được sử dụng cho việc học trực tuyến. Như được thể hiện trên Fig.4(a), màn hình chính (chẳng hạn, màn hình chính) của điện thoại di động A bao gồm biểu tượng 403 của ứng dụng mua sắm, biểu tượng 402 của ứng dụng viđeo, và biểu tượng 401 của ứng dụng học.

Phương án của sáng chế đề xuất phương pháp chia sẻ dữ liệu tài khoản. Như được thể hiện trên Fig.3A và Fig.3C, phương pháp có thể bao gồm ba thủ tục: thủ tục (1) đến thủ tục (3). Thủ tục (1): Thủ tục đăng nhập thủ công của điện thoại di động A. Thủ tục (2): Thủ tục trong đó điện thoại di động A chia sẻ dữ liệu tài khoản với điện thoại di động B. Thủ tục (3): Thủ tục đăng nhập tự động của điện thoại di động B.

Như được thể hiện trên Fig.3A và Fig.3C, thủ tục (1) nêu trên, nghĩa là, "thủ tục đăng nhập thủ công của điện thoại di động A", có thể bao gồm S301 đến S305.

S301: Điện thoại di động A thu dữ liệu tài khoản được nhập bởi người dùng trên giao diện đăng nhập tài khoản của ứng dụng thứ nhất.

Theo kịch bản ứng dụng thứ nhất, giao diện đăng nhập tài khoản của ứng dụng thứ nhất có thể bao gồm "hộp đầu vào tài khoản" và "hộp đầu vào mật khẩu đăng nhập". “Hộp đầu vào tài khoản" được sử dụng để nhập tài khoản (ví dụ, tài khoản thứ nhất) của ứng dụng thứ nhất, và "hộp đầu vào mật khẩu đăng nhập" được sử dụng để nhập mật khẩu đăng nhập của tài khoản thứ nhất. Theo kịch bản ứng dụng thứ nhất, dữ liệu tài khoản có thể bao gồm tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất.

Giao diện đăng nhập tài khoản có thể còn bao gồm nút nhấn “đăng nhập (Log in)”. Nút nhấn “đăng nhập” được sử dụng để kích hoạt điện thoại di động A đăng nhập vào tài khoản thứ nhất nhờ sử dụng tài khoản thứ nhất được nhập trong “hộp đầu vào tài khoản" và mật khẩu đăng nhập của tài khoản thứ nhất được nhập trong “hộp đầu vào mật khẩu đăng nhập". Ví dụ, ứng dụng thứ nhất là ứng dụng mua sắm. Điện thoại di động A có thể hiển thị giao diện đăng nhập tài khoản 410 được thể hiện trên Fig.4(b). Giao diện đăng

nhập tài khoản 410 bao gồm "hộp đầu vào tài khoản" 411, "hộp đầu vào mật khẩu đăng nhập" 412, và nút nhấn “đăng nhập” 413.

Một cách tùy chọn, giao diện đăng nhập tài khoản của ứng dụng thứ nhất có thể còn bao gồm tùy chọn “lưu tự động”. Tùy chọn “lưu tự động” được sử dụng để kích hoạt điện thoại di động A để tự động lưu tài khoản được nhập trong “hộp đầu vào tài khoản" và mật khẩu đăng nhập được nhập trong “hộp đầu vào mật khẩu đăng nhập". Ví dụ, ứng dụng thứ nhất là ứng dụng học. Điện thoại di động A có thể hiển thị giao diện đăng nhập tài khoản 420 được thể hiện trên Fig.4(c). Giao diện đăng nhập tài khoản 420 bao gồm "hộp đầu vào tài khoản" 421, "hộp đầu vào mật khẩu đăng nhập" 422, nút nhấn “đăng nhập” 424, và nút nhấn “lưu tự động” 423.

Theo kịch bản ứng dụng thứ hai, giao diện đăng nhập tài khoản có thể bao gồm "hộp đầu vào tài khoản", "hộp đầu vào mã xác thực", và nút nhấn “thu nhận mã xác thực”. “Hộp đầu vào tài khoản" được sử dụng để nhập tài khoản chẳng hạn như số điện thoại hoặc địa chỉ thư điện tử. Nói cách khác, tài khoản thứ nhất có thể bao gồm ít nhất số điện thoại hoặc địa chỉ thư điện tử của điện thoại di động A. Nút nhấn “thu nhận mã xác thực” được sử dụng để kích hoạt điện thoại di động A để yêu cầu máy chủ của ứng dụng thứ nhất gửi mã xác thực cho tài khoản (nghĩa là, tài khoản thứ nhất, ví dụ, số điện thoại) được nhập trong “hộp đầu vào tài khoản". “Hộp đầu vào mã xác thực" được sử dụng để nhập mã xác thực được gửi bởi máy chủ tới thiết bị điện tử mà sử dụng tài khoản nêu trên (ví dụ, số điện thoại).

Theo kịch bản ứng dụng thứ hai, dữ liệu tài khoản có thể bao gồm tài khoản thứ nhất và mã xác thực. Mã xác thực 1 là mã xác thực thứ nhất. Mã xác thực 1 là mã mà điện thoại di động A yêu cầu máy chủ cấp phát. Cả mật khẩu đăng nhập của tài khoản thứ nhất và mã xác thực 1 đều có thể được sử dụng như các thông tin đăng nhập để đăng nhập vào tài khoản thứ nhất. Tuy nhiên, khác nhau ở chỗ mã xác thực 1 là không hợp lệ sau khi điện thoại di động A đăng nhập thành công vào tài khoản thứ nhất trong ứng dụng thứ nhất; hoặc mã xác thực 1 là hợp lệ nằm trong khoảng thời gian được thiết đặt trước 1 (ví dụ, 5 phút hoặc 10 phút), và mã xác thực 1 là không hợp lệ sau khoảng thời gian được thiết đặt trước 1. Thời gian bắt đầu của khoảng thời gian được thiết đặt trước 1 là thời gian mà tại đó máy chủ cấp phát mã xác thực.

Giao diện đăng nhập tài khoản có thể còn bao gồm nút nhấn “đăng nhập”. Nút nhấn “đăng nhập” được sử dụng để kích hoạt điện thoại di động A đăng nhập vào tài khoản thứ nhất nhờ sử dụng tài khoản thứ nhất được nhập trong “hộp đầu vào tài khoản" và mã xác thực 1 được nhập trong “hộp đầu vào mã xác thực".

Ví dụ, ứng dụng thứ nhất là ứng dụng viđeo. Điện thoại di động A có thể hiển thị giao diện đăng nhập tài khoản 500 của ứng dụng viđeo được thể hiện trên Fig.5. Giao diện đăng nhập tài khoản 500 bao gồm "hộp đầu vào tài khoản" 501, "hộp đầu vào mã xác thực" 502, nút nhấn “thu nhận mã xác thực” 503, và nút nhấn “đăng nhập” 504.

S302: Điện thoại di động A đăng nhập, đáp lại thao tác đăng nhập được thực hiện bởi người dùng trên giao diện đăng nhập tài khoản, vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng dữ liệu tài khoản.

Ví dụ, thao tác đăng nhập có thể là thao tác nhấn (ví dụ, thao tác nhấn đơn) được thực hiện bởi người dùng trên nút nhấn “đăng nhập” trên Fig.4(b), Fig.4(c), hoặc Fig.5. Cần lưu ý rằng, theo phương án này của sáng chế, phương pháp trong đó điện thoại di động A đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất bao gồm nhưng không giới hạn ở phương pháp được mô tả ở S301 và S302. Đối với phương pháp khác trong đó điện thoại di động A đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất, tham chiếu tới phương pháp đăng nhập tài khoản ứng dụng trong công nghệ thông thường. Chi tiết không được mô tả ở đây.

Khác với công nghệ thông thường, theo phương án này của sáng chế, sau bước S302, điện thoại di động A có thể còn lưu tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất hoặc lưu tài khoản thứ nhất dựa vào sự lựa chọn của người dùng. Cụ thể là, sau bước S302, phương pháp theo phương án này của sáng chế có thể còn bao gồm S303.

S303: Điện thoại di động A hiển thị giao diện thứ hai. Giao diện thứ hai được tạo cấu hình để yêu cầu người dùng xác nhận xem có lưu thông tin đăng nhập của tài khoản thứ nhất hay không.

Theo kịch bản ứng dụng thứ nhất, thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất. Nói cách khác,

giao diện thứ hai được tạo cấu hình để yêu cầu người dùng xác nhận xem có lưu tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất hay không. Ví dụ, điện thoại di động A có thể đăng nhập vào tài khoản thứ nhất đáp lại thao tác nhấn được thực hiện bởi người dùng trên nút nhấn “đăng nhập” được thể hiện trên Fig.4(b). Ví dụ, tài khoản thứ nhất là 180****7812. Sau khi đăng nhập vào tài khoản thứ nhất, điện thoại di động A có thể hiển thị giao diện thứ hai 610 được thể hiện ở (a) trên Fig.6A. Giao diện thứ hai 610 có thể bao gồm thông tin gợi ý 611, ví dụ, "Vui lòng xác nhận xem có lưu tài khoản 180****7812 và mật khẩu đăng nhập hay không!" (“Please confirm whether to save the account 180****7812 and the login password!”). Giao diện thứ hai 610 có thể còn bao gồm nút nhấn “Có (YES)” 612 và nút nhấn “Không (NO)” 613. Nút nhấn “Có” 612 được sử dụng để kích hoạt điện thoại di động A lưu tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất. Nút nhấn “Không” 613 được sử dụng để chỉ báo điện thoại di động A không lưu tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất. Một cách tùy chọn, giao diện thứ hai 610 có thể còn bao gồm thông tin gợi ý 614, ví dụ, "tài khoản và mật khẩu được lưu có thể được chia sẻ với thiết bị khác, và tài khoản có thể tự động được đăng nhập trên thiết bị khác!".

Có thể nhận thấy từ các phần mô tả của phương án nêu trên rằng, theo kịch bản ứng dụng thứ nhất, giao diện đăng nhập tài khoản của ứng dụng thứ nhất bao gồm "hộp đầu vào tài khoản" và "hộp đầu vào mật khẩu đăng nhập". Ví dụ, giao diện đăng nhập các tài khoản được thể hiện trên Fig.4(b) và Fig.4(c) mỗi bao gồm "hộp đầu vào tài khoản" và "hộp đầu vào mật khẩu đăng nhập". Một cách tùy chọn, giao diện đăng nhập tài khoản của ứng dụng thứ nhất có thể còn bao gồm tùy chọn “lưu tự động”. Ví dụ, giao diện đăng nhập tài khoản 420 được thể hiện trên Fig.4(c) bao gồm tùy chọn “lưu tự động” 423.

Trong trường hợp (1) của kịch bản ứng dụng thứ nhất, bất luận việc giao diện đăng nhập tài khoản của ứng dụng thứ nhất bao gồm tùy chọn “lưu tự động” hay không, sau bước S302, điện thoại di động A có thể thực hiện S303 việc hiển thị giao diện thứ hai.

Trong trường hợp (2) của kịch bản ứng dụng thứ nhất, giao diện đăng nhập tài khoản của ứng dụng thứ nhất bao gồm "lưu tự động". Trong trường hợp này, bất luận việc "lưu tự động" được lựa chọn hay không khi điện thoại di động A thực hiện S302, sau bước S302, điện thoại di động A có thể thực hiện S303 việc hiển thị giao diện thứ hai.

Trong trường hợp (3) của kịch bản ứng dụng thứ nhất, giao diện đăng nhập tài khoản của ứng dụng thứ nhất bao gồm "lưu tự động". Trong trường hợp này, nếu "lưu tự động" không được lựa chọn khi điện thoại di động A thực hiện S302, sau bước S302, điện thoại di động A có thể thực hiện S303 việc hiển thị giao diện thứ hai. Nếu "lưu tự động" được lựa chọn khi điện thoại di động A thực hiện S302, sau bước S302, điện thoại di động A có thể không thực hiện S303 (nói cách khác, có thể không hiển thị giao diện thứ hai), nhưng lưu trực tiếp thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất.

Nói chung, nếu "lưu tự động" được lựa chọn khi điện thoại di động A thực hiện S302, điện thoại di động A theo cách khác có thể lưu thông tin đăng nhập của tài khoản thứ nhất. Thông tin đăng nhập của tài khoản thứ nhất mà được lưu bởi điện thoại di động A được sử dụng để tự động đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất khi điện thoại di động A bắt đầu thời gian tiếp theo ứng dụng thứ nhất. Trong trường hợp (3), thông tin đăng nhập của tài khoản thứ nhất mà được lưu bởi điện thoại di động A không chỉ có thể được sử dụng để tự động đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất khi điện thoại di động A bắt đầu thời gian tiếp theo ứng dụng thứ nhất, mà còn có thể được sử dụng để chia sẻ thông tin đăng nhập của tài khoản thứ nhất với thiết bị khác (ví dụ, điện thoại di động B), sao cho điện thoại di động B có thể tự động đăng nhập vào tài khoản thứ nhất dựa vào thông tin đăng nhập của tài khoản thứ nhất.

Theo kịch bản ứng dụng thứ hai, thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất. Nói cách khác, giao diện thứ hai được tạo cấu hình để yêu cầu người dùng xác nhận xem có lưu tài khoản thứ nhất hay không. Ví dụ, điện thoại di động A có thể đăng nhập vào tài khoản thứ nhất đáp lại thao tác nhấn được thực hiện bởi người dùng trên nút nhấn “đăng nhập” được thể hiện trên Fig.5. Ví dụ, tài khoản thứ nhất là 176****1860. Sau khi đăng nhập vào tài khoản thứ nhất, điện thoại di động A có thể hiển thị giao diện thứ hai 620 được thể hiện ở (b) trên Fig.6A. Giao diện thứ hai 620 có thể bao gồm thông tin gợi ý 621, ví dụ, "Vui lòng xác nhận có lưu tài khoản 176****1860 hay không!" ("Please confirm whether to save the account 176****1860!"). Giao diện thứ hai 620 có thể còn bao gồm nút nhấn “Có” 622 và nút nhấn “Không” 623. Nút nhấn “Có” 622 được sử dụng để kích hoạt điện thoại di động A lưu tài khoản thứ nhất. Nút nhấn “Không”

623 được sử dụng để chỉ báo điện thoại di động A không lưu tài khoản thứ nhất. Một cách tùy chọn, giao diện thứ hai 620 có thể còn bao gồm thông tin gợi ý 624, ví dụ, "tài khoản được lưu có thể được chia sẻ với thiết bị, và tài khoản có thể tự động được đăng nhập trên thiết bị khác!".

Theo một số phương án, điện thoại di động A có thể còn cung cấp chuyển mạch chức năng (cũng được gọi là chuyển mạch thực đơn) của hệ thống. Điện thoại di động A có thể thu thao tác cho phép được thực hiện bởi người dùng trên chuyển mạch chức năng. Nếu người dùng nhập dữ liệu tài khoản trên giao diện đăng nhập tài khoản của ứng dụng thứ nhất, điện thoại di động A có thể tự động lưu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất đáp lại thao tác cho phép. Nếu chuyển mạch chức năng bị vô hiệu, điện thoại di động A không tự động lưu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất.

Ví dụ, điện thoại di động A có thể hiển thị chuyển mạch chức năng trên giao diện thiết đặt của điện thoại di động A, hoặc điện thoại di động A có thể hiển thị chuyển mạch chức năng trên thanh thực đơn. Thiết kế của chuyển mạch chức năng trong điện thoại di động A bao gồm nhưng không giới hạn ở cách thức nêu trên. Vị trí cụ thể của chuyển mạch chức năng là không giới hạn ở phương án này của sáng chế.

S304: Điện thoại di động A lưu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất đáp lại thao tác 1 được thực hiện bởi người dùng trên giao diện thứ hai.

Thao tác 1 là thao tác thứ hai. Thông tin nhận dạng của ứng dụng thứ nhất có thể bao gồm tên gói của ứng dụng thứ nhất, hoặc tên gói của ứng dụng thứ nhất và khóa công khai chữ ký của ứng dụng thứ nhất.

Ví dụ, hệ thống Android (Android) sử dụng tên gói (package name) để xác định nhận dạng của ứng dụng (nghĩa là, application). Tuy nhiên, tên gói của ứng dụng có thể là thiết đặt tự do bởi nhà phát triển của ứng dụng. Do đó, để bảo vệ ứng dụng khỏi bị lừa đảo, khi ứng dụng được phát hành, ký hiệu của nhà phát triển có thể được bổ sung tới ứng dụng. Nhà phát triển có thể tạo ra khóa ký hiệu riêng và khóa công khai chữ ký. Khóa ký hiệu riêng được sử dụng để tạo ra ký hiệu nêu trên. Khóa công khai chữ ký được sử dụng để thực hiện việc xác nhận hoặc xác thực trên ký hiệu khi ứng dụng được bắt đầu.

Có thể hiểu rằng, sau khi ứng dụng thứ nhất được cài đặt trong điện thoại di động A, ngay cả khi ứng dụng thứ nhất bị giả mạo, khóa công khai chữ ký của ứng dụng thứ nhất không thay đổi. Tuy nhiên, nếu ứng dụng thứ nhất bị giả mạo, ký hiệu của ứng dụng thứ nhất thay đổi. Theo phương án này của sáng chế, khi điện thoại di động A bắt đầu ứng dụng thứ nhất, điện thoại di động A (ví dụ, PMS ở lớp chương trình khung (framework) của điện thoại di động A) có thể thực hiện việc xác nhận trên ký hiệu của ứng dụng thứ nhất nhờ sử dụng khóa công khai chữ ký của ứng dụng thứ nhất, để xác định xem ứng dụng thứ nhất bị giả mạo hay không. Nếu ứng dụng thứ nhất bị giả mạo, điện thoại di động A không thể bắt đầu ứng dụng thứ nhất. Nếu ứng dụng thứ nhất không bị giả mạo, điện thoại di động A có thể bắt đầu ứng dụng thứ nhất. PMS là dịch vụ trình quản lý gói (package manager service, viết tắt là PMS).

Theo phương án này của sáng chế, điện thoại di động A (ví dụ, PMS ở chương trình khung của điện thoại di động A) có thể xác định xem tên gói và khóa công khai chữ ký của ứng dụng thứ nhất trong PMS trùng khớp thông tin nhận dạng của ứng dụng thứ nhất mà được lưu trong điện thoại di động A hay không, để xác định xem tên gói của ứng dụng thứ nhất bị giả mạo hay không.

Cụ thể là, điện thoại di động A có thể thu nhận tên gói và khóa công khai chữ ký của ứng dụng thứ nhất từ PMS, và so sánh tên gói và khóa công khai chữ ký được thu nhận của ứng dụng thứ nhất với thông tin nhận dạng (bao gồm tên gói và khóa công khai chữ ký) của ứng dụng thứ nhất mà được lưu trong điện thoại di động A. Nếu tên gói của ứng dụng thứ nhất mà được thu nhận bởi điện thoại di động A từ dịch vụ PMS là giống như tên gói của ứng dụng thứ nhất trong thông tin nhận dạng của ứng dụng thứ nhất mà được lưu trong điện thoại di động A, và khóa công khai chữ ký của ứng dụng thứ nhất mà được thu nhận bởi điện thoại di động A từ dịch vụ PMS là giống như khóa công khai chữ ký của ứng dụng thứ nhất trong thông tin nhận dạng của ứng dụng thứ nhất mà được lưu trong điện thoại di động A, nó chỉ báo rằng tên gói của ứng dụng thứ nhất không bị giả mạo.

Một cách tùy chọn, theo một số phương án, dịch vụ trình quản lý hoạt động (activity manager service, viết tắt là AMS) ở lớp chương trình khung (framework) của điện thoại di động A theo cách khác có thể xác định xem tên gói và khóa công khai chữ ký của ứng dụng thứ nhất trong PMS trùng khớp thông tin nhận dạng của ứng dụng thứ nhất mà

được lưu trong điện thoại di động A hay không, để xác định xem tên gói của ứng dụng thứ nhất bị giả mạo hay không.

Ví dụ, thông tin nhận dạng của ứng dụng thứ nhất bao gồm tên gói của ứng dụng thứ nhất và khóa công khai chữ ký của ứng dụng thứ nhất. Khóa công khai chữ ký của ứng dụng thứ nhất có thể là chuỗi ký tự bao gồm hàng chục đến hàng trăm byte. Theo kịch bản ứng dụng thứ nhất nêu trên, điện thoại di động A có thể thu nhận và lưu thông tin nhận dạng và thông tin đăng nhập sau đây:

<appid=com.android.shopping+deaf04e5jfhsgrck; \\package name "shopping", signature public key "deaf04e5jfhsgrck"\\

id=180****7812; \\account "180****7812"\\

pw=123xyz56789> \\login account "123xyz56789"\\

Ví dụ, thông tin nhận dạng của ứng dụng thứ nhất bao gồm tên gói của ứng dụng thứ nhất và khóa công khai chữ ký của ứng dụng thứ nhất. Theo kịch bản ứng dụng thứ hai nêu trên, điện thoại di động A có thể thu nhận và lưu thông tin nhận dạng và thông tin đăng nhập sau đây:

<appid=com.android.video+deaf04e64hfslfh; \\package name "video", signature public key signature "deaf04e64hfslfh"\\

id=176****1860> \\account "176****1860"\\

Theo phương án sau đây, ví dụ trong đó thông tin nhận dạng của ứng dụng thứ nhất bao gồm tên gói của ứng dụng thứ nhất được sử dụng để mô tả phương pháp theo phương án này của sáng chế. Cần lưu ý rằng, đối với phương pháp trong đó điện thoại di động A thu nhận thông tin nhận dạng của ứng dụng thứ nhất, tham chiếu tới phương pháp liên quan trong công nghệ thông thường. Chi tiết không được mô tả ở đây theo phương án này của sáng chế.

Có thể hiểu rằng điện thoại di động A có thể lưu các thông số liên quan của các ứng dụng khác nhau trong các vùng lưu trữ khác nhau, ví dụ, dữ liệu (chẳng hạn như dữ liệu auđio, dữ liệu hình ảnh, hoặc dữ liệu viđeo) được tạo ra khi ứng dụng được sử dụng. Theo một số phương án, điện thoại di động A có thể lưu thông tin đăng nhập của ứng dụng thứ nhất trong vùng lưu trữ tương ứng với ứng dụng thứ nhất. Theo một số phương án khác,

vùng lưu trữ có thể được thiết đặt cụ thể đối với điện thoại di động A. vùng lưu trữ có thể được sử dụng để lưu thông tin đăng nhập của mỗi ứng dụng. Ví dụ, điện thoại di động A có thể lưu thông tin đăng nhập của nhiều ứng dụng được thể hiện trong Bảng 1 trong vùng lưu trữ.

Bảng 1

Bảng thông tin đăng nhập		
Tên gói ứng dụng	Tài khoản (nghĩa là, ID)	Mật khẩu đăng nhập
mua sắm	180****7812	123xyz56789
mua sắm	157****7568	123abc56789
viđeo	176****1860	NULL
học tập	Xy123456	Abc369x246

Giả sử rằng tên gói của ứng dụng mua sắm là “mua sắm (shopping)", tên gói của ứng dụng viđeo là “viđeo (video)", và tên gói của ứng dụng học là “học tập (study)". Như được thể hiện trong Bảng 1, điện thoại di động A lưu thông tin đăng nhập của tài khoản "180****7812" của ứng dụng mua sắm, ví dụ, tài khoản "180****7812" và mật khẩu đăng nhập "123xyz56789"; lưu thông tin đăng nhập của tài khoản "176****1860" của ứng dụng viđeo, ví dụ, tài khoản "176****1860"; và lưu thông tin đăng nhập của tài khoản "Xy123456" của ứng dụng học, ví dụ, tài khoản "Xy123456" và mật khẩu đăng nhập "Abc369x246".

Một cách tùy chọn, điện thoại di động A có thể lưu thông tin đăng nhập của nhiều tài khoản của một ứng dụng. Ví dụ, như được thể hiện trong Bảng 1, điện thoại di động A lưu thông tin đăng nhập của tài khoản "180****7812" của ứng dụng mua sắm, và còn lưu thông tin đăng nhập của tài khoản "157****7568" của ứng dụng mua sắm, ví dụ, tài khoản "157****7568" và mật khẩu đăng nhập "123abc56789".

Ví dụ, điện thoại di động A có thể lưu thông tin nhận dạng của mỗi ứng dụng và thông tin đăng nhập của tài khoản dưới dạng cơ sở dữ liệu, dạng tệp tin, hoặc dạng khác.

Cách thức cụ thể trong đó điện thoại di động A lưu thông tin nhận dạng của mỗi ứng dụng và thông tin đăng nhập của tài khoản là không giới hạn ở phương án này của sáng chế.

S305: Điện thoại di động A không lưu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất đáp lại thao tác 2 được thực hiện bởi người dùng trên giao diện thứ hai.

Ví dụ, thao tác 1 là thao tác thứ hai, và thao tác 2 là thao tác thứ sáu. Thao tác 1 có thể là thao tác nhấn được thực hiện bởi người dùng trên nút nhấn "Có" 612 trên giao diện thứ hai 610 được thể hiện ở (a) trên Fig.6A; hoặc thao tác 1 có thể là thao tác nhấn được thực hiện bởi người dùng trên nút nhấn "Có" 622 trên giao diện thứ hai 620 được thể hiện ở (b) trên Fig.6A. Theo cách khác, thao tác 1 có thể là cử chỉ được thiết đặt trước thứ nhất được nhập bởi người dùng trên giao diện thứ hai, ví dụ, cử chỉ dạng chữ S. Theo cách khác, thao tác 1 có thể là lệnh âm thanh được nhập bởi người dùng khi điện thoại di động A hiển thị giao diện thứ hai. Ví dụ, lệnh âm thanh có thể bao gồm dữ liệu âm thanh chẳng hạn như "Save (lưu)", "YES (có)", "OK", hoặc "Good (tốt)".

Thao tác 2 có thể là thao tác nhấn được thực hiện bởi người dùng trên nút nhấn "Không" 613 trên giao diện thứ hai 610 được thể hiện ở (a) trên Fig.6A; hoặc thao tác 2 có thể là thao tác nhấn được thực hiện bởi người dùng trên nút nhấn "Không" 623 trên giao diện thứ hai 620 được thể hiện ở (b) trên Fig.6A. Theo cách khác, thao tác 2 có thể là cử chỉ được thiết đặt trước thứ hai được nhập bởi người dùng trên giao diện thứ hai, ví dụ, cử chỉ dạng chữ L. Theo cách khác, thao tác 2 có thể là lệnh âm thanh được nhập bởi người dùng khi điện thoại di động A hiển thị giao diện thứ hai. Ví dụ, lệnh âm thanh có thể bao gồm dữ liệu âm thanh chẳng hạn như "Do not save (không lưu)" hoặc "NO (không)".

Fig.6B thể hiện lưu đồ sơ đồ khối của thủ tục (1) (nghĩa là, thủ tục đăng nhập thủ công của điện thoại di động A). Như được thể hiện trên Fig.6B, điện thoại di động A có thể thực hiện S301 và S302 để đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất. Sau đó, điện thoại di động A có thể thực hiện S303 để yêu cầu người dùng xác nhận xem có lưu thông tin đăng nhập của tài khoản thứ nhất hay không. Cuối cùng, điện thoại di động A có thể thu thao tác 1 của người dùng. Thao tác 1 được sử dụng để chỉ báo điện thoại di động A để lưu thông tin đăng nhập của tài khoản thứ nhất. Điện thoại di động A có thể thực hiện S304 việc lưu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng

nhập của tài khoản thứ nhất đáp lại thao tác 1. Theo cách khác, sau bước S303, điện thoại di động A có thể thu thao tác 2 của người dùng. Thao tác 2 được sử dụng để chỉ báo điện thoại di động A không lưu thông tin đăng nhập của tài khoản thứ nhất. Điện thoại di động A có thể thực hiện S305 việc bỏ qua lưu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất đáp lại thao tác 2.

Theo phương án này của sáng chế, Sau khi đăng nhập vào tài khoản thứ nhất, điện thoại di động A có thể lưu thông tin đăng nhập của tài khoản thứ nhất đáp lại thao tác 1 của người dùng. Theo cách này, khi thu thao tác được sử dụng để chia sẻ tài khoản thứ nhất, điện thoại di động A có thể chia sẻ thông tin đăng nhập được lưu với thiết bị khác.

Có thể hiểu rằng, sau thủ tục (1) nêu trên, điện thoại di động A đã đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất, và điện thoại di động A lưu thông tin đăng nhập của tài khoản thứ nhất. Có thể nhận thấy từ Bảng 1 rằng điện thoại di động A có thể đăng nhập vào nhiều tài khoản trong ứng dụng thứ nhất, và điện thoại di động A có thể lưu thông tin đăng nhập của nhiều tài khoản đối với ứng dụng thứ nhất. Tuy nhiên, điện thoại di động A không thể đăng nhập đồng thời vào nhiều tài khoản trong ứng dụng thứ nhất, và có thể đăng nhập một cách có lựa chọn vào chỉ một tài khoản ở cùng thời gian. Tài khoản thứ nhất theo phương án này của sáng chế là tài khoản hiện được đăng nhập bởi điện thoại di động A trong ứng dụng thứ nhất.

Phương án của sáng chế đề xuất phương pháp chia sẻ dữ liệu tài khoản. Như được thể hiện trên Fig.3A và Fig.3C, thủ tục (2) nêu trên, nghĩa là, "thủ tục trong đó điện thoại di động A chia sẻ dữ liệu tài khoản với điện thoại di động B", có thể bao gồm S701 đến S704. Theo cách khác, như được thể hiện trên Fig.7A-1 và Fig.7A-2, phương pháp chia sẻ dữ liệu tài khoản có thể bao gồm S701 đến S704.

S701: Điện thoại di động A thu thao tác 3 được thực hiện bởi người dùng trên ứng dụng thứ nhất, trong đó thao tác 3 được sử dụng để kích hoạt điện thoại di động A chia sẻ thông tin đăng nhập của tài khoản thứ nhất với thiết bị khác.

Thao tác 3 là thao tác thứ nhất. Ví dụ, thao tác 3 có thể là thao tác người dùng được mô tả theo cách thực hiện (1) hoặc cách thực hiện (2) sau đây.

Cách thực hiện (1)

Điện thoại di động A có thể thu thao tác được thiết đặt trước được thực hiện bởi người dùng trên biểu tượng của ứng dụng thứ nhất được hiển thị trên màn hình chính (chẳng hạn, màn hình chính). Ví dụ, thao tác được thiết đặt trước là thao tác bất kỳ chẳng hạn như thao tác chạm và giữ, thao tác nhấn đúp, hoặc thao tác trượt (ví dụ, thao tác trượt lên hoặc thao tác trượt xuống) được thực hiện trên biểu tượng của ứng dụng thứ nhất. Điện thoại di động A có thể hiển thị tùy chọn được thiết đặt trước (cũng được gọi là tùy chọn "chia sẻ đăng nhập (Share login)" hoặc tùy chọn "chia sẻ trạng thái đăng nhập (Share login status)" của ứng dụng thứ nhất đáp lại thao tác được thiết đặt trước. Điện thoại di động A có thể thực hiện S702 đáp lại thao tác nhấn (ví dụ, thao tác nhấn đơn) được thực hiện bởi người dùng trên tùy chọn được thiết đặt trước, để hiển thị giao diện tìm kiếm thiết bị của điện thoại di động A.

Ví dụ, ứng dụng thứ nhất là ứng dụng mua sắm, và thao tác được thiết đặt trước là thao tác chạm và giữ. Điện thoại di động A có thể hiển thị tùy chọn "chia sẻ đăng nhập" 701 được thể hiện ở (a) trên Fig.7B đáp lại thao tác chạm và giữ được thực hiện bởi người dùng trên biểu tượng 403 của ứng dụng mua sắm. Điện thoại di động A có thể hiển thị giao diện tìm kiếm thiết bị 703 được thể hiện ở (b) trên Fig.7B đáp lại thao tác nhấn được thực hiện bởi người dùng trên tùy chọn "chia sẻ đăng nhập" 701.

Có thể nhận thấy từ các phần mô tả nêu trên rằng, theo cách thực hiện (1), thao tác 3 (nghĩa là, thao tác thứ nhất) có thể bao gồm thao tác được thiết đặt trước được thực hiện bởi người dùng trên biểu tượng của ứng dụng thứ nhất và thao tác nhấn được thực hiện bởi người dùng trên tùy chọn "chia sẻ đăng nhập".

Cách thực hiện (2)

Điện thoại di động A có thể hiển thị trang được thiết đặt trước của ứng dụng thứ nhất. Trang được thiết đặt trước có thể là trang bất kỳ của ứng dụng thứ nhất, ví dụ, trang chủ của ứng dụng thứ nhất hoặc trang khác của ứng dụng thứ nhất. Trang được thiết đặt trước có thể bao gồm sự điều khiển được thiết đặt trước, ví dụ, sự điều khiển "chia sẻ đăng nhập". Sự điều khiển được thiết đặt trước được sử dụng để kích hoạt điện thoại di động A chia sẻ thông tin đăng nhập của tài khoản thứ nhất với thiết bị khác. Thao tác 3 (nghĩa là, thao tác thứ nhất) có thể là thao tác nhấn được thực hiện bởi người dùng trên sự điều khiển được thiết đặt trước, ví dụ, thao tác bất kỳ chẳng hạn như thao tác nhấn đơn hoặc thao tác

nhấn đúp. Theo cách khác, thao tác 3 (ví dụ, thao tác thứ nhất) có thể là lệnh âm thanh mà được thu khi điện thoại di động A hiển thị trang được thiết đặt trước bao gồm sự điều khiển được thiết đặt trước và mà được sử dụng để chỉ báo điện thoại di động A để kích hoạt sự điều khiển được thiết đặt trước.

Ví dụ, trang được thiết đặt trước là giao diện quản lý tài khoản 705 của ứng dụng mua sắm được thể hiện trên Fig.7C. Giao diện quản lý tài khoản 705 bao gồm sự điều khiển "chia sẻ đăng nhập" 706 (nghĩa là, sự điều khiển được thiết đặt trước). Điện thoại di động A có thể hiển thị giao diện tìm kiếm thiết bị 703 được thể hiện ở (b) trên Fig.7B đáp lại thao tác nhấn được thực hiện bởi người dùng trên sự điều khiển "chia sẻ đăng nhập" 706 được thể hiện trên Fig.7C.

S702: Điện thoại di động A hiển thị giao diện thứ nhất đáp lại thao tác 3, trong đó giao diện thứ nhất bao gồm một hoặc nhiều tùy chọn thiết bị, và mỗi tùy chọn thiết bị tương ứng với một thiết bị không dây được tìm thấy bởi điện thoại di động A.

Ví dụ, các thiết bị không dây tương ứng với một hoặc nhiều tùy chọn thiết bị là các thiết bị không dây có các tín hiệu không dây mà có thể được tìm thấy bởi điện thoại di động A. Tín hiệu không dây có thể là tín hiệu bất kỳ chẳng hạn như tín hiệu Bluetooth, tín hiệu Wi-Fi, hoặc tín hiệu NFC. Ví dụ, tín hiệu không dây là tín hiệu Bluetooth. Giao diện thứ nhất có thể là giao diện tìm kiếm thiết bị 703 được thể hiện ở (b) trên Fig.7B. Giao diện tìm kiếm thiết bị 703 bao gồm các tùy chọn thiết bị sau đây: tùy chọn "ABC", tùy chọn "SHOUJI-B" 704, tùy chọn "Xyzd", và tùy chọn "G1B-1B-19-7R". Mỗi tùy chọn thiết bị tương ứng với một thiết bị Bluetooth. Giả sử rằng tùy chọn "SHOUJI-B" 704 là tên Bluetooth của điện thoại di động B, và thiết bị Bluetooth tương ứng với tùy chọn "SHOUJI-B" 704 là điện thoại di động B.

Có thể hiểu rằng trạng thái trong đó điện thoại di động A hiển thị giao diện thứ nhất đáp lại thao tác 3 có thể được gọi là trạng thái cần được chia sẻ. Nói cách khác, điện thoại di động A có thể nhập trạng thái cần được chia sẻ đáp lại thao tác 3. Trong trạng thái cần được chia sẻ, điện thoại di động A có thể chia sẻ, đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị, thông tin đăng nhập của tài khoản thứ nhất với thiết bị không dây tương ứng với tùy chọn thiết bị được lựa chọn bởi người dùng.

S703: Điện thoại di động A thu thao tác lựa chọn được thực hiện bởi người dùng

trên tùy chọn thiết bị thứ nhất trên giao diện thứ nhất.

S704: Điện thoại di động A gửi, đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất, thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới điện thoại di động B tương ứng với tùy chọn thiết bị thứ nhất.

Tùy chọn thiết bị thứ nhất có thể là tùy chọn thiết bị bất kỳ được lựa chọn bởi người dùng trên giao diện thứ nhất. Giả sử rằng tùy chọn thiết bị thứ nhất là tùy chọn "SHOUJI-B" 704 trên giao diện tìm kiếm thiết bị 703 (nghĩa là, giao diện thứ nhất) được thể hiện ở (b) trên Fig.7B. Điện thoại di động A có thể gửi, đáp lại thao tác lựa chọn (ví dụ, thao tác nhấn) được thực hiện bởi người dùng trên tùy chọn "SHOUJI-B" 704 được thể hiện ở (b) trên Fig.7B, thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới điện thoại di động B qua kết nối Bluetooth giữa điện thoại di động A và điện thoại di động B.

Trong trường hợp, điện thoại di động B tương ứng với tùy chọn thiết bị thứ nhất đã thiết lập sự kết nối không dây tới điện thoại di động A. Trong trường hợp này, điện thoại di động A có thể gửi trực tiếp thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới điện thoại di động B qua kết nối Bluetooth giữa điện thoại di động A và điện thoại di động B.

Trong trường hợp khác, điện thoại di động B tương ứng với tùy chọn thiết bị thứ nhất không thiết lập sự kết nối không dây tới điện thoại di động A. Trong trường hợp này, điện thoại di động A có thể yêu cầu thiết lập sự kết nối không dây tới điện thoại di động B đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất. Sau khi thiết lập sự kết nối không dây tới điện thoại di động B, điện thoại di động A có thể tự động gửi thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới điện thoại di động B.

Cần lưu ý rằng, đối với phương pháp thiết lập sự kết nối không dây giữa điện thoại di động A và điện thoại di động B, tham chiếu tới phương pháp thiết lập sự kết nối không dây giữa hai thiết bị trong công nghệ thông thường. Chi tiết không được mô tả ở đây theo phương án này của sáng chế.

Theo một số phương án, điện thoại di động A có thể hiển thị thông tin gợi ý thứ nhất đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất. Thông tin gợi ý thứ nhất được sử dụng để yêu cầu người dùng xác nhận xem có chia sẻ thông tin đăng nhập của tài khoản thứ nhất với thiết bị không dây tương ứng với tùy chọn thiết bị thứ nhất hay không. Ví dụ, điện thoại di động A có thể hiển thị thông tin gợi ý thứ nhất 707 được thể hiện trên Fig.7D đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn "SHOUJI-B" 704 được thể hiện ở (b) trên Fig.7B, ví dụ, "Vui lòng xác nhận xem có chia sẻ thông tin đăng nhập của tài khoản '180****7812' với SHOUJI-B hay không!" ("Please confirm whether to share login information of account '180****7812' with SHOUJI-B!"). Thông tin gợi ý thứ nhất có thể còn bao gồm nút nhấn "Có" và nút nhấn "Không". Điện thoại di động A có thể thu thao tác 4 được thực hiện bởi người dùng trên thông tin gợi ý thứ nhất. Thao tác 4 là thao tác thứ ba. Điện thoại di động A có thể gửi thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới điện thoại di động B đáp lại thao tác 4 được thực hiện trên thông tin gợi ý thứ nhất (ví dụ, thao tác nhấn được thực hiện trên nút nhấn "Có"). Điện thoại di động A không gửi thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới điện thoại di động B đáp lại thao tác 5 được thực hiện trên thông tin gợi ý thứ nhất (ví dụ, thao tác nhấn được thực hiện trên nút nhấn "Không"), và điện thoại di động A có thể hiển thị giao diện thứ nhất 703 được thể hiện ở (b) trên Fig.7B hoặc màn hình chính 400 được thể hiện trên Fig.4(a).

Theo một số phương án, để bảo vệ bảo mật thông tin người dùng, điện thoại di động A có thể thực hiện việc xác thực danh tính người dùng đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất. Nếu việc xác thực danh tính người dùng thành công, điện thoại di động A có thể gửi thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới điện thoại di động B. Theo cách khác, nếu việc xác thực danh tính người dùng thành công, điện thoại di động A có thể hiển thị thông tin gợi ý thứ nhất, và điện thoại di động A có thể gửi thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới điện thoại di động B đáp lại thao tác thứ nhất được thực hiện bởi người dùng trên thông tin gợi ý thứ nhất.

Theo một số phương án khác, để bảo vệ bảo mật thông tin người dùng, điện thoại

di động A có thể thực hiện việc xác thực danh tính người dùng đáp lại thao tác thứ ba (ví dụ, thao tác 4) được thực hiện trên thông tin gợi ý thứ nhất. Nếu việc xác thực danh tính người dùng thành công, điện thoại di động A có thể gửi thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới điện thoại di động B.

Theo phương án nêu trên, nếu việc xác thực danh tính bị lỗi, điện thoại di động A không gửi thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới điện thoại di động B, và điện thoại di động A có thể gửi trả lại giao diện thứ nhất 703 được thể hiện ở (b) trên Fig.7B hoặc màn hình chính 400 được thể hiện trên Fig.4(a).

Ví dụ, việc xác thực danh tính người dùng có thể là việc xác thực mật khẩu hoặc xác thực dấu vân tay. Điện thoại di động A có thể hiển thị giao diện đăng ký mật khẩu và/hoặc dấu vân tay, và thu mật khẩu hoặc dấu vân tay được nhập bởi người dùng, để thực hiện việc xác thực danh tính người dùng. Theo cách khác, việc xác thực danh tính người dùng có thể là nhận dạng khuôn mặt hoặc nhận dạng mống mắt. Điện thoại di động A có thể hiển thị giao diện nhận dạng khuôn mặt hoặc giao diện nhận dạng mống mắt, và tập hợp thông tin mống mắt hoặc hình ảnh khuôn mặt được nhập bởi người dùng, để thực hiện việc xác thực danh tính người dùng. Theo cách khác, điện thoại di động A có thể tập hợp thông tin mống mắt hoặc hình ảnh khuôn mặt của người dùng theo cách thức người dùng không biết, để thực hiện việc xác thực danh tính người dùng.

Theo một số phương án, sau bước S704, điện thoại di động A có thể hiển thị thông tin gợi ý thứ hai. Thông tin gợi ý thứ hai được sử dụng để chỉ báo rằng điện thoại di động A đã chia sẻ thông tin đăng nhập của tài khoản thứ nhất với điện thoại di động B. Ví dụ, điện thoại di động A có thể hiển thị thông tin gợi ý thứ hai 708 được thể hiện trên Fig.7E, ví dụ, "thông tin đăng nhập của tài khoản '180****7812' đã được chia sẻ với SHOUJI-B!" ("login information of account '180****7812' has been shared with SHOUJI-B!").

Theo phương pháp chia sẻ dữ liệu tài khoản được đề xuất theo phương án này của sáng chế, máy khách và máy chủ của ứng dụng bất kỳ không cần được phát triển thêm, và điện thoại di động A có thể chia sẻ thông tin đăng nhập của ứng dụng với thiết bị khác đáp lại thao tác 3 (nghĩa là, thao tác thứ nhất) được thực hiện bởi người dùng trên ứng dụng. Nói cách khác, theo phương pháp theo phương án này của sáng chế, thiết bị điện tử có thể

chia sẻ một cách thích hợp thông tin đăng nhập của ứng dụng được lựa chọn bởi người dùng với thiết bị khác (ví dụ, điện thoại di động B). Tóm lại, phương pháp theo phương án này của sáng chế có thể bảo vệ bảo mật thông tin người dùng và thực hiện một cách thông minh việc đăng nhập được ủy quyền một lần giữa các thiết bị với chi phí thấp.

Có thể hiểu rằng, sau thủ tục (2) nêu trên, điện thoại di động B có thể thu thông tin đăng nhập của tài khoản thứ nhất được gửi bởi điện thoại di động A. Điện thoại di động B có thể đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất dựa vào thông tin đăng nhập của tài khoản thứ nhất. Cụ thể là, như được thể hiện trên Fig.3A và Fig.3C, thủ tục (3) nêu trên, nghĩa là, "thủ tục đăng nhập tự động của điện thoại di động B", có thể bao gồm S801 đến S805. Theo cách khác, như được thể hiện trên Fig.7A-1 và Fig.7A-2, phương pháp chia sẻ dữ liệu tài khoản có thể bao gồm S801 đến S805.

S801: Điện thoại di động B thu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất từ điện thoại di động A.

Điện thoại di động B có thể thu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất từ điện thoại di động A qua sự kết nối không dây giữa điện thoại di động B và điện thoại di động A.

S802: Điện thoại di động B xác định, dựa vào thông tin nhận dạng của ứng dụng thứ nhất, xem điện thoại di động B chạy ứng dụng thứ nhất hay không.

Theo phương án này của sáng chế, điện thoại di động B chạy ứng dụng thứ nhất có thể cụ thể là bao gồm bất kỳ một trong số ba trường hợp sau đây. Trường hợp (1): điện thoại di động B chạy ứng dụng thứ nhất trong nền trước. Trường hợp (2): điện thoại di động B chạy ứng dụng thứ nhất trong nền sau. Trường hợp (3): điện thoại di động B hiển thị trang web của ứng dụng thứ nhất trong trình duyệt.

Ví dụ, theo một số phương án, điện thoại di động B có thể xác định, bằng cách thực hiện bước 1 đến bước 7, xem điện thoại di động B chạy ứng dụng thứ nhất hay không.

Bước 1: Điện thoại di động A so sánh thông tin nhận dạng của ứng dụng thứ nhất (ví dụ, tên gói của ứng dụng thứ nhất) với tên gói của ứng dụng chạy trong nền trước của điện thoại di động B. Bước 2: Nếu tên gói của ứng dụng thứ nhất là giống như tên gói của ứng dụng chạy trong nền trước, nó chỉ báo rằng điện thoại di động B đang chạy ứng dụng

thứ nhất, nói cách khác, điện thoại di động B chạy ứng dụng thứ nhất trong trường hợp (1) nêu trên.

Bước 3: Nếu tên gói của ứng dụng thứ nhất là khác với tên gói của ứng dụng chạy trong nền trước, điện thoại di động B có thể so sánh tên gói của ứng dụng thứ nhất với tên gói của ứng dụng chạy trong nền sau của điện thoại di động B. Bước 4: Nếu tên gói của ứng dụng thứ nhất là giống như tên gói của ứng dụng bất kỳ chạy trong nền sau của điện thoại di động B, nó chỉ báo rằng điện thoại di động B đang chạy ứng dụng thứ nhất, nói cách khác, điện thoại di động B chạy ứng dụng thứ nhất trong trường hợp (2) nêu trên.

Bước 5: Nếu tên gói của ứng dụng thứ nhất là khác với tên gói của mỗi ứng dụng chạy trong nền sau của điện thoại di động B, điện thoại di động B có thể xác định xem điện thoại di động B mở trang web của ứng dụng thứ nhất trong trình duyệt hay không. Bước 6: Nếu điện thoại di động B mở trang web của ứng dụng thứ nhất trong trình duyệt, nó chỉ báo rằng điện thoại di động B đang chạy ứng dụng thứ nhất, nói cách khác, điện thoại di động B chạy ứng dụng thứ nhất trong trường hợp (3) nêu trên. Bước 7: Nếu điện thoại di động B không mở trang web của ứng dụng thứ nhất trong trình duyệt, nó chỉ báo rằng điện thoại di động B không chạy ứng dụng thứ nhất.

Điện thoại di động B có thể chạy trình duyệt trong nền trước hoặc chạy trình duyệt trong nền sau. Điện thoại di động B có thể lưu trữ trước sự tương ứng giữa tên gói của ứng dụng thứ nhất và trang web của ứng dụng thứ nhất. Theo cách khác, điện thoại di động B có thể thu nhận sự tương ứng giữa tên gói của ứng dụng thứ nhất và trang web của ứng dụng thứ nhất từ máy chủ của ứng dụng thứ nhất.

Theo một số phương án khác, sau bước 3, nếu tên gói của ứng dụng thứ nhất là khác với tên gói của mỗi ứng dụng chạy trong nền sau của điện thoại di động B, điện thoại di động B có thể không thực hiện bước 5 (nói cách khác, có thể không xác định xem điện thoại di động B mở trang web của ứng dụng thứ nhất trong trình duyệt hay không), nhưng trực tiếp xác định rằng điện thoại di động B không chạy ứng dụng thứ nhất.

Cụ thể là, nếu điện thoại di động B đang chạy ứng dụng thứ nhất, điện thoại di động B có thể thực hiện S803. Nếu điện thoại di động B không chạy ứng dụng thứ nhất, điện thoại di động B có thể thực hiện S805.

Theo một số phương án, sau bước S801, điện thoại di động B có thể hiển thị giao diện thứ ba. Giao diện thứ ba được tạo cấu hình để yêu cầu người dùng xác nhận xem có đăng nhập vào tài khoản thứ nhất hay không nhờ sử dụng thông tin đăng nhập của tài khoản thứ nhất mà được chia sẻ bởi điện thoại di động A. Ví dụ, điện thoại di động B có thể hiển thị giao diện thứ ba 800 được thể hiện trên Fig.8. Giao diện thứ ba 800 bao gồm thông tin gợi ý "điện thoại đã thu thông tin đăng nhập của tài khoản '180****7812' được chia sẻ bởi SHOUJI-A. Vui lòng xác nhận xem có đăng nhập vào tài khoản hay không!" ("phone has received login information of account '180****7812' shared by SHOUJI-A. Please confirm whether to log in to account!"). Giao diện thứ ba 800 còn bao gồm nút nhấn “đăng nhập” và nút nhấn “Loại bỏ”. Điện thoại di động B có thể thu thao tác 6 được thực hiện bởi người dùng trên giao diện thứ ba 800. Thao tác 6 là thao tác thứ năm. Điện thoại di động A có thể thực hiện S802 đáp lại thao tác 6 được thực hiện bởi người dùng trên giao diện thứ ba 800. Điện thoại di động A có thể thực hiện S805 đáp lại thao tác 7 được thực hiện bởi người dùng trên giao diện thứ ba 800. Thao tác 6 được sử dụng để kích hoạt điện thoại di động B để đăng nhập vào tài khoản thứ nhất. Ví dụ, thao tác 6 có thể là thao tác nhấn được thực hiện bởi người dùng trên nút nhấn “đăng nhập” trên giao diện thứ ba 800. Thao tác 7 được sử dụng để chỉ báo điện thoại di động B không đăng nhập vào tài khoản thứ nhất. Ví dụ, thao tác 7 có thể là thao tác nhấn được thực hiện bởi người dùng trên nút nhấn “Loại bỏ (Discard)” trên giao diện thứ ba 800.

Theo một số phương án khác, sau bước S802, nếu điện thoại di động B đang chạy ứng dụng thứ nhất, điện thoại di động B có thể hiển thị giao diện thứ ba. Ví dụ, điện thoại di động B có thể hiển thị giao diện thứ ba 800 được thể hiện trên Fig.8. Điện thoại di động B có thể thực hiện S803 đáp lại thao tác thứ nhất được thực hiện bởi người dùng trên giao diện thứ ba 800. Điện thoại di động B có thể thực hiện S805 đáp lại thao tác thứ hai được thực hiện bởi người dùng trên giao diện thứ ba 800.

S803: Điện thoại di động B hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất, và điền thông tin đăng nhập của tài khoản thứ nhất trên giao diện đăng nhập tài khoản.

Trong trường hợp, khi điện thoại di động B thực hiện S801, điện thoại di động B chạy ứng dụng thứ nhất trong nền trước. Ngoài ra, điện thoại di động B đang hiển thị

giao diện đăng nhập tài khoản của ứng dụng thứ nhất. Ví dụ, để cho phép điện thoại di động B đăng nhập vào tài khoản thứ nhất dựa vào thông tin đăng nhập của tài khoản thứ nhất từ điện thoại di động A, người dùng của điện thoại di động B có thể thao tác điện thoại di động B trước để hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất. Nói cách khác, trước khi thực hiện S801 (nghĩa là, thu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất từ điện thoại di động A), điện thoại di động B đã chạy ứng dụng thứ nhất trong nền trước đáp lại thao tác người dùng, và đang hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất. Trong trường hợp này, điện thoại di động B có thể nhập trực tiếp thông tin đăng nhập của tài khoản thứ nhất trên giao diện đăng nhập tài khoản.

Trong trường hợp khác, khi điện thoại di động B thực hiện S801, điện thoại di động B chạy ứng dụng thứ nhất trong nền trước. Tuy nhiên, điện thoại di động B không hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất. Ví dụ, điện thoại di động B hiển thị trang chủ của ứng dụng thứ nhất. Trong trường hợp này, điện thoại di động B có thể tự động nhảy tới giao diện đăng nhập tài khoản của ứng dụng thứ nhất, nói cách khác, tự động hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất, và nhập thông tin đăng nhập của tài khoản thứ nhất trên giao diện đăng nhập tài khoản.

Trong trường hợp khác, khi điện thoại di động B thực hiện S801, điện thoại di động B chạy ứng dụng thứ nhất trong nền sau. Ngoài ra, giao diện được hiển thị khi điện thoại di động B chạy ứng dụng thứ nhất trong nền sau là giao diện đăng nhập tài khoản. Trong trường hợp này, điện thoại di động B có thể chạy ứng dụng thứ nhất trong nền trước, hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất, và nhập thông tin đăng nhập của tài khoản thứ nhất trên giao diện đăng nhập tài khoản.

Trong trường hợp khác, khi điện thoại di động B thực hiện S801, điện thoại di động B chạy ứng dụng thứ nhất trong nền sau. Ngoài ra, giao diện được hiển thị khi điện thoại di động B chạy ứng dụng thứ nhất trong nền sau không phải giao diện đăng nhập tài khoản. Trong trường hợp này, điện thoại di động B có thể chạy ứng dụng thứ nhất trong nền trước, tự động nhảy tới giao diện đăng nhập tài khoản của ứng dụng thứ nhất, nói cách khác, tự động hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất, và nhập thông tin đăng nhập của tài khoản thứ nhất trên giao diện đăng nhập tài khoản.

Trong trường hợp khác, khi điện thoại di động B thực hiện S801, điện thoại di động B hiển thị trang web của ứng dụng thứ nhất trong trình duyệt. Điện thoại di động B có thể chạy trình duyệt trong nền trước hoặc chạy trình duyệt trong nền sau. Ngoài ra, trang web là giao diện đăng nhập tài khoản của ứng dụng thứ nhất. Trong trường hợp này, điện thoại di động B có thể chạy trình duyệt trong nền trước, và hiển thị trang web của ứng dụng thứ nhất trong trình duyệt, nghĩa là, giao diện đăng nhập tài khoản. Sau đó, điện thoại di động B có thể nhập thông tin đăng nhập của tài khoản thứ nhất trên giao diện đăng nhập tài khoản.

Theo kịch bản ứng dụng thứ nhất, thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất. Theo kịch bản ứng dụng, giao diện đăng nhập tài khoản của ứng dụng thứ nhất ở S803 có thể là giao diện đăng nhập tài khoản 901 của ứng dụng thứ nhất được thể hiện ở (a) trên Fig.9. Giao diện đăng nhập tài khoản 901 bao gồm "hộp đầu vào tài khoản" 902 và "hộp đầu vào mật khẩu đăng nhập" 903.

Theo kịch bản ứng dụng, điện thoại di động B có thể phát hiện "hộp đầu vào tài khoản" trên giao diện đăng nhập tài khoản, điền tài khoản thứ nhất vào “hộp đầu vào tài khoản" 902 được phát hiện, phát hiện "hộp đầu vào mật khẩu đăng nhập" trên giao diện đăng nhập tài khoản, và điền mật khẩu đăng nhập của tài khoản thứ nhất vào “hộp đầu vào mật khẩu đăng nhập" 903 được phát hiện. Điện thoại di động B có thể hiển thị giao diện đăng nhập tài khoản được thể hiện ở (b) trên Fig.9. Trên giao diện đăng nhập tài khoản được thể hiện ở (b) trên Fig.9, "hộp đầu vào tài khoản" 902 được điền với tài khoản thứ nhất "180****7812", và "hộp đầu vào mật khẩu đăng nhập" 903 được điền với mật khẩu đăng nhập.

Điện thoại di động B có thể xác định, bằng cách phát hiện thông tin gợi ý và thuộc tính của sự điều khiển hộp đầu vào (ví dụ, "hộp đầu vào tài khoản" 902 hoặc "hộp đầu vào mật khẩu đăng nhập" 903) trên trang hiện tại được hiển thị bởi điện thoại di động B, xem sự điều khiển hộp đầu vào được sử dụng để nhập tài khoản hay mật khẩu. Thông tin gợi ý là thông tin gợi ý mặc định trong hộp văn bản (ví dụ, sự điều khiển hộp đầu vào nêu trên). Ví dụ, thông tin gợi ý có thể là thông tin gợi ý "Vui lòng nhập tài khoản" ("Please enter account") vào “hộp đầu vào tài khoản" 902 và thông tin gợi ý "Vui lòng nhập mật

khẩu" ("Please enter password") vào "hộp đầu vào mật khẩu đăng nhập" 903 được thể hiện ở (a) trên Fig.9. Thông tin gợi ý trong sự điều khiển hộp đầu vào có thể biến mất đáp lại thao tác nhấn được thực hiện bởi người dùng trên sự điều khiển hộp đầu vào.

Ví dụ, giao diện đăng nhập tài khoản của ứng dụng thứ nhất là giao diện đăng nhập trang web của ứng dụng thứ nhất. Nhờ sử dụng phương pháp gethtmlinfo, điện thoại di động B có thể thu nhận thông tin liên quan (chẳng hạn như thuộc tính và thông tin gợi ý) của sự điều khiển hộp đầu vào để xác định xem sự điều khiển hộp đầu vào được sử dụng để nhập tài khoản hay mật khẩu. Nhờ sử dụng phương pháp gethtmlinfo, điện thoại di động B có thể thu nhận thông tin ngôn ngữ đánh dấu siêu văn bản (Hypertext Markup Language, viết tắt là HTML) trên giao diện đăng nhập tài khoản của ứng dụng thứ nhất, nghĩa là, thông tin liên quan của sự điều khiển hộp đầu vào, để nhận dạng sự điều khiển hộp đầu vào được sử dụng để nhập tài khoản hoặc mật khẩu.

Theo kịch bản ứng dụng thứ hai, thông tin đăng nhập của tài khoản thứ nhất bao gồm tài khoản thứ nhất, nhưng không bao gồm mật khẩu đăng nhập của tài khoản thứ nhất. Theo kịch bản ứng dụng, giao diện đăng nhập tài khoản của ứng dụng thứ nhất ở S803 có thể là giao diện đăng nhập tài khoản 1001 của ứng dụng thứ nhất được thể hiện trên Fig.10(a). Giao diện đăng nhập tài khoản 1001 bao gồm "hộp đầu vào tài khoản" 1002, "hộp đầu vào mã xác thực" 1003, và nút nhấn "thu nhận mã xác thực" 1004.

Theo kịch bản ứng dụng, điện thoại di động B có thể phát hiện "hộp đầu vào tài khoản" trên giao diện đăng nhập tài khoản, và điền tài khoản thứ nhất vào "hộp đầu vào tài khoản" 1002 được phát hiện. Điện thoại di động B có thể hiển thị giao diện đăng nhập tài khoản được thể hiện trên Fig.10(b). Trên giao diện đăng nhập tài khoản được thể hiện trên Fig.10(b), "hộp đầu vào tài khoản" 1002 được điền với tài khoản thứ nhất "180****7812".

Theo một số phương án, thông tin nhận dạng của ứng dụng thứ nhất bao gồm tên gói của ứng dụng thứ nhất và khóa công khai chữ ký của ứng dụng thứ nhất. Trước khi thực hiện S803, điện thoại di động B có thể còn xác định xem tên gói của ứng dụng thứ nhất bị giả mạo hay không. Phương pháp trong đó điện thoại di động B xác định xem tên gói của ứng dụng thứ nhất bị giả mạo hay không là tương tự với phương pháp trong đó điện thoại di động A xác định xem tên gói của ứng dụng thứ nhất bị giả mạo hay không. Chi tiết không được mô tả lại ở đây theo phương án này của sáng chế. Nếu tên gói của ứng

dụng thứ nhất không bị giả mạo, điện thoại di động B có thể thực hiện S803; hoặc nếu tên gói của ứng dụng thứ nhất bị giả mạo, điện thoại di động B có thể thực hiện S805.

S804: Điện thoại di động B đăng nhập, đáp lại thao tác 8 được thực hiện trên giao diện đăng nhập tài khoản, vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng thông tin đăng nhập của tài khoản thứ nhất.

Thao tác 8 là thao tác thứ tư. Theo kịch bản ứng dụng thứ nhất, thao tác 8 có thể là thao tác nhấn được thực hiện bởi người dùng trên nút nhấn "đăng nhập" 904 được thể hiện ở (b) trên Fig.9. Theo cách khác, thao tác 8 có thể là thao tác nhấn tự động được thực hiện trên nút nhấn "đăng nhập" 904 sau khi điện thoại di động B điền tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất trên giao diện đăng nhập tài khoản được thể hiện ở (b) trên Fig.9. Ví dụ, điện thoại di động B có thể thực hiện S803 việc hiển thị giao diện đăng nhập tài khoản được thể hiện ở (a) trên Fig.9. Sau đó, điện thoại di động B có thể hiển thị hoạt ảnh trong đó tài khoản thứ nhất và mật khẩu đăng nhập của tài khoản thứ nhất tự động được điền trên giao diện đăng nhập tài khoản và nút nhấn "đăng nhập" 904 tự động được nhấp. Cuối cùng, điện thoại di động B có thể đăng nhập vào tài khoản thứ nhất, và hiển thị giao diện sau khi đăng nhập tới ứng dụng thứ nhất.

Theo kịch bản ứng dụng thứ hai, S804 có thể bao gồm S804a đến S804e. Ví dụ, như được thể hiện trên Fig.11A và Fig.11B, S804 được thể hiện trên Fig.7A-1 và Fig.7A-2 có thể bao gồm S804a đến S804e.

S804a: Điện thoại di động B gửi yêu cầu thu nhận mã xác thực tới máy chủ của ứng dụng thứ nhất đáp lại thao tác thu nhận mã xác thực.

Yêu cầu thu nhận mã xác thực bao gồm tài khoản thứ nhất "176****1860", và yêu cầu thu nhận mã xác thực được sử dụng để yêu cầu máy chủ gửi mã xác thực tới 176****1860.

Ví dụ, thao tác thu nhận mã xác thực có thể là thao tác nhấn được thực hiện bởi người dùng trên nút nhấn "thu nhận mã xác thực" 1004 được thể hiện trên Fig.10(b). Theo cách khác, thao tác thu nhận mã xác thực có thể là thao tác nhấn tự động được thực hiện bởi điện thoại di động B trên nút nhấn "thu nhận mã xác thực" được thể hiện trên Fig.10(b).

S804b: Máy chủ thu yêu cầu thu nhận mã xác thực, và gửi mã xác thực 2 tới điện

thoại di động A (nghĩa là, thiết bị sử dụng 180****7812).

Mã xác thực 2 là mã xác thực thứ hai. Mã xác thực 2 là mã mà điện thoại di động B yêu cầu máy chủ cấp phát tới tài khoản thứ nhất (nghĩa là, thiết bị sử dụng tài khoản thứ nhất).

S804c: Điện thoại di động A thu mã xác thực 2 từ máy chủ.

Đối với phương pháp trong đó điện thoại di động B gửi yêu cầu thu nhận mã xác thực tới máy chủ, phương pháp trong đó máy chủ gửi mã xác thực tới điện thoại di động A đáp lại yêu cầu thu nhận mã xác thực, và phương pháp trong đó điện thoại di động A thu mã xác thực 2, đề cập đến các cách thực hiện cụ thể trong công nghệ thông thường. Chi tiết không được mô tả ở đây theo phương án này của sáng chế.

S804d: Điện thoại di động A gửi mã xác thực 2 tới điện thoại di động B.

Điện thoại di động A có thể gửi mã xác thực 2 tới điện thoại di động B qua sự kết nối không dây giữa điện thoại di động A và điện thoại di động B. Theo một số phương án, bắt đầu từ thời điểm mà tại đó điện thoại di động A gửi thông tin đăng nhập của tài khoản thứ nhất tới điện thoại di động B, nếu điện thoại di động A thu mã xác thực 2 từ máy chủ nằm trong khoảng thời gian được thiết đặt trước 2, điện thoại di động A có thể gửi mã xác thực 2 tới điện thoại di động B. Nếu điện thoại di động A thu mã xác thực 2 từ máy chủ sau khoảng thời gian được thiết đặt trước 2, điện thoại di động A không gửi mã xác thực 2 tới điện thoại di động B. Trong trường hợp này, điện thoại di động A có thể loại bỏ mã xác thực 2.

S804e: Điện thoại di động B điền mã xác thực 2 trên giao diện đăng nhập tài khoản, và đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mã xác thực 2.

Ví dụ, như được thể hiện trên Fig.10(c), điện thoại di động B có thể thu mã xác thực 2 (ví dụ, 567568) từ điện thoại di động A, và điền mã xác thực 2 trên giao diện đăng nhập tài khoản. Đối với phương pháp trong đó điện thoại di động B điền mã xác thực 2 trên giao diện đăng nhập tài khoản, tham chiếu tới phương pháp trong đó điện thoại di động B điền mật khẩu đăng nhập của tài khoản thứ nhất trên giao diện đăng nhập tài khoản. Chi tiết không được mô tả lại ở đây theo phương án này của sáng chế.

Theo một số phương án, sau khi điện thoại di động B điền mã xác thực 2 trên giao diện đăng nhập tài khoản, điện thoại di động B có thể tự động đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mã xác thực 2, nói cách khác, điện thoại di động B có thể tự động kích hoạt nút nhấn "đăng nhập" 1005 được thể hiện trên Fig.10(c) để đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mã xác thực 2.

Theo một số phương án khác, sau khi điện thoại di động B điền mã xác thực 2 trên giao diện đăng nhập tài khoản, điện thoại di động B có thể đăng nhập, đáp lại thao tác nhấn được thực hiện bởi người dùng trên nút nhấn "đăng nhập" 1005 được thể hiện trên Fig.10(c), vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mã xác thực 2.

Tóm lại, thao tác 8 (nghĩa là, thao tác thứ tư) có thể bao gồm thao tác thu nhận mã xác thực nêu trên (ví dụ, thao tác nhấn được thực hiện trên nút nhấn "thu nhận mã xác thực" 1004 được thể hiện trên Fig.10(b)) và thao tác nhấn được thực hiện trên nút nhấn "đăng nhập" 1005 được thể hiện trên Fig.10(c).

S805: Điện thoại di động B loại bỏ thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất, và thủ tục chia sẻ tài khoản kết thúc.

Theo một số phương án, nếu điện thoại di động B không chạy ứng dụng thứ nhất, điện thoại di động B có thể thực hiện S805. Theo phương án này, điện thoại di động B không tự động đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất dựa vào thông tin đăng nhập của tài khoản thứ nhất.

Theo một số phương án khác, nếu điện thoại di động B không chạy ứng dụng thứ nhất, điện thoại di động B có thể xác định, dựa vào thông tin nhận dạng của ứng dụng thứ nhất, xem ứng dụng thứ nhất được cài đặt trong điện thoại di động B hay không. Nếu ứng dụng thứ nhất được cài đặt trong điện thoại di động B, điện thoại di động B có thể tự động bắt đầu ứng dụng thứ nhất, và sau đó thực hiện S803 và S804.

Theo phương pháp chia sẻ dữ liệu tài khoản được đề xuất theo phương án của sáng chế, điện thoại di động B có thể đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng thông tin đăng nhập của tài khoản thứ nhất mà được chia sẻ bởi điện

thoại di động A. Theo giải pháp này, thông tin đăng nhập của tài khoản thứ nhất có thể được chia sẻ giữa các thiết bị mà không phải triển thêm máy khách và máy chủ của ứng dụng, sao cho chi phí của việc thông tin đăng nhập giữa các thiết bị có thể được giảm.

Ngoài ra, điện thoại di động A chia sẻ thông tin đăng nhập của ứng dụng được lựa chọn bởi người dùng với điện thoại di động B, thay vì sao chép thông tin đăng nhập của tất cả các ứng dụng trong điện thoại di động A qua việc nhân bản. Nói cách khác, phương pháp theo phương án này của sáng chế có thể thực hiện việc đăng nhập được ủy quyền một lần giữa các thiết bị. Theo cách này, độ bảo mật thông ttrong thiết bị có thể được nâng cao.

Theo một số phương án, sau khi thu nhận thông tin đăng nhập của tài khoản thứ nhất, điện thoại di động B theo cách khác có thể lưu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất. Sau khi lưu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất, điện thoại di động B theo cách khác có thể thực hiện phương pháp các bước được thực hiện bởi điện thoại di động A trong thủ tục (1) đến thủ tục (3) nêu trên, để chia sẻ thông tin đăng nhập của tài khoản thứ nhất với thiết bị khác.

Ví dụ, sau khi điện thoại di động B thu nhận thông tin đăng nhập của tài khoản thứ nhất hoặc điện thoại di động B đăng nhập vào tài khoản thứ nhất nhờ sử dụng thông tin đăng nhập của tài khoản thứ nhất, điện thoại di động B có thể hiển thị giao diện thứ hai, để yêu cầu người dùng xác nhận xem có lưu thông tin đăng nhập của tài khoản thứ nhất hay không. Điện thoại di động B có thể lưu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất đáp lại thao tác thứ nhất được thực hiện bởi người dùng trên giao diện thứ hai. Điện thoại di động B có thể xóa thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất đáp lại thao tác thứ hai được thực hiện bởi người dùng trên giao diện thứ hai.

Theo một số phương án khác, để nâng cao bảo mật của thông tin đăng nhập của tài khoản thứ nhất và ngăn ngừa thông tin đăng nhập của tài khoản thứ nhất khỏi bị đánh cắp trong suốt thời gian chia sẻ, điện thoại di động A có thể thương lượng khóa phiên với điện thoại di động B. Điện thoại di động A có thể mã hóa, nhờ sử dụng khóa phiên, dữ liệu được chia sẻ với điện thoại di động B. Cụ thể là, S704 có thể được thay thế bằng S1201

đến S1203, và S801 có thể được thay thế bằng S1204 và S1205. Ví dụ, như được thể hiện trên Fig.12A và Fig.12B, S704 được thể hiện trên Fig.7A-1 và Fig.7A-2 có thể được thay thế bằng S1201 đến S1203, và S801 có thể được thay thế bằng S1204 và S1205.

S1201: Điện thoại di động A thương lượng khóa phiên với điện thoại di động B đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất.

Điện thoại di động A có thể thương lượng khóa phiên với điện thoại di động B qua truyền thông kết nối không dây giữa điện thoại di động A và điện thoại di động B.

S1202: Điện thoại di động A mã hóa thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất nhờ sử dụng khóa phiên, để thu nhận dữ liệu được mã hóa.

Ví dụ, điện thoại di động A có thể mã hóa thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất nhờ sử dụng thuật toán bất kỳ chẳng hạn như thuật toán mã hóa chuẩn mã hóa nâng cao (Advanced Encryption Standard, viết tắt là AES), thuật toán mã hóa Ron Rivest, Adi Shamir, Leonard Adleman (Ron Rivest, Adi Shamir, Leonard Adleman, viết tắt là RSA), hoặc thuật toán mã hóa thích hợp sơ đồ mã hóa đường cong hình elip (elliptic curve integrated encryption scheme, viết tắt là ECIES) và nhờ sử dụng khóa phiên, để thu nhận dữ liệu được mã hóa.

S1203: Điện thoại di động A gửi dữ liệu được mã hóa tới điện thoại di động B.

S1204: Điện thoại di động B thu dữ liệu được mã hóa từ điện thoại di động A.

Dữ liệu được mã hóa có thể được truyền giữa điện thoại di động A và điện thoại di động B qua sự kết nối không dây giữa điện thoại di động A và điện thoại di động B.

S1205: Điện thoại di động B giải mã dữ liệu được mã hóa nhờ sử dụng khóa phiên, để thu nhận thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất.

Cần lưu ý rằng, đối với phương pháp trong đó điện thoại di động B giải mã dữ liệu được mã hóa nhờ sử dụng khóa phiên, tham chiếu tới phương pháp giải mã dữ liệu được mã hóa theo công nghệ thông thường. Chi tiết không được mô tả ở đây theo phương án này của sáng chế.

Theo một số phương án, mã xác thực được gửi bởi điện thoại di động A tới điện thoại di động B ở S804d có thể cũng là mã xác thực được mã hóa nhờ sử dụng khóa phiên. Sau khi thu mã xác thực được mã hóa, điện thoại di động B có thể giải mã mã xác thực nhờ sử dụng khóa phiên.

Có thể hiểu rằng, bởi vì khóa phiên là khóa được thương lượng bởi điện thoại di động A và điện thoại di động B, chỉ điện thoại di động A và điện thoại di động B biết khóa phiên. Thiết bị khác không học khóa phiên, và do đó không thể giải mã dữ liệu được mã hóa và không thể thu nhận thông tin đăng nhập của tài khoản thứ nhất. Điều này có thể nâng cao độ bảo mật thông tin của việc chia sẻ thông tin đăng nhập giữa các thiết bị.

Có thể hiểu rằng, để thực hiện các chức năng nêu trên, thiết bị điện tử (ví dụ, điện thoại di động) nêu trên bao gồm các cấu trúc phần cứng và/hoặc các môđun phần mềm tương ứng để thực hiện các chức năng. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật tương ứng có thể là dễ dàng nhận thấy rằng, theo sự kết hợp với các ví dụ được mô tả theo các phương án được bộc lộ trong sáng chế này, các bộ phận và các bước thuật toán có thể được thực hiện ở dạng phần cứng hoặc sự kết hợp của phần cứng và phần mềm máy tính theo các phương án của sáng chế. Việc xem các chức năng được thực hiện bởi phần cứng hay phần cứng dẫn động phần mềm máy tính tùy thuộc vào các ứng dụng và các ràng buộc thiết kế cụ thể của các giải pháp kỹ thuật. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật tương ứng có thể sử dụng các phương pháp khác nhau để thực hiện các chức năng được mô tả đối với mỗi ứng dụng cụ thể, nhưng sẽ không được coi là việc thực hiện vượt quá phạm vi của các phương án của sáng chế.

Theo các phương án của sáng chế, thiết bị điện tử (ví dụ, điện thoại di động) nêu trên có thể được chia thành các môđun chức năng dựa vào các ví dụ phương pháp nêu trên. Ví dụ, mỗi môđun chức năng có thể được thu nhận qua việc phân chia dựa vào mỗi chức năng tương ứng, hoặc hai hoặc nhiều hơn hai chức năng có thể được tích hợp trong một môđun xử lý. Môđun được tích hợp có thể được thực hiện ở dạng phần cứng, hoặc có thể được thực hiện ở dạng môđun chức năng phần mềm. Cần lưu ý rằng, theo các phương án của sáng chế, việc chia môđun là ví dụ, và chỉ là sự chia chức năng lôgic. Trong suốt thời gian thực hiện thực tế, cách chia khác có thể được sử dụng.

Trên Fig.13, (a) là hình vẽ giản lược của cấu trúc khả thi của thiết bị thứ nhất (ví

dụ, điện thoại di động A) theo phương án nêu trên. Trên Fig.13, (b) là hình vẽ giản lược của cấu trúc khả thi của thiết bị thứ hai (ví dụ, điện thoại di động B) theo phương án nêu trên. Như được thể hiện ở (a) trên Fig.13, thiết bị thứ nhất 1310 có thể bao gồm môđun lưu trữ tài khoản và mật khẩu 1311, môđun xử lý trạng thái chia sẻ 1312, môđun kết nối thiết bị 1313, và môđun gửi 1314. Như được thể hiện ở (b) trên Fig.13, thiết bị thứ hai 1320 có thể bao gồm môđun kết nối thiết bị 1321, môđun thu 1322, môđun điền 1323, và môđun lưu trữ tài khoản và mật khẩu 1324.

Môđun lưu trữ tài khoản và mật khẩu 1311 được tạo cấu hình để lưu trữ tài khoản mà được đăng nhập trong ứng dụng được cài đặt trong thiết bị thứ nhất 1310 và mật khẩu đăng nhập của tài khoản. Ví dụ, môđun lưu trữ tài khoản và mật khẩu 1311 được tạo cấu hình để hỗ trợ thiết bị thứ nhất 1310 trong việc thực hiện S304 trong trường hợp nêu trên, và/hoặc được tạo cấu hình để thực hiện quy trình xử lý khác của công nghệ được mô tả trong sáng chế này.

Môđun xử lý trạng thái chia sẻ 1312 được tạo cấu hình để kích hoạt thiết bị thứ nhất 1310 để chia sẻ thông tin đăng nhập của tài khoản thứ nhất với thiết bị khác. Cụ thể là, môđun xử lý trạng thái chia sẻ 1312 có thể kích hoạt thiết bị thứ nhất 1310 để thiết lập sự kết nối không dây tới thiết bị khác, và chia sẻ thông tin đăng nhập của tài khoản thứ nhất với thiết bị khác qua sự kết nối không dây. Ví dụ, môđun xử lý trạng thái chia sẻ 1312 được tạo cấu hình để hỗ trợ thiết bị thứ nhất 1310 trong việc thực hiện S701, S702, và S703 trong trường hợp nêu trên, và/hoặc được tạo cấu hình để thực hiện quy trình xử lý khác của công nghệ được mô tả trong sáng chế này.

Môđun kết nối thiết bị 1313 được tạo cấu hình để hỗ trợ thiết bị thứ nhất 1310 trong việc thiết lập sự kết nối không dây tới thiết bị khác. Ví dụ, môđun kết nối thiết bị 1313 có thể tương tác với môđun kết nối thiết bị 1321 của thiết bị thứ hai 1320, sao cho thiết bị thứ nhất 1310 thiết lập sự kết nối không dây tới thiết bị thứ hai 1320.

Môđun gửi 1314 được tạo cấu hình để gửi thông tin đăng nhập của tài khoản thứ nhất tới thiết bị khác. Ví dụ, môđun gửi 1314 được tạo cấu hình để hỗ trợ thiết bị thứ nhất 1310 trong việc thực hiện S704 trong trường hợp nêu trên, và/hoặc được tạo cấu hình để thực hiện quy trình xử lý khác của công nghệ được mô tả trong sáng chế này.

Một cách tùy chọn, thiết bị thứ nhất 1310 có thể còn bao gồm môđun đăng nhập

tài khoản. Ví dụ, môđun đăng nhập tài khoản được tạo cấu hình để hỗ trợ thiết bị thứ nhất 1310 trong việc thực hiện S301 và S302, và/hoặc được tạo cấu hình để thực hiện quy trình xử lý khác của công nghệ được mô tả trong sáng chế này.

Môđun kết nối thiết bị 1321 được tạo cấu hình để hỗ trợ thiết bị thứ hai 1320 trong việc thiết lập sự kết nối không dây tới thiết bị khác. Ví dụ, môđun kết nối thiết bị 1321 có thể tương tác với môđun kết nối thiết bị 1313 của thiết bị thứ nhất 1310, sao cho thiết bị thứ hai 1320 thiết lập sự kết nối không dây tới thiết bị thứ nhất 1310.

Môđun thu 1322 được tạo cấu hình để thu thông tin đăng nhập của tài khoản thứ nhất từ thiết bị thứ nhất 1310. Ví dụ, môđun thu 1322 được tạo cấu hình để hỗ trợ thiết bị thứ hai 1320 trong việc thực hiện S801 trong trường hợp nêu trên, và/hoặc được tạo cấu hình để thực hiện quy trình xử lý khác của công nghệ được mô tả trong sáng chế này.

Môđun điền 1323 được tạo cấu hình để điền, trên giao diện đăng nhập tài khoản, thông tin đăng nhập của tài khoản thứ nhất mà được thu bởi môđun thu 1322. Ví dụ, môđun điền 1323 được tạo cấu hình để hỗ trợ thiết bị thứ hai 1320 trong việc thực hiện S803 và S804e trong việc điền mã xác thực trong trường hợp nêu trên, và/hoặc được tạo cấu hình để thực hiện quy trình xử lý khác của công nghệ được mô tả trong sáng chế này.

Môđun lưu trữ tài khoản và mật khẩu 1324 được tạo cấu hình để lưu trữ tài khoản mà được đăng nhập trong ứng dụng được cài đặt trong thiết bị thứ hai 1320 và mật khẩu đăng nhập của tài khoản. Ví dụ, môđun lưu trữ tài khoản và mật khẩu 1324 được tạo cấu hình để hỗ trợ thiết bị thứ hai 1320 trong việc lưu trữ thông tin đăng nhập của tài khoản thứ nhất từ thiết bị thứ nhất 1310.

Một cách tùy chọn, thiết bị thứ hai 1320 có thể còn bao gồm môđun đăng nhập tài khoản. Ví dụ, môđun đăng nhập tài khoản được tạo cấu hình để hỗ trợ thiết bị thứ hai 1320 trong việc thực hiện S804, và/hoặc được tạo cấu hình để thực hiện quy trình xử lý khác của công nghệ được mô tả trong sáng chế này.

Khi bộ phận được tích hợp được sử dụng, trong thiết bị thứ nhất 1310, chức năng của môđun xử lý trạng thái chia sẻ 1312 có thể được tích hợp trong môđun xử lý cho việc thực hiện, các chức năng của môđun kết nối thiết bị 1313 và môđun gửi 1314 có thể được tích hợp trong môđun truyền thông cho việc thực hiện, và chức năng của môđun lưu trữ tài

khoản và mật khẩu 1311 có thể được tích hợp trong môđun lưu trữ cho việc thực hiện. Trong thiết bị thứ hai 1320, các chức năng của môđun kết nối thiết bị 1321 và môđun thu 1322 có thể được tích hợp trong môđun truyền thông cho việc thực hiện, chức năng của môđun điền 1323 có thể được tích hợp trong môđun xử lý cho việc thực hiện, và chức năng của môđun lưu trữ tài khoản và mật khẩu 1324 có thể được tích hợp trong môđun lưu trữ cho việc thực hiện. Tất nhiên, các môđun bộ phận của mỗi của thiết bị thứ nhất 1310 và thiết bị thứ hai 1320 bao gồm nhưng không giới hạn ở môđun xử lý, môđun lưu trữ, và môđun truyền thông không dây. Ví dụ, thiết bị thứ nhất 1310 và thiết bị thứ hai 1320 đều có thể còn bao gồm môđun hiển thị.

Ví dụ, môđun xử lý có thể là một hoặc nhiều bộ xử lý (ví dụ, bộ xử lý 210 được thể hiện trên Fig.2), và môđun truyền thông bao gồm môđun truyền thông không dây (ví dụ, môđun truyền thông không dây 260 được thể hiện trên Fig.2). Môđun truyền thông không dây có thể được gọi là giao diện truyền thông. Môđun lưu trữ có thể là bộ nhớ (ví dụ, bộ nhớ trong 221 được thể hiện trên Fig.2). Môđun hiển thị có thể là màn hình (ví dụ, màn hình 294 được thể hiện trên Fig.2). Một hoặc nhiều bộ xử lý, bộ nhớ, màn hình, và tương tự có thể được kết nối với nhau, ví dụ, qua bus. Bộ nhớ có thể được tạo cấu hình để lưu trữ mã chương trình máy tính. Mã chương trình máy tính bao gồm các lệnh máy tính. Khi bộ xử lý thực hiện các lệnh máy tính, thiết bị điện tử có thể thực hiện các chức năng hoặc các bước được thực hiện bởi điện thoại di động theo các phương án về phương pháp nêu trên. Đối với cấu trúc của thiết bị điện tử, tham chiếu tới cấu trúc của thiết bị điện tử 200 được thể hiện trên Fig.2.

Phương án của sáng chế còn đề xuất hệ thống chip. Như được thể hiện trên Fig.14, hệ thống chip bao gồm ít nhất một bộ xử lý 1401 và ít nhất một mạch giao diện 1402. Bộ xử lý 1401 và mạch giao diện 1402 có thể được kết nối với nhau qua đường dây. Ví dụ, mạch giao diện 1402 có thể được tạo cấu hình để thu tín hiệu từ máy khác (ví dụ, bộ nhớ của thiết bị điện tử). Đối với ví dụ khác, mạch giao diện 1402 có thể được tạo cấu hình để gửi tín hiệu tới máy khác (ví dụ, bộ xử lý 1401). Ví dụ, mạch giao diện 1402 có thể đọc các lệnh được lưu trữ trong bộ nhớ, và gửi các lệnh tới bộ xử lý 1401. Khi các lệnh được thực hiện bởi bộ xử lý 1401, thiết bị điện tử (ví dụ, thiết bị điện tử 200 được thể hiện trên Fig.2) có thể được phép thực hiện các bước theo các phương án nêu trên. Tất nhiên,

hệ thống chip có thể còn bao gồm thiết bị rời rạc khác. Điều này không giới hạn cụ thể ở phương án này của sáng chế.

Phương án của sáng chế còn đề xuất phương tiện lưu trữ máy tính. Phương tiện lưu trữ máy tính bao gồm các lệnh máy tính. Khi các lệnh máy tính được chạy trên thiết bị điện tử (ví dụ, thiết bị điện tử 200 được thể hiện trên Fig.2) nêu trên, thiết bị điện tử được phép thực hiện các chức năng hoặc các bước được thực hiện bởi điện thoại di động theo các phương án về phương pháp nêu trên.

Phương án của sáng chế còn đề xuất sản phẩm chương trình máy tính. Khi sản phẩm chương trình máy tính chạy trên máy tính, máy tính được phép thực hiện các chức năng hoặc các bước được thực hiện bởi điện thoại di động theo các phương án về phương pháp nêu trên.

Dựa vào các phần mô tả về các cách thực hiện nêu trên, người có hiểu biết trung bình trong lĩnh vực kỹ thuật tương ứng có thể hiểu rõ rằng, nhằm đơn giản và ngắn gọn phần mô tả, việc chia thành các môđun chức năng nêu trên chỉ được sử dụng làm ví dụ cho phần mô tả. Trong thời gian ứng dụng thực tế, các chức năng nêu trên có thể được cấp phát tới các môđun chức năng khác nhau theo yêu cầu, nói cách khác, cấu trúc bên trong của máy được chia thành các môđun chức năng khác nhau, để thực hiện tất cả hoặc một số trong số các chức năng được nêu trên.

Theo một vài phương án được đề xuất trong sáng chế, cần hiểu rằng các máy và các phương pháp được bộc lộ có thể được thực hiện theo cách khác. Ví dụ, các phương án về máy nêu trên chỉ là các ví dụ. Ví dụ, việc chia thành các môđun hoặc các bộ phận chỉ là sự chia chức năng lôgic và có thể là sự chia khác trong thời gian thực hiện thực tế. Ví dụ, nhiều bộ phận hoặc thành phần có thể được kết hợp hoặc được tích hợp trong máy khác, hoặc một số đặc điểm có thể được bỏ qua hoặc không được thực hiện. Ngoài ra, các sự ghép nối lẫn nhau hoặc các sự ghép nối trực tiếp hoặc các sự kết nối truyền thông được hiển thị hoặc được thảo luận được thực hiện qua một số giao diện. Các sự ghép nối gián tiếp hoặc các sự kết nối truyền thông giữa các máy hoặc các bộ phận có thể được thực hiện ở dạng điện, dạng cơ, hoặc dạng khác.

Các bộ phận được mô tả như các phần tách biệt có thể hoặc có thể không tách biệt về mặt vật lý, và các phần được hiển thị như các bộ phận có thể là một hoặc nhiều bộ

phận vật lý, nói cách khác, có thể được nằm trong một vị trí, hoặc có thể được phân bố ở nhiều vị trí khác nhau. Một số hoặc tất cả trong số các bộ phận có thể được lựa chọn theo các yêu cầu thực tế để đạt được các mục đích của các giải pháp của các phương án.

Ngoài ra, các bộ phận chức năng theo các phương án của sáng chế có thể được tích hợp trong một bộ phận xử lý, hoặc mỗi trong số các bộ phận có thể chỉ tồn tại ở dạng vật lý, hoặc hai hoặc nhiều hơn hai bộ phận được tích hợp trong một bộ phận. Bộ phận được tích hợp có thể được thực hiện ở dạng phần cứng, hoặc có thể được thực hiện ở dạng bộ phận chức năng phần mềm.

Khi bộ phận được tích hợp được thực hiện ở dạng bộ phận chức năng phần mềm và được bán hoặc được sử dụng dưới dạng sản phẩm độc lập, bộ phận được tích hợp có thể được lưu trữ trong phương tiện lưu trữ có thể đọc được. Dựa vào cách hiểu như vậy, các giải pháp kỹ thuật của các phương án của sáng chế về bản chất, hoặc phần góp phần vào công nghệ thông thường, hoặc tất cả hoặc một số trong số các giải pháp kỹ thuật có thể được thực hiện ở dạng sản phẩm phần mềm. Sản phẩm phần mềm được lưu trữ trong phương tiện lưu trữ, và bao gồm một số lệnh để lệnh cho thiết bị (mà có thể là máy vi tính chip đơn, chip, hoặc tương tự) hoặc bộ xử lý (bộ xử lý) thực hiện tất cả hoặc một số trong số các bước của các phương pháp được mô tả theo các phương án của sáng chế. Phương tiện lưu trữ nêu trên bao gồm phương tiện bất kỳ mà có thể lưu trữ mã chương trình, chẳng hạn như ổ đĩa tia chớp USB, đĩa cứng có thể tháo được, bộ nhớ chỉ đọc (read-only memory, viết tắt là ROM), bộ nhớ truy cập ngẫu nhiên (random access memory, viết tắt là RAM), đĩa từ, hoặc đĩa quang.

Các phần mô tả nêu trên chỉ là các cách thực hiện cụ thể của sáng chế, mà không nhằm giới hạn phạm vi bảo hộ của sáng chế. Bất kỳ biến thể hoặc sự thay thế nào nằm trong phạm vi kỹ thuật được bộc lộ trong sáng chế sẽ nằm trong phạm vi bảo hộ của sáng chế. Do đó, phạm vi bảo hộ của sáng chế sẽ thuộc phạm vi bảo hộ của các điểm yêu cầu bảo hộ.

YÊU CẦU BẢO HỘ

1. Phương pháp chia sẻ dữ liệu tài khoản, được áp dụng cho hệ thống bao gồm thiết bị điện tử thứ nhất và thiết bị điện tử thứ hai, trong đó phương pháp này bao gồm các bước:

bắt đầu, bởi thiết bị điện tử thứ hai, ứng dụng thứ nhất, và hiển thị giao diện ứng dụng thứ nhất, trong đó giao diện ứng dụng thứ nhất bao gồm hộp đầu vào tài khoản, hộp đầu vào mã xác thực, và sự điều khiển thu nhận mã xác thực;

thu, bởi thiết bị điện tử thứ hai, thao tác thứ nhất, trong đó thao tác thứ nhất được sử dụng để nhập thông tin tài khoản trong hộp đầu vào tài khoản; và;

thu, bởi thiết bị điện tử thứ hai, thao tác thứ hai dùng cho sự điều khiển thu nhận mã xác thực; và;

thu nhận, bởi thiết bị điện tử thứ nhất, mã xác thực đáp lại thao tác thứ hai; và;

sau khi thiết bị điện tử thứ nhất thu nhận mã xác thực, thu, bởi thiết bị điện tử thứ hai, mã xác thực, và điền mã xác thực vào hộp đầu vào mã xác thực; và;

sau khi điền mã xác thực vào hộp đầu vào mã xác thực, đăng nhập, bởi thiết bị điện tử thứ hai, vào ứng dụng thứ nhất nhờ sử dụng thông tin tài khoản và mã xác thực.

2. Phương pháp theo điểm 1, trong đó bước thu nhận, bởi thiết bị điện tử thứ nhất, mã xác thực đáp lại thao tác thứ hai bao gồm:

gửi, bởi thiết bị điện tử thứ hai, yêu cầu thu nhận mã xác thực tới máy chủ của ứng dụng thứ nhất đáp lại thao tác thứ hai; và;

gửi, bởi máy chủ, mã xác thực tới thiết bị điện tử thứ nhất theo yêu cầu thu nhận mã xác thực; và;

thu, bởi thiết bị điện tử thứ nhất, mã xác thực được gửi bởi máy chủ.

3. Phương pháp theo điểm 1, trong đó sau khi thu nhận mã xác thực, việc gửi, bởi thiết bị điện tử thứ nhất, mã xác thực tới thiết bị điện tử thứ hai bao gồm:

khi thiết bị điện tử thứ nhất thu mã xác thực nằm trong khoảng thời gian được thiết đặt trước, gửi, bởi thiết bị điện tử thứ nhất, mã xác thực tới thiết bị điện tử thứ hai; và;

khi thiết bị điện tử thứ nhất thu mã xác thực sau khoảng thời gian được thiết đặt trước,

bỏ qua bước gửi, bởi thiết bị điện tử thứ nhất, mã xác thực tới thiết bị điện tử thứ hai.

4. Phương pháp theo điểm 1, trong đó giao diện ứng dụng thứ nhất còn bao gồm sự điều khiển đăng nhập; và; sau khi điền mã xác thực vào hộp đầu vào mã xác thực, bước đăng nhập, bởi thiết bị điện tử thứ hai, vào ứng dụng thứ nhất nhờ sử dụng thông tin tài khoản và mã xác thực bao gồm:

thu, bởi thiết bị điện tử thứ hai, thao tác thứ ba dùng cho sự điều khiển đăng nhập; và;

đáp lại thao tác thứ ba, đăng nhập, bởi thiết bị điện tử thứ hai, vào ứng dụng thứ nhất nhờ sử dụng thông tin tài khoản và mã xác thực.

5. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 4, trong đó thông tin tài khoản là số điện thoại hoặc địa chỉ thư điện tử của thiết bị điện tử thứ nhất.

6. Phương pháp chia sẻ dữ liệu tài khoản, trong đó phương pháp này bao gồm các bước:

bắt đầu, bởi thiết bị điện tử thứ hai, ứng dụng thứ nhất, và hiển thị giao diện ứng dụng thứ nhất, trong đó giao diện ứng dụng thứ nhất bao gồm hộp đầu vào tài khoản, hộp đầu vào mã xác thực, và sự điều khiển thu nhận mã xác thực;

thu, bởi thiết bị điện tử thứ hai, thao tác thứ nhất, trong đó thao tác thứ nhất được sử dụng để nhập thông tin tài khoản trong hộp đầu vào tài khoản; và;

thu, bởi thiết bị điện tử thứ hai, thao tác thứ hai dùng cho sự điều khiển thu nhận mã xác thực; và;

đáp lại thao tác thứ hai, thu, bởi thiết bị điện tử thứ hai, mã xác thực, và điền mã xác thực vào hộp đầu vào mã xác thực; và;

sau khi điền mã xác thực vào hộp đầu vào mã xác thực, đăng nhập, bởi thiết bị điện tử thứ hai, vào ứng dụng thứ nhất nhờ sử dụng thông tin tài khoản và mã xác thực.

7. Phương pháp theo điểm 6, trong đó bước thu, bởi thiết bị điện tử thứ hai đáp lại thao tác thứ hai, mã xác thực được gửi bởi thiết bị điện tử thứ nhất bao gồm:

gửi, bởi thiết bị điện tử thứ hai, yêu cầu thu nhận mã xác thực tới máy chủ của ứng dụng thứ nhất đáp lại thao tác thứ hai; và; máy chủ được tạo cấu hình để gửi mã xác thực tới thiết bị điện tử thứ nhất theo yêu cầu thu nhận mã xác thực; và; thiết bị điện tử thứ nhất

được tạo cấu hình để thu mã xác thực được gửi bởi máy chủ, và gửi mã xác thực tới thiết bị điện tử thứ hai; và;

thu, bởi thiết bị điện tử thứ hai, mã xác thực được gửi bởi thiết bị điện tử thứ nhất.

8. Phương pháp theo điểm 6, trong đó bước thu, bởi thiết bị điện tử thứ hai, mã xác thực được gửi bởi thiết bị điện tử thứ nhất bao gồm:

khi thiết bị điện tử thứ nhất thu mã xác thực nằm trong khoảng thời gian được thiết đặt trước, thu, bởi thiết bị điện tử thứ hai, mã xác thực được gửi bởi thiết bị điện tử thứ nhất; và;

khi thiết bị điện tử thứ nhất thu mã xác thực sau khoảng thời gian được thiết đặt trước, thu, bởi thiết bị điện tử thứ hai, mã xác thực được gửi bởi thiết bị điện tử thứ nhất.

9. Phương pháp theo điểm 6, trong đó giao diện ứng dụng thứ nhất còn bao gồm sự điều khiển đăng nhập; và; sau khi điền mã xác thực vào hộp đầu vào mã xác thực, bước đăng nhập, bởi thiết bị điện tử thứ hai, vào ứng dụng thứ nhất nhờ sử dụng thông tin tài khoản và mã xác thực bao gồm:

thu, bởi thiết bị điện tử thứ hai, thao tác thứ ba dùng cho sự điều khiển đăng nhập; và;

đáp lại thao tác thứ ba, đăng nhập, bởi thiết bị điện tử thứ hai, vào ứng dụng thứ nhất nhờ sử dụng thông tin tài khoản và mã xác thực.

10. Phương pháp theo điểm bất kỳ trong số các điểm từ 6 đến 9, trong đó thông tin tài khoản là số điện thoại hoặc địa chỉ thư điện tử của thiết bị điện tử thứ nhất.

11. Thiết bị điện tử, trong đó thiết bị điện tử là thiết bị điện tử thứ hai, và thiết bị điện tử thứ hai bao gồm môđun truyền thông không dây, bộ nhớ, màn hình hiển thị, và một hoặc nhiều bộ xử lý, trong đó; môđun truyền thông không dây, bộ nhớ, và màn hình hiển thị được ghép nối với bộ xử lý; và;

bộ nhớ được tạo cấu hình để lưu trữ mã chương trình máy tính, và mã chương trình máy tính bao gồm lệnh máy tính; và; khi lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị điện tử thứ hai thực hiện các thao tác sau:

bắt đầu ứng dụng thứ nhất, và hiển thị giao diện ứng dụng thứ nhất, trong đó giao diện ứng dụng thứ nhất bao gồm hộp đầu vào tài khoản, hộp đầu vào mã xác thực, và sự điều

khiển thu nhận mã xác thực;

thu thao tác thứ nhất, trong đó thao tác thứ nhất được sử dụng để nhập thông tin tài khoản trong hộp đầu vào tài khoản; và;

thu thao tác thứ hai dùng cho sự điều khiển thu nhận mã xác thực; và;

đáp lại thao tác thứ hai, thu mã xác thực, và điền mã xác thực vào hộp đầu vào mã xác thực; và;

sau khi điền mã xác thực vào hộp đầu vào mã xác thực, đăng nhập vào ứng dụng thứ nhất nhờ sử dụng thông tin tài khoản và mã xác thực.

12. Thiết bị điện tử theo điểm 11, trong đó khi lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị điện tử thứ hai còn thực hiện các bước sau:

gửi yêu cầu thu nhận mã xác thực tới máy chủ của ứng dụng thứ nhất đáp lại thao tác thứ hai; và; máy chủ được tạo cấu hình để gửi mã xác thực tới thiết bị điện tử thứ nhất theo yêu cầu thu nhận mã xác thực; và; thiết bị điện tử thứ nhất được tạo cấu hình để thu mã xác thực được gửi bởi máy chủ, và gửi mã xác thực tới thiết bị điện tử thứ hai; và;

thu mã xác thực được gửi bởi thiết bị điện tử thứ nhất.

13. Thiết bị điện tử theo điểm 11, trong đó khi lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị điện tử thứ hai còn thực hiện các bước sau:

khi thiết bị điện tử thứ nhất thu mã xác thực nằm trong khoảng thời gian được thiết đặt trước, thu mã xác thực được gửi bởi thiết bị điện tử thứ nhất; và;

khi thiết bị điện tử thứ nhất thu mã xác thực sau khoảng thời gian được thiết đặt trước, thu mã xác thực được gửi bởi thiết bị điện tử thứ nhất.

14. Thiết bị điện tử theo điểm 11, trong đó giao diện ứng dụng thứ nhất còn bao gồm sự điều khiển đăng nhập; và; khi lệnh máy tính được thực hiện bởi bộ xử lý, thiết bị điện tử thứ hai còn thực hiện các bước sau:

thu thao tác thứ ba dùng cho sự điều khiển đăng nhập; và;

đáp lại thao tác thứ ba, đăng nhập vào ứng dụng thứ nhất nhờ sử dụng thông tin tài khoản và mã xác thực.

15. Thiết bị điện tử theo điểm bất kỳ trong số các điểm từ 11 đến 14, trong đó thông tin tài khoản là số điện thoại hoặc địa chỉ thư điện tử của thiết bị điện tử thứ nhất.

16. Hệ thống chip, trong đó hệ thống chip được áp dụng cho thiết bị điện tử bao gồm môđun truyền thông không dây, bộ nhớ, và màn hình hiển thị, trong đó; hệ thống chip bao gồm một hoặc nhiều mạch giao diện và một hoặc nhiều bộ xử lý; mạch giao diện và bộ xử lý được liên kết nhờ sử dụng đường dây; và; mạch giao diện được tạo cấu hình để thu tín hiệu từ bộ nhớ, và gửi tín hiệu tới bộ xử lý, trong đó tín hiệu bao gồm lệnh máy tính được lưu trữ trong bộ nhớ; và; khi bộ xử lý thực hiện lệnh máy tính, thiết bị điện tử thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 6 đến 10.

17. Phương tiện lưu trữ đọc được bởi máy tính, bao gồm lệnh máy tính, trong đó khi lệnh máy tính chạy trên thiết bị điện tử, thiết bị điện tử được phép thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 6 đến 10.

1/27

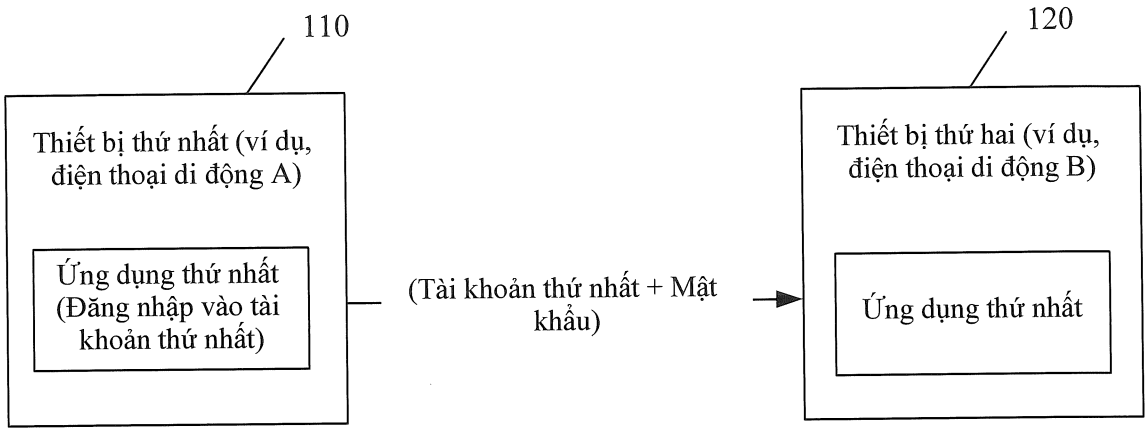
110
Thiết bị thứ nhất (ví dụ, điện thoại di động A)
Ứng dụng thứ nhất (Đăng nhập vào tài khoản thứ nhất)
(Tài khoản thứ nhất + Mật khẩu)
120
Thiết bị thứ hai (ví dụ, điện thoại di động B)
Ứng dụng thứ nhất

FIG. 1

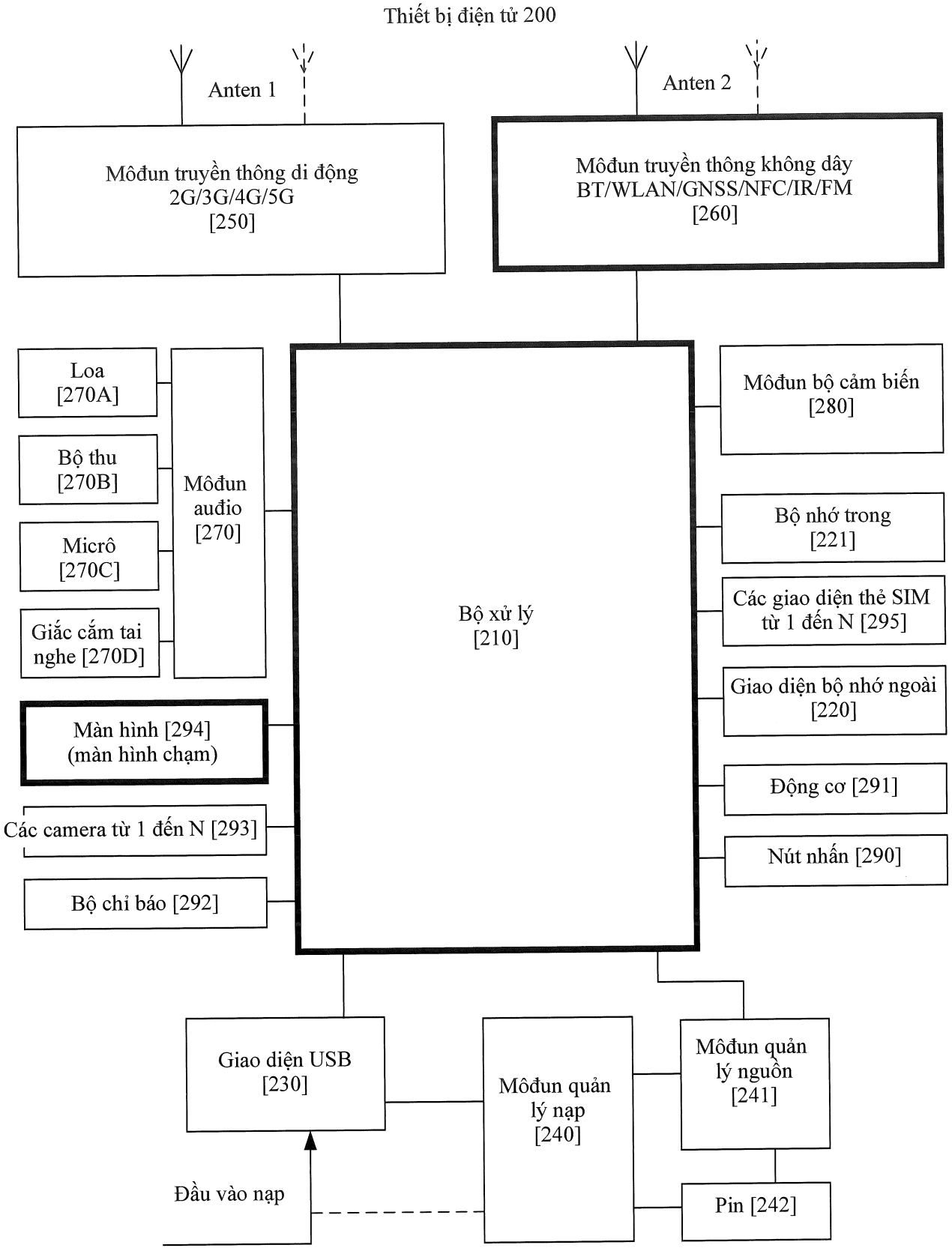
Thiết bị điện tử 200
Anten 1
Anten 2
Môđun truyền thông di động 2G/3G/4G/5G [250]
Môđun truyền thông không dây BT/WLAN/GNSS/NFC/IR/FM [260]
Loa [270A]
Bộ thu [270B]
Micrô [270C]
Giắc cắm tai nghe [270D]
Môđun auđio [270]
Màn hình [294] (màn hình chạm)
Các camera từ 1 đến N [293]
Bộ chỉ báo [292]
Bộ xử lý [210]
Môđun bộ cảm biến [280]
Bộ nhớ trong [221]
Các giao diện thẻ SIM từ 1 đến N [295]
Giao diện bộ nhớ ngoài [220]
Động cơ [291]
Nút nhấn [290]
Giao diện USB [230]
Môđun quản lý nạp [240]
Môđun quản lý nguồn [241]
Đầu vào nạp
Pin [242]

FIG. 2

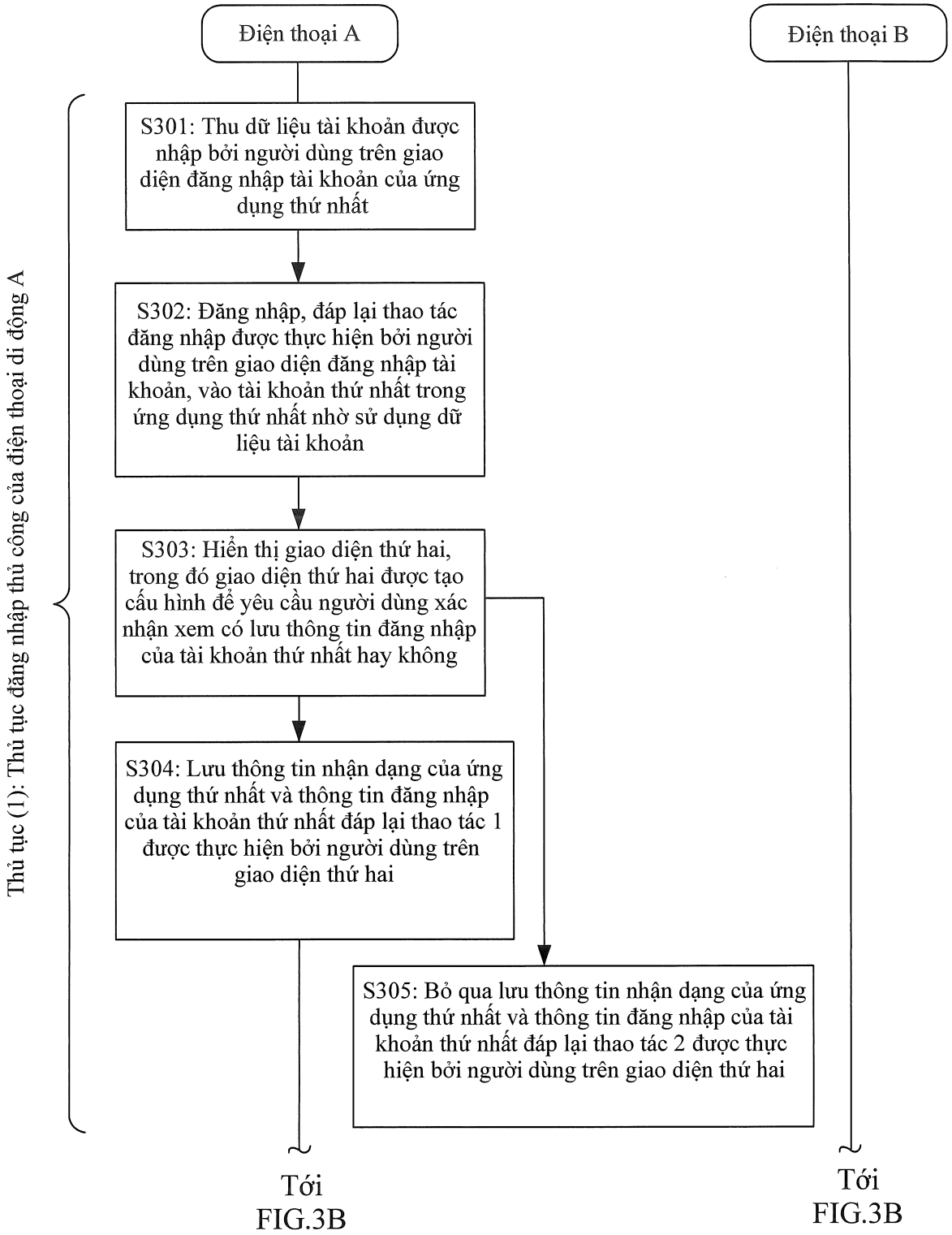
Điện thoại A
Điện thoại B
Thủ tục (1): Thủ tục đăng nhập thủ công của điện thoại di động A
S301: Thu dữ liệu tài khoản được nhập bởi người dùng trên giao diện đăng nhập tài khoản của ứng dụng thứ nhất
S302: Đăng nhập, đáp lại thao tác đăng nhập được thực hiện bởi người dùng trên giao diện đăng nhập tài khoản, vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng dữ liệu tài khoản
S303: Hiển thị giao diện thứ hai, trong đó giao diện thứ hai được tạo cấu hình để yêu cầu người dùng xác nhận xem có lưu thông tin đăng nhập của tài khoản thứ nhất hay không
S304: Lưu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất đáp lại thao tác 1 được thực hiện bởi người dùng trên giao diện thứ hai
S305: Bỏ qua lưu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất đáp lại thao tác 2 được thực hiện bởi người dùng trên giao diện thứ hai
Tới FIG.3B
Tới FIG.3B

FIG. 3A

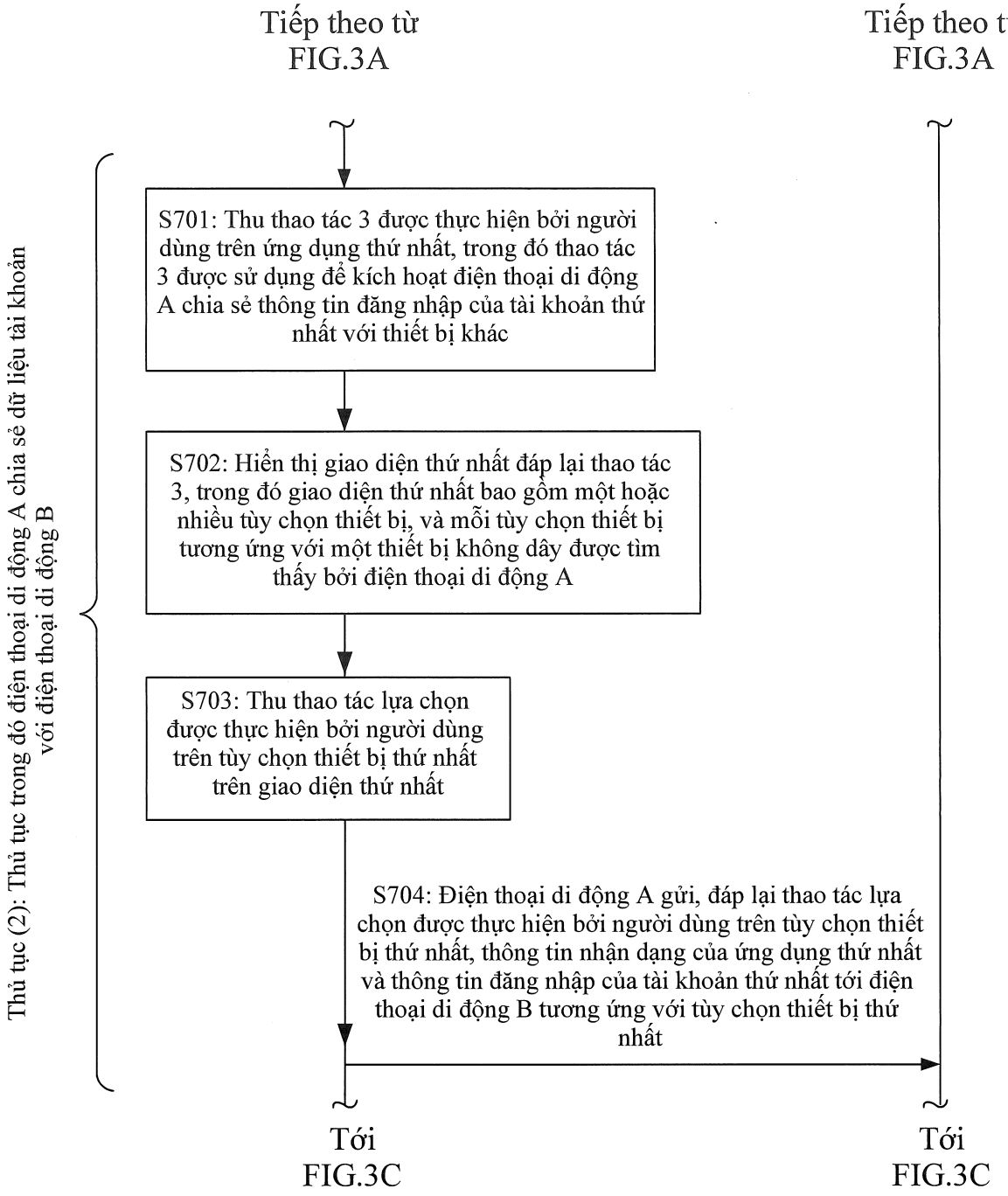
Tiếp theo từ FIG.3A
Tiếp theo từ FIG.3A
Thủ tục (2): Thủ tục trong đó điện thoại di động A chia sẻ dữ liệu tài khoản với điện thoại di động B
S701: Thu thao tác 3 được thực hiện bởi người dùng trên ứng dụng thứ nhất, trong đó thao tác 3 được sử dụng để kích hoạt điện thoại di động A chia sẻ thông tin đăng nhập của tài khoản thứ nhất với thiết bị khác
S702: Hiển thị giao diện thứ nhất đáp lại thao tác 3, trong đó giao diện thứ nhất bao gồm một hoặc nhiều tùy chọn thiết bị, và mỗi tùy chọn thiết bị tương ứng với một thiết bị không dây được tìm thấy bởi điện thoại di động A
S703: Thu thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất trên giao diện thứ nhất
S704: Điện thoại di động A gửi, đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất, thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới điện thoại di động B tương ứng với tùy chọn thiết bị thứ nhất
Tới FIG.3C
Tới FIG.3C

FIG. 3B

Tiếp theo từ FIG.3B

Tiếp theo từ FIG.3B

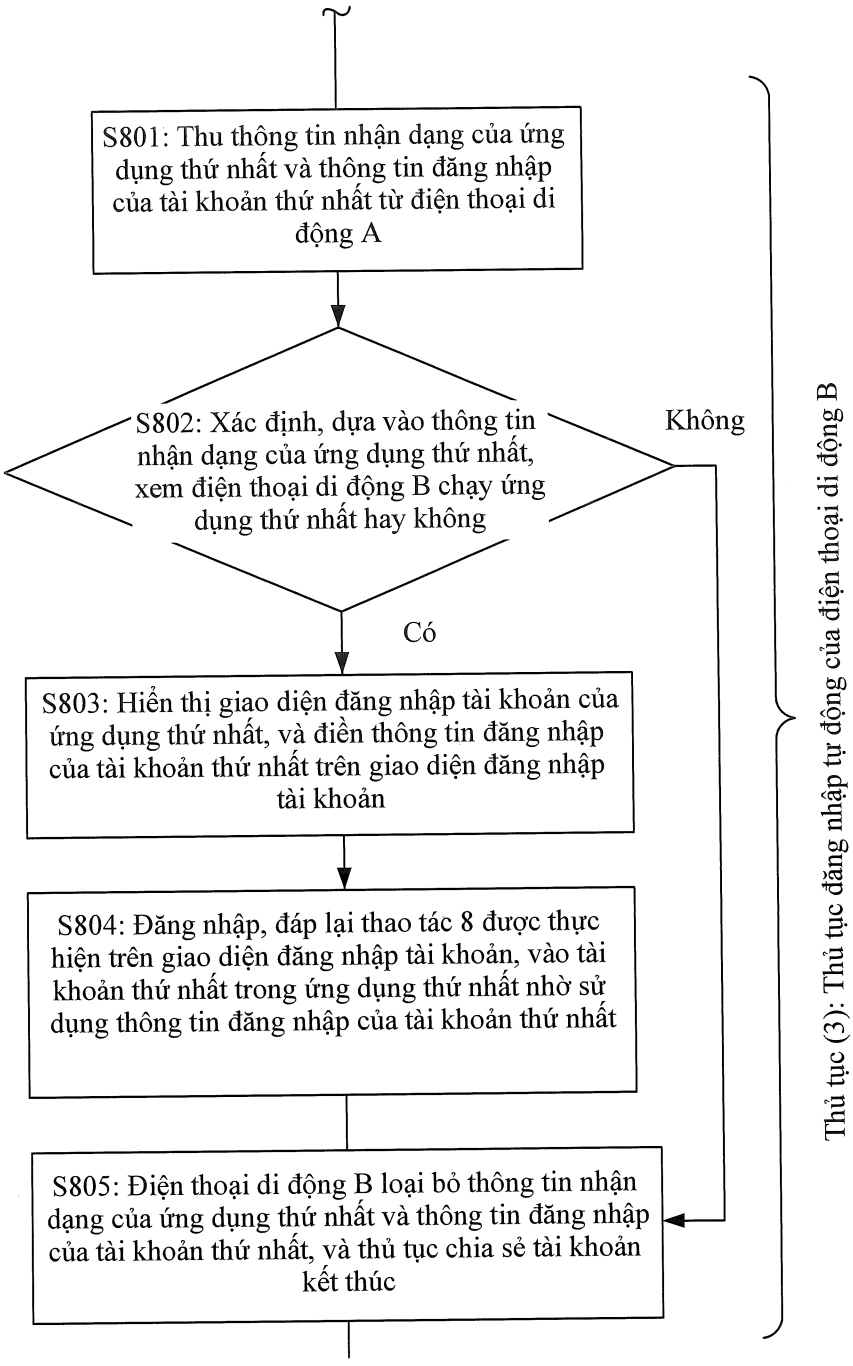

FIG. 3C

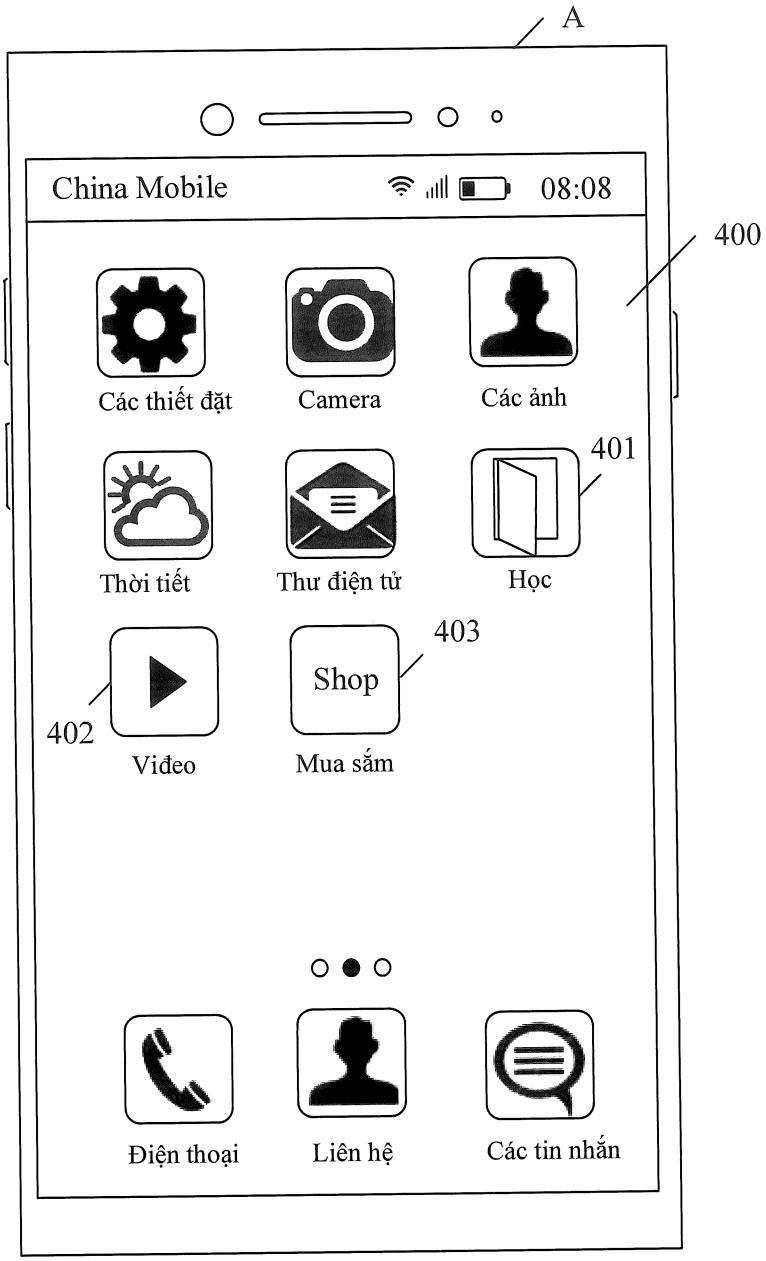
A
China Mobile
08:08
400
Các thiết đặt
Camera
Các ảnh
401
Thời tiết
Thư điện tử
Học
403
Shop
402
Viđeo
Mua sắm
Điện thoại
Liên hệ
Các tin nhắn

FIG. 4(a)

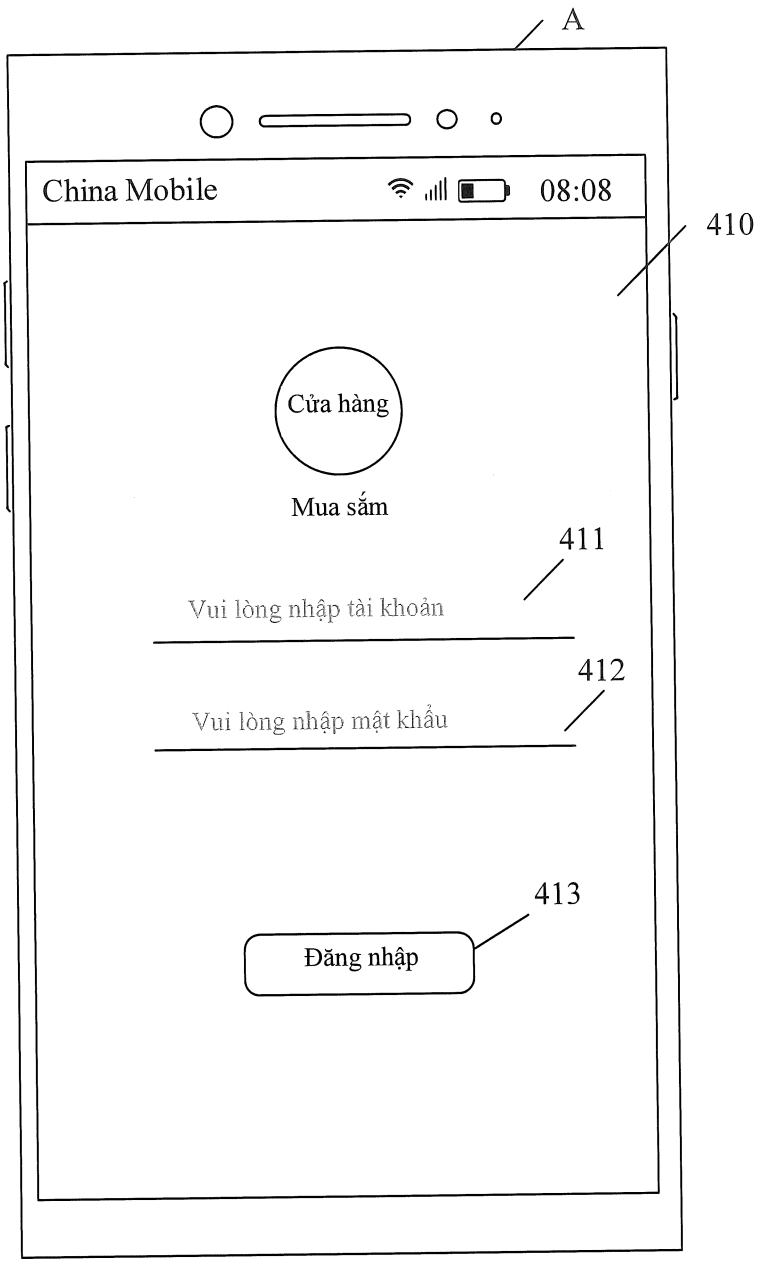
A
China Mobile
08:08
410
Cửa hàng
Mua sắm
411
Vui lòng nhập tài khoản
412
Vui lòng nhập mật khẩu
413
Đăng nhập

FIG. 4(b)

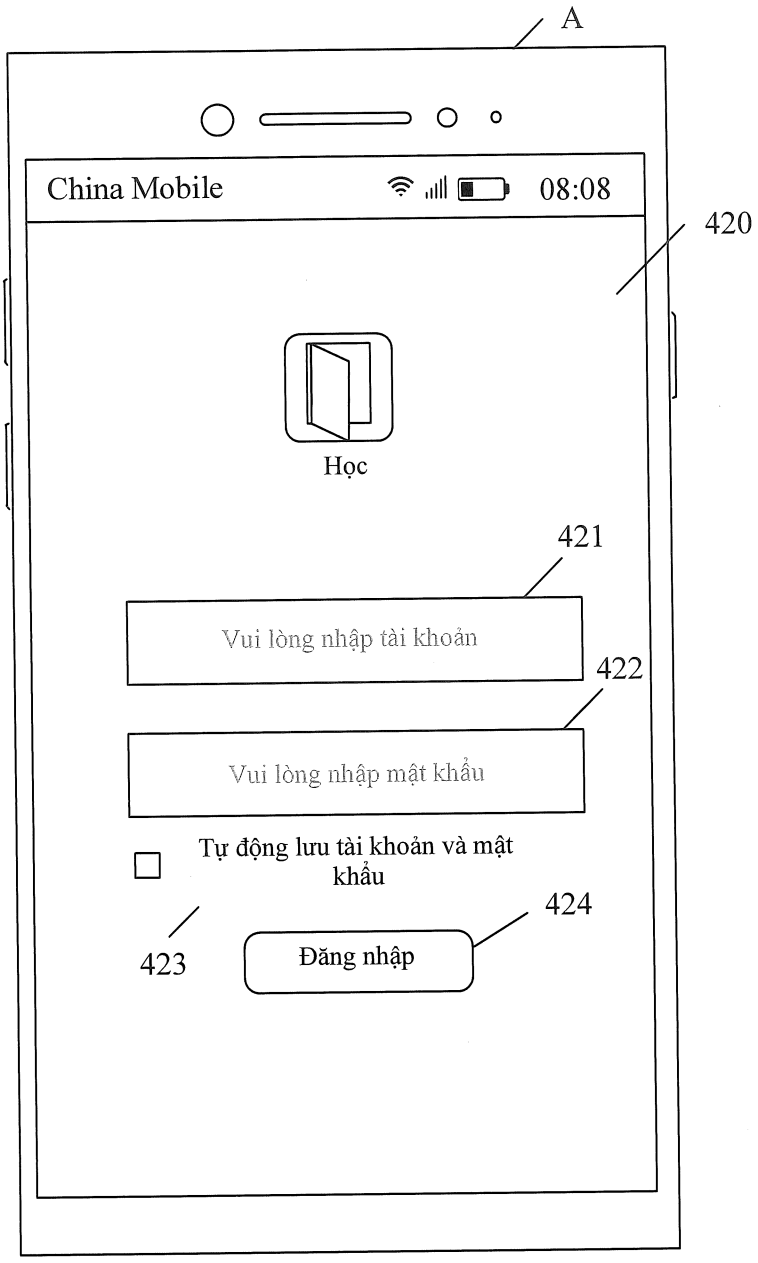
A
China Mobile
08:08
420
Học
421
Vui lòng nhập tài khoản
422
Vui lòng nhập mật khẩu
Tự động lưu tài khoản và mật khẩu
423
424
Đăng nhập

FIG. 4(c)

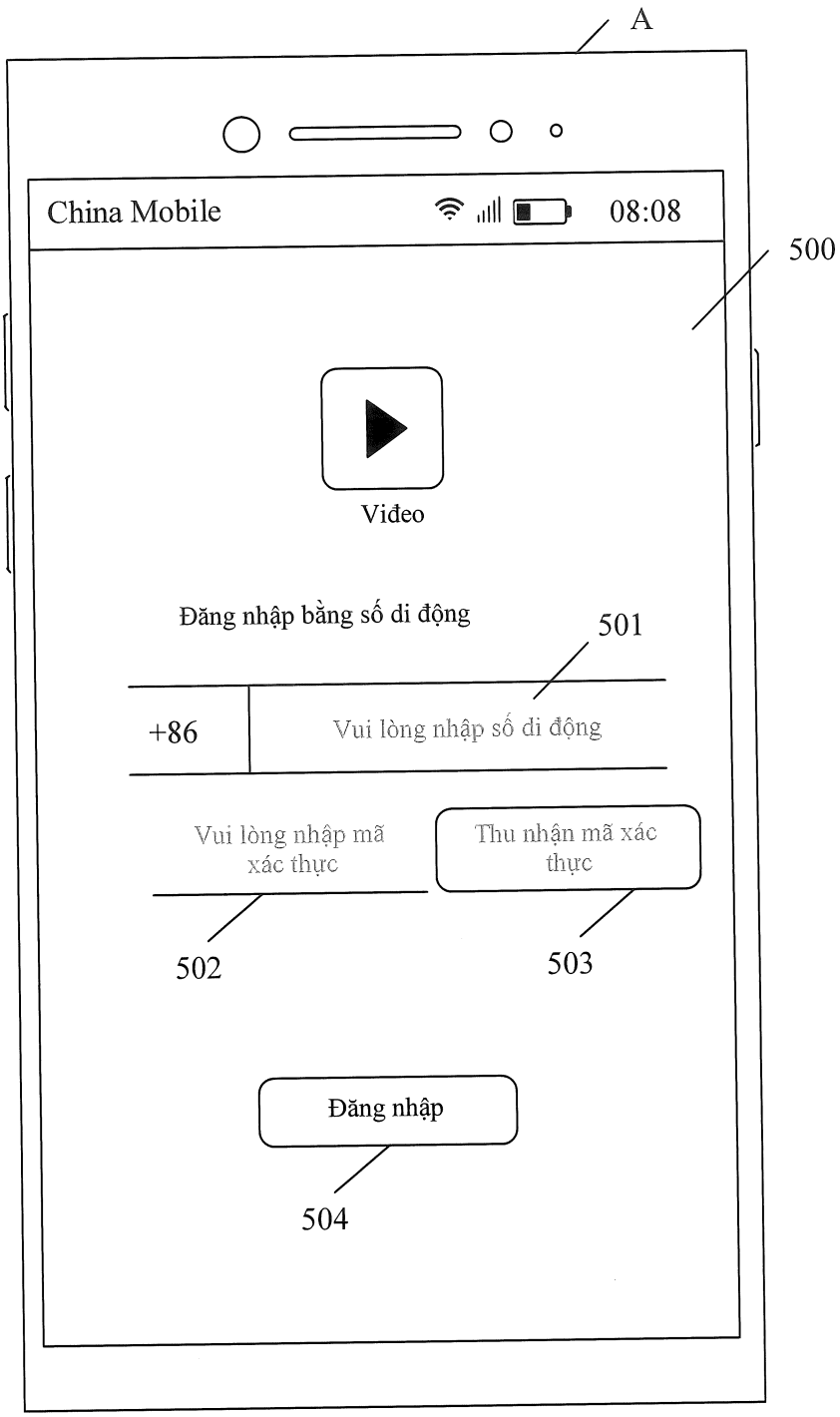
A
China Mobile
08:08
500
Viđeo
Đăng nhập bằng số di động
501
+86
Vui lòng nhập số di động
Vui lòng nhập mã xác thực
Thu nhận mã xác thực
502
503
Đăng nhập
504

FIG. 5

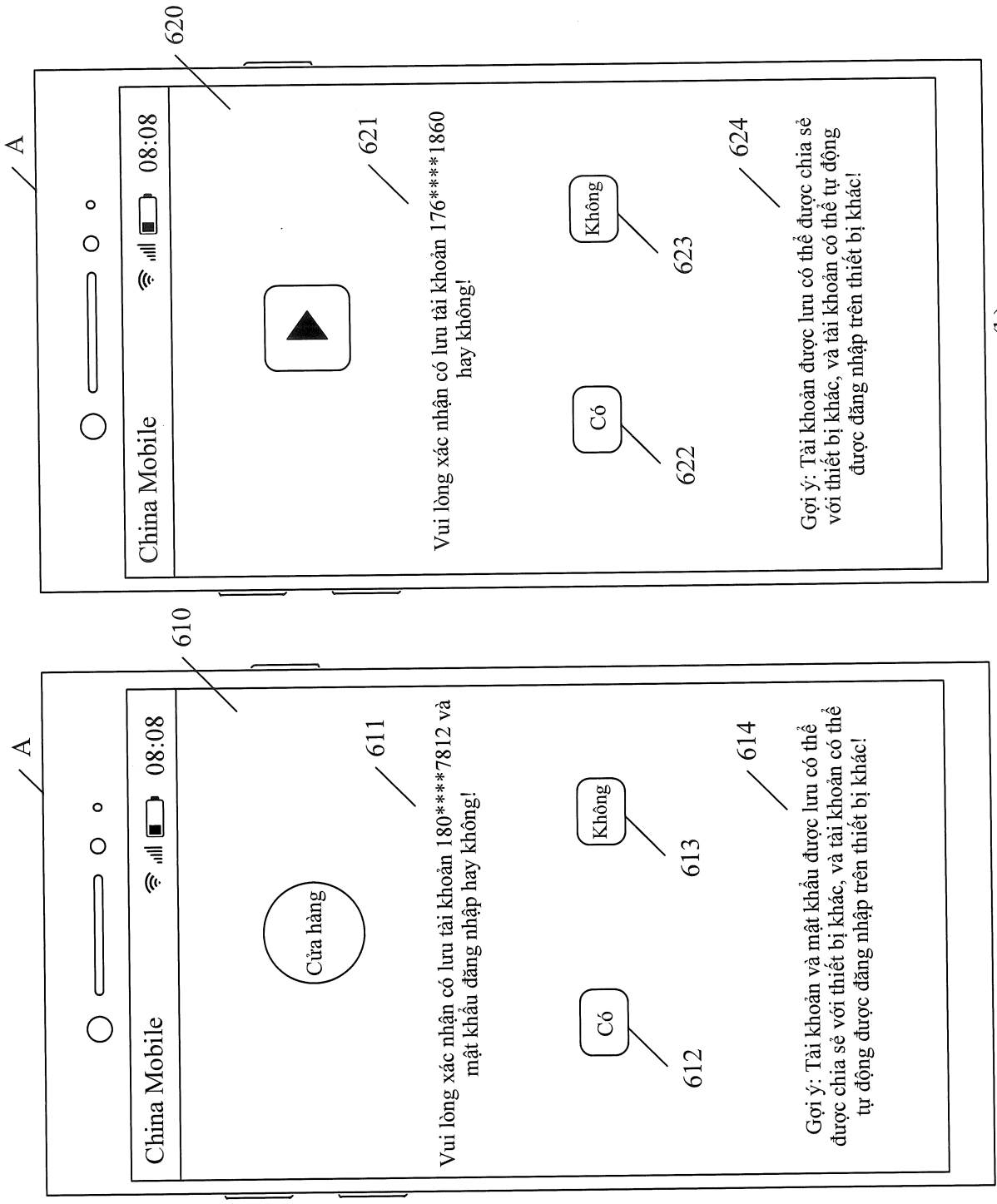
A
610
China Mobile
08:08
Cửa hàng
611
Vui lòng xác nhận có lưu tài khoản 180****7812 và mật khẩu đăng nhập hay không!
Có
612
Không
613
Gợi ý: Tài khoản và mật khẩu được lưu có thể được chia sẻ với thiết bị khác, và tài khoản có thể tự động được đăng nhập trên thiết bị khác!
614
(a)
A
620
China Mobile
08:08
621
Vui lòng xác nhận có lưu tài khoản 176****1860 hay không!
Có
622
Không
623
Gợi ý: Tài khoản được lưu có thể được chia sẻ với thiết bị khác, và tài khoản có thể tự động được đăng nhập trên thiết bị khác!
624
(b)

FIG. 6A

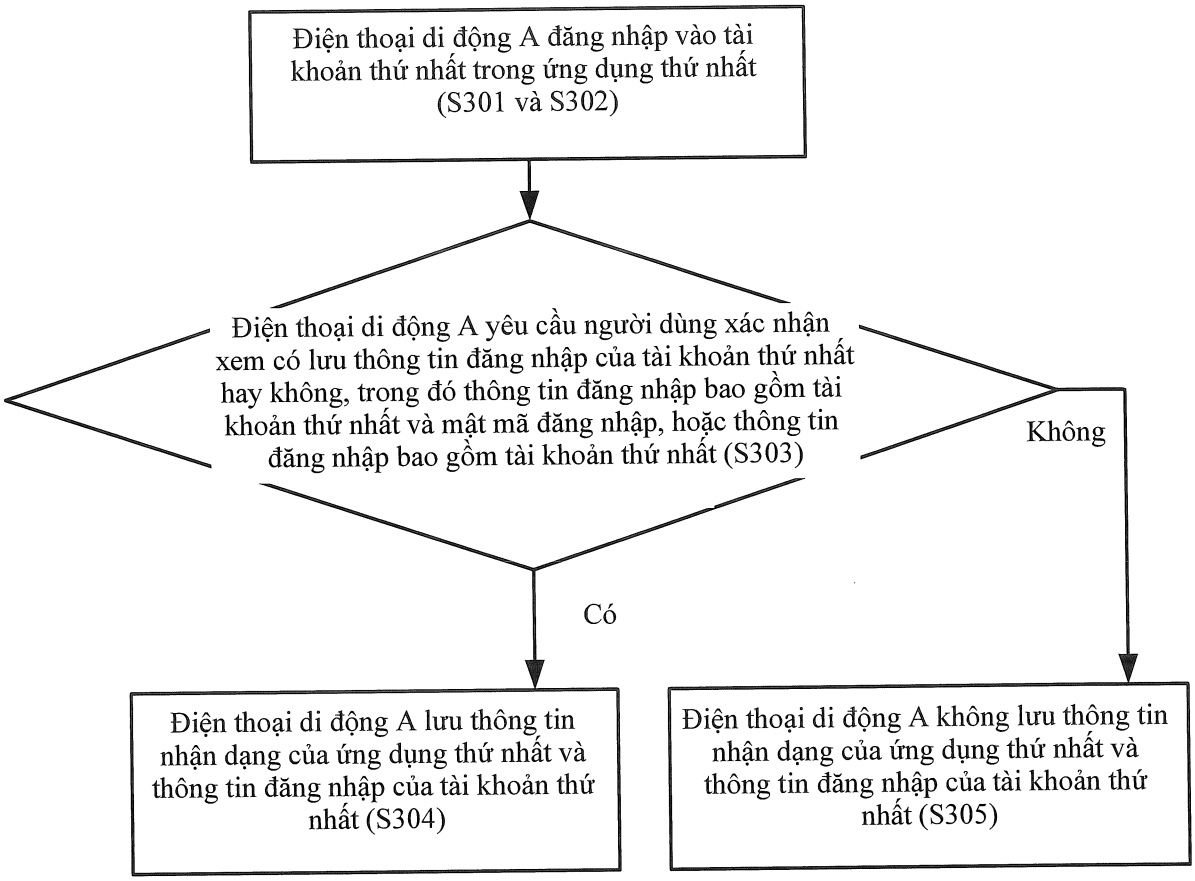
Điện thoại di động A đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất (S301 và S302)
Điện thoại di động A yêu cầu người dùng xác nhận xem có lưu thông tin đăng nhập của tài khoản thứ nhất hay không, trong đó thông tin đăng nhập bao gồm tài khoản thứ nhất và mật mã đăng nhập, hoặc thông tin đăng nhập bao gồm tài khoản thứ nhất (S303)
Không
Có
Điện thoại di động A lưu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất (S304)
Điện thoại di động A không lưu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất (S305)

FIG. 6B

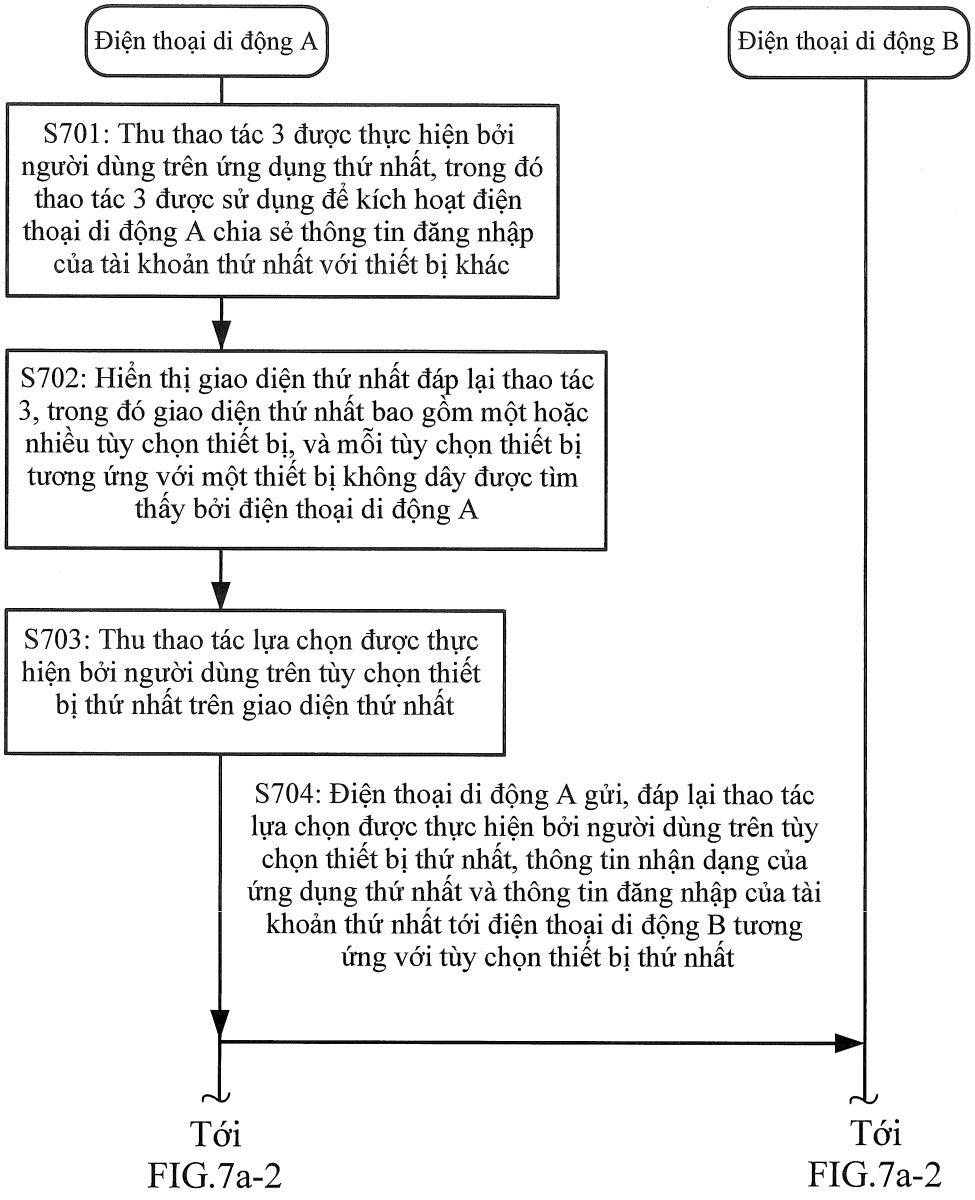
Điện thoại di động A
Điện thoại di động B
S701: Thu thao tác 3 được thực hiện bởi người dùng trên ứng dụng thứ nhất, trong đó thao tác 3 được sử dụng để kích hoạt điện thoại di động A chia sẻ thông tin đăng nhập của tài khoản thứ nhất với thiết bị khác
S702: Hiển thị giao diện thứ nhất đáp lại thao tác 3, trong đó giao diện thứ nhất bao gồm một hoặc nhiều tùy chọn thiết bị, và mỗi tùy chọn thiết bị tương ứng với một thiết bị không dây được tìm thấy bởi điện thoại di động A
S703: Thu thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất trên giao diện thứ nhất
S704: Điện thoại di động A gửi, đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất, thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới điện thoại di động B tương ứng với tùy chọn thiết bị thứ nhất
Tới FIG.7a-2
Tới FIG.7a-2

FIG. 7A-1

Tiếp theo từ FIG.7a-1

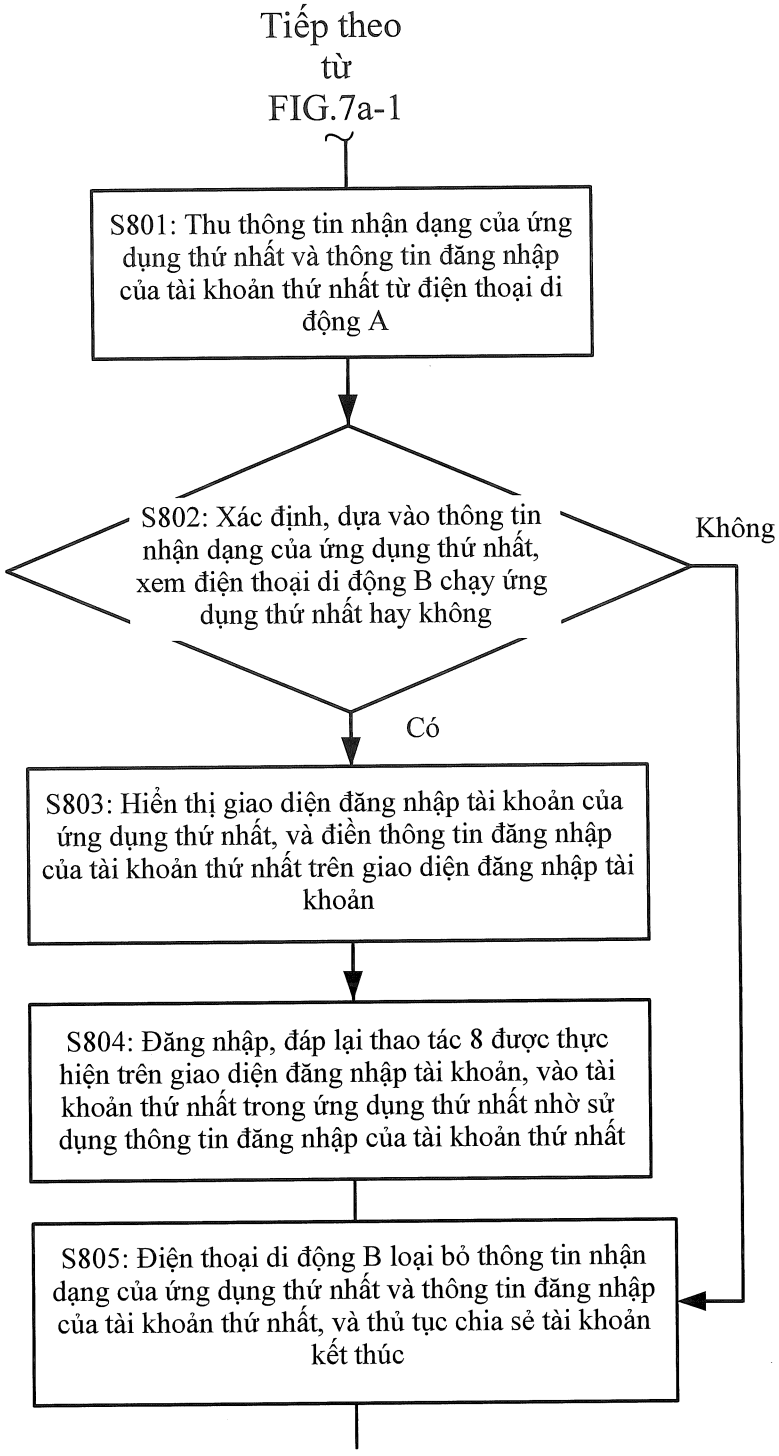

FIG. 7A-2

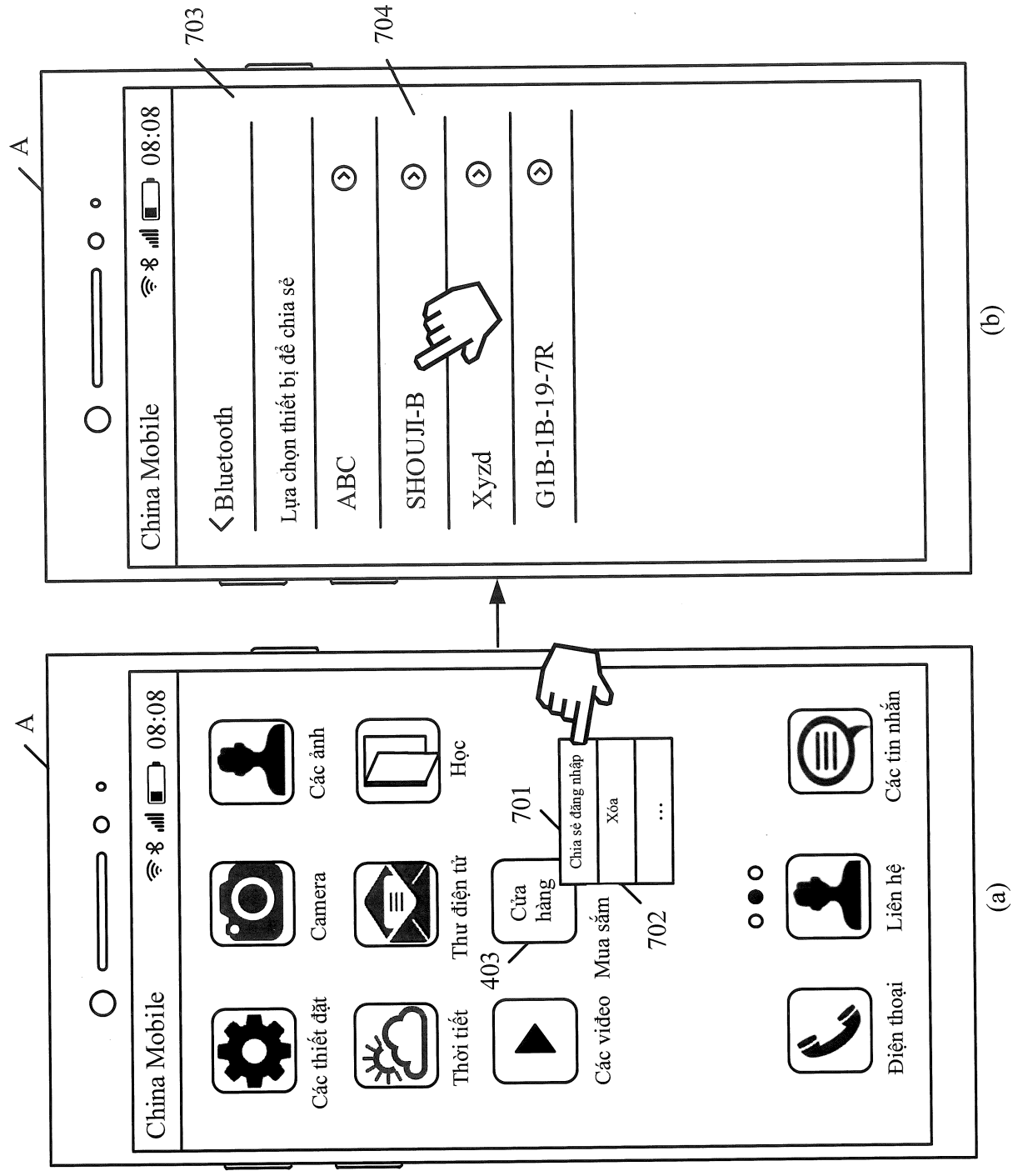
A
China Mobile
08:08
Các thiết đặt
Camera
Các ảnh
Thời tiết
Thư điện tử
Học
Các video
Cửa hàng
Mua sắm
Điện thoại
Liên hệ
Các tin nhắn
403
701
Chia sẻ đăng nhập
Xóa
...
702
(a)
A
China Mobile
08:08
Bluetooth
Lựa chọn thiết bị để chia sẻ
ABC
SHOUJI-B
Xyzd
G1B-1B-19-7R
703
704
(b)

FIG. 7B

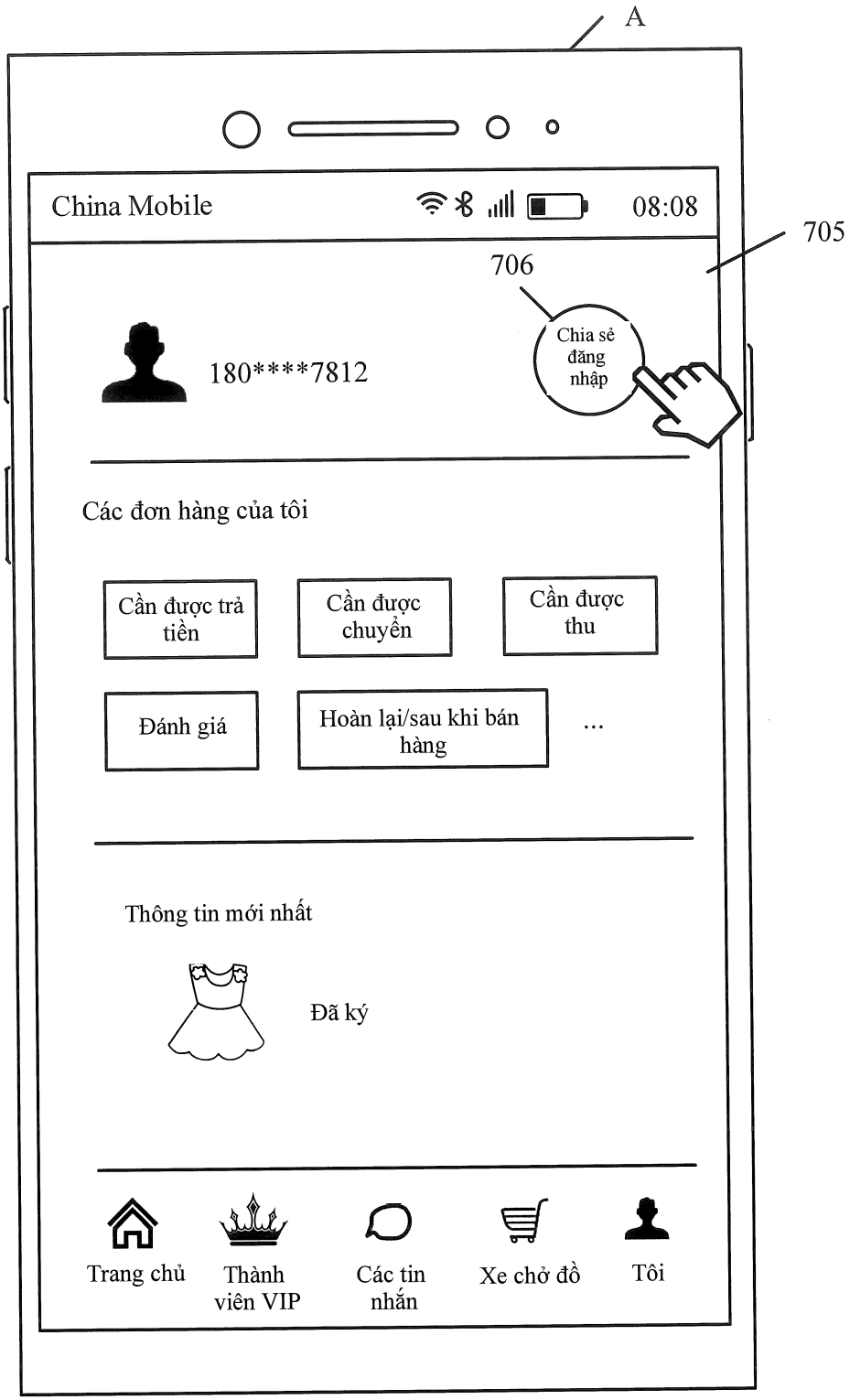
A
China Mobile
08:08
705
706
Chia sẻ đăng nhập
180****7812
Các đơn hàng của tôi
Cần được trả tiền
Cần được chuyển
Cần được thu
Đánh giá
Hoàn lại/sau khi bán hàng
...
Thông tin mới nhất
Đã ký
Trang chủ
Thành viên VIP
Các tin nhắn
Xe chở đồ
Tôi

FIG. 7C

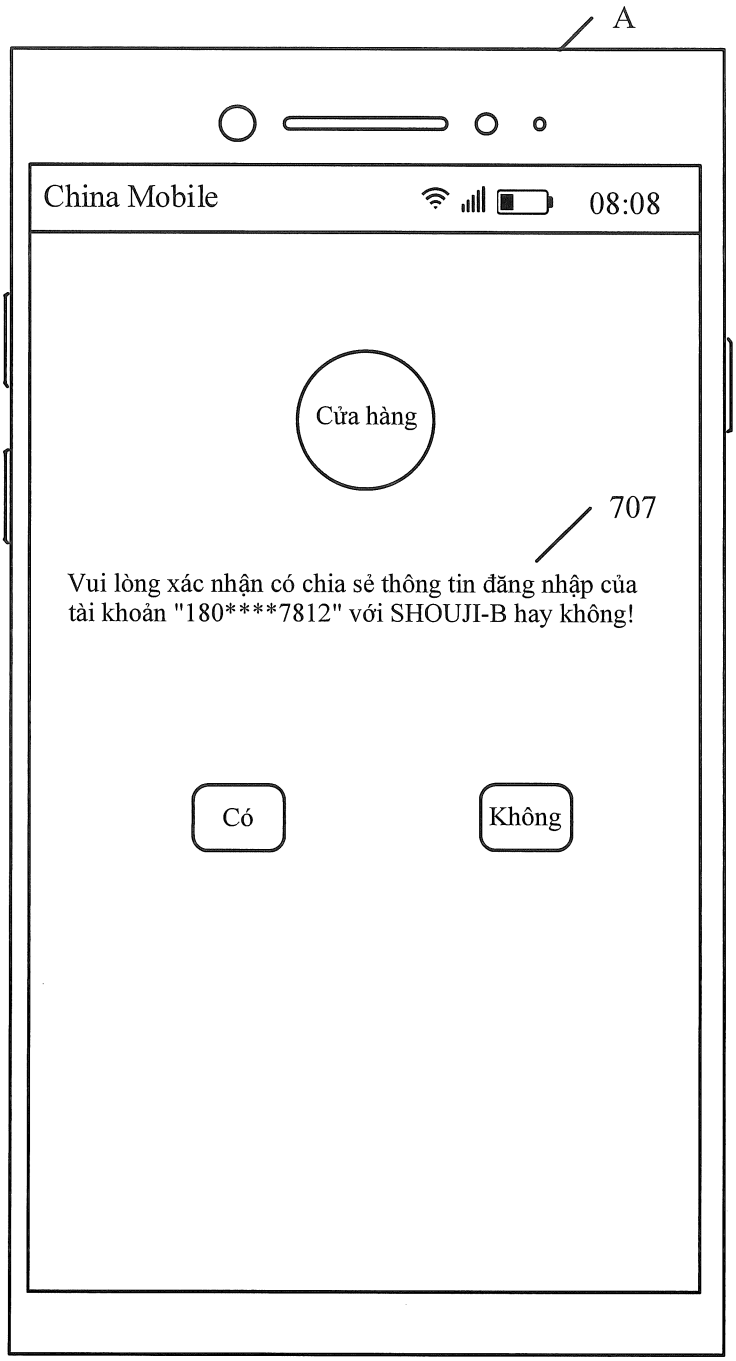
A
China Mobile
08:08
Cửa hàng
707
Vui lòng xác nhận có chia sẻ thông tin đăng nhập của tài khoản "180****7812" với SHOUJI-B hay không!
Có
Không

FIG. 7D

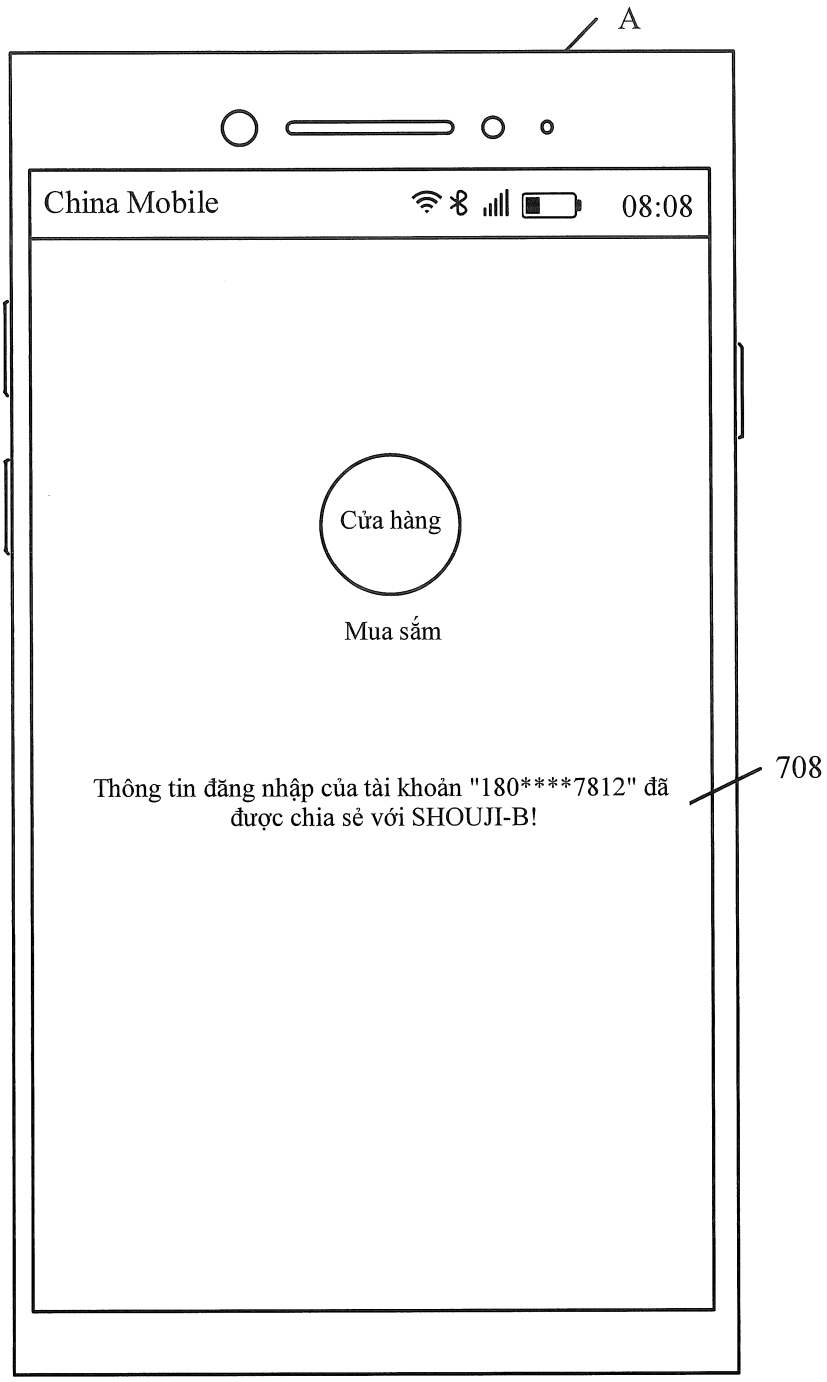
A
China Mobile
08:08
Cửa hàng
Mua sắm
Thông tin đăng nhập của tài khoản "180****7812" đã được chia sẻ với SHOUJI-B!
708

FIG. 7E

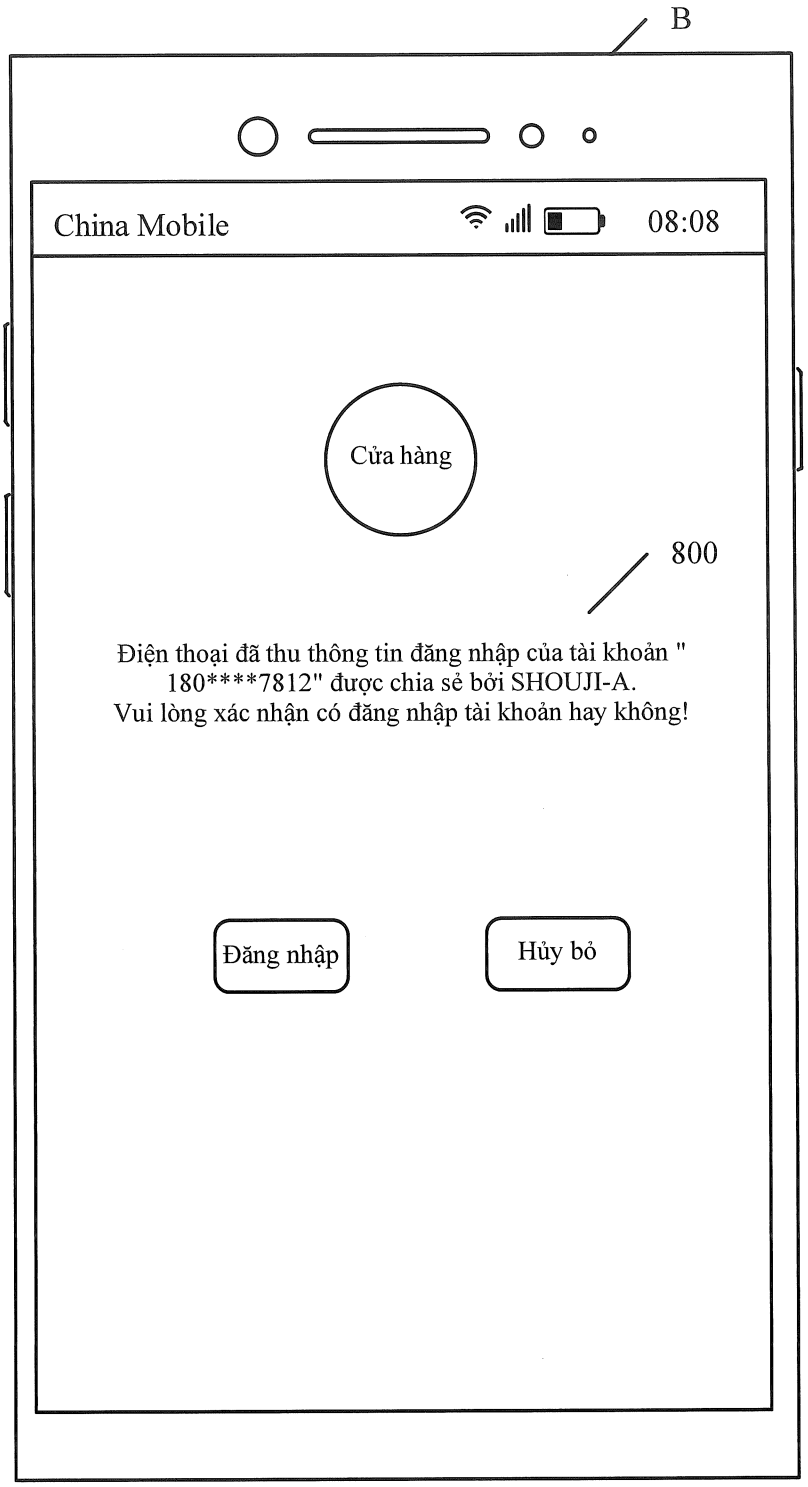
B
China Mobile
08:08
Cửa hàng
800
Điện thoại đã thu thông tin đăng nhập của tài khoản "
180****7812" được chia sẻ bởi SHOUJI-A.
Vui lòng xác nhận có đăng nhập tài khoản hay không!
Đăng nhập
Hủy bỏ

FIG. 8

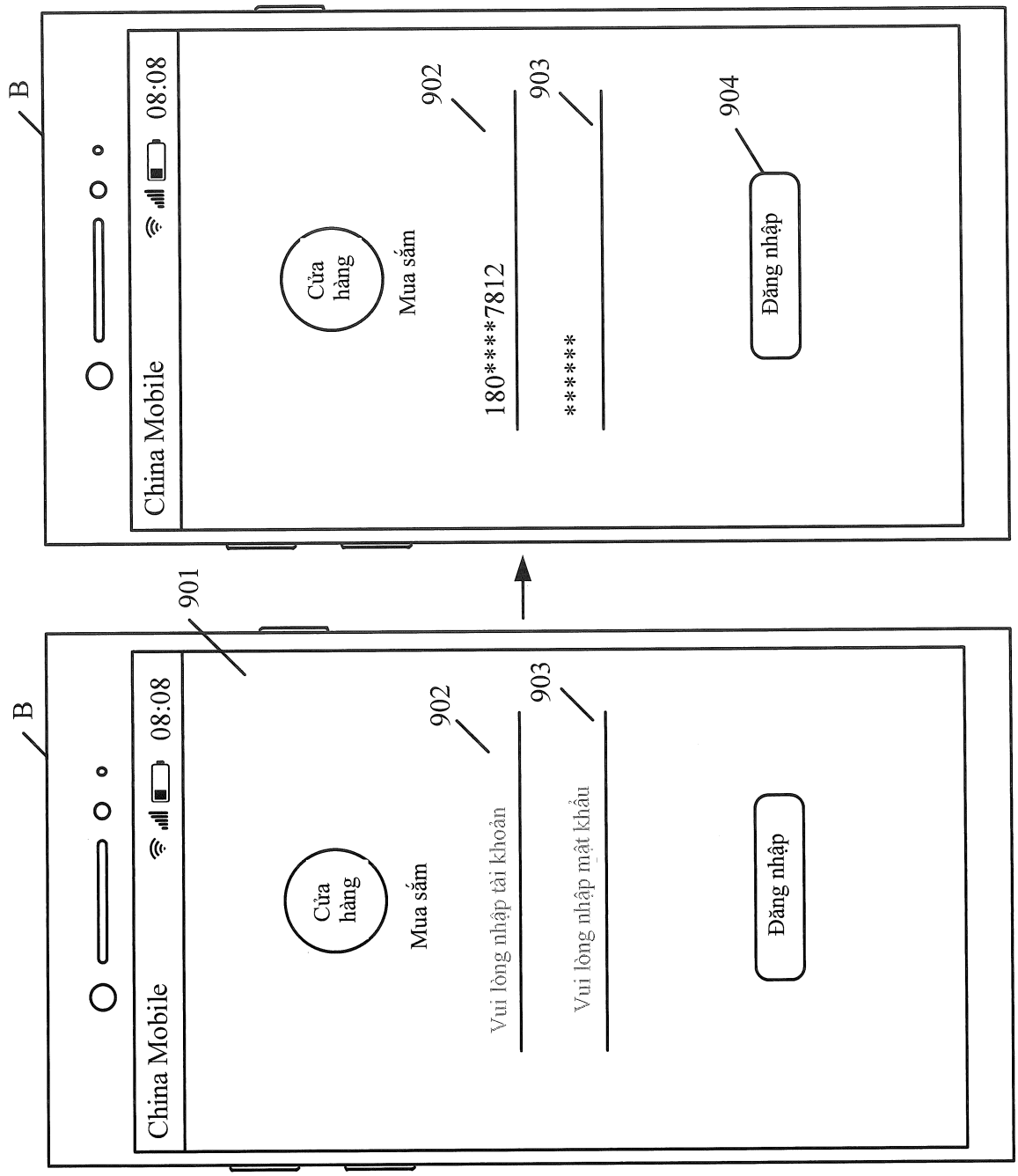
B
08:08
China Mobile
901
Cửa hàng
Mua sắm
902
Vui lòng nhập tài khoản
903
Vui lòng nhập mật khẩu
Đăng nhập
(a)
B
08:08
China Mobile
Cửa hàng
Mua sắm
902
180****7812
903
******
904
Đăng nhập
(b)

FIG. 9

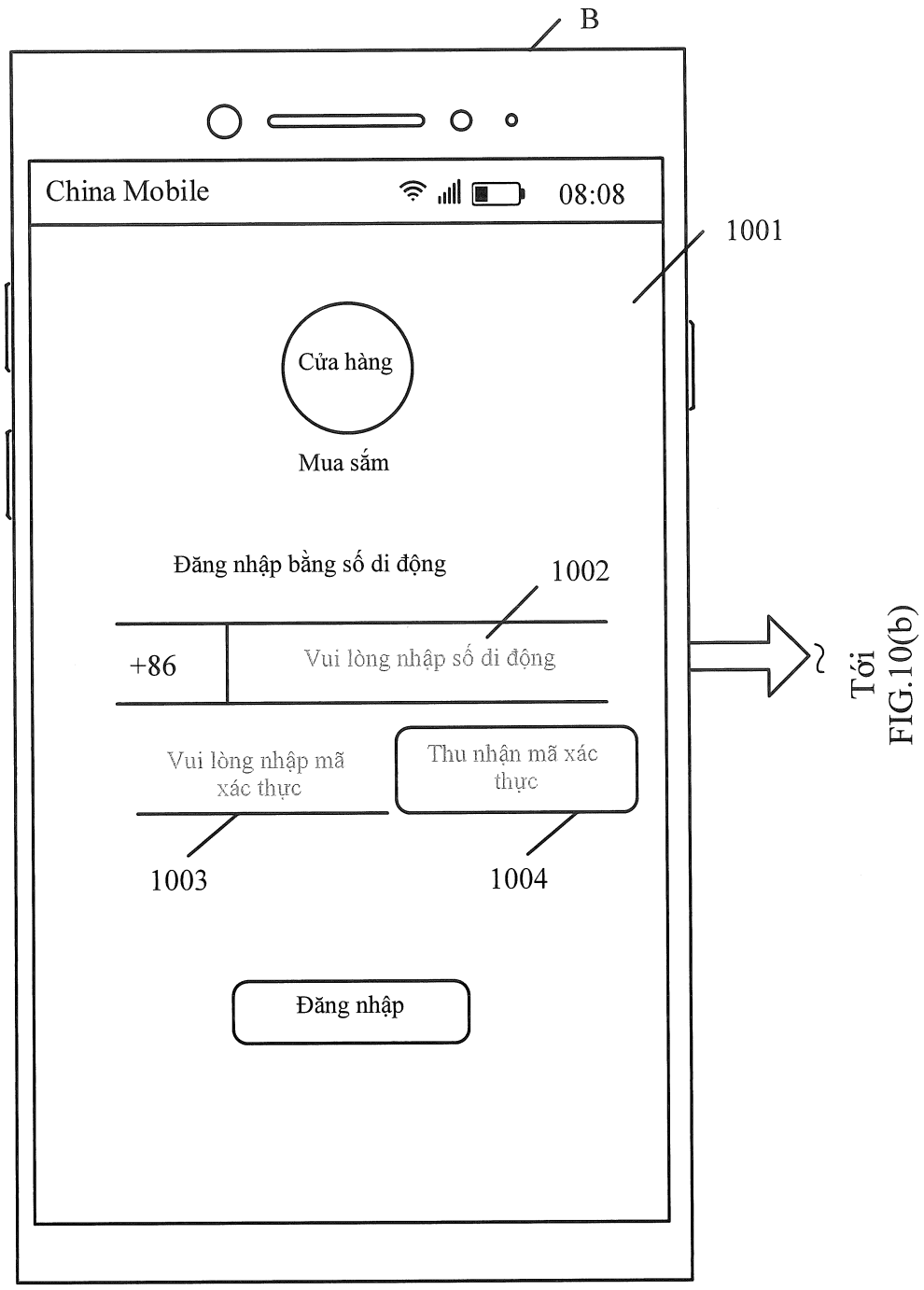
B
China Mobile
08:08
1001
Cửa hàng
Mua sắm
Đăng nhập bằng số di động
1002
+86
Vui lòng nhập số di động
Vui lòng nhập mã xác thực
Thu nhận mã xác thực
1003
1004
Đăng nhập
Tới FIG.10(b)

FIG. 10(a)

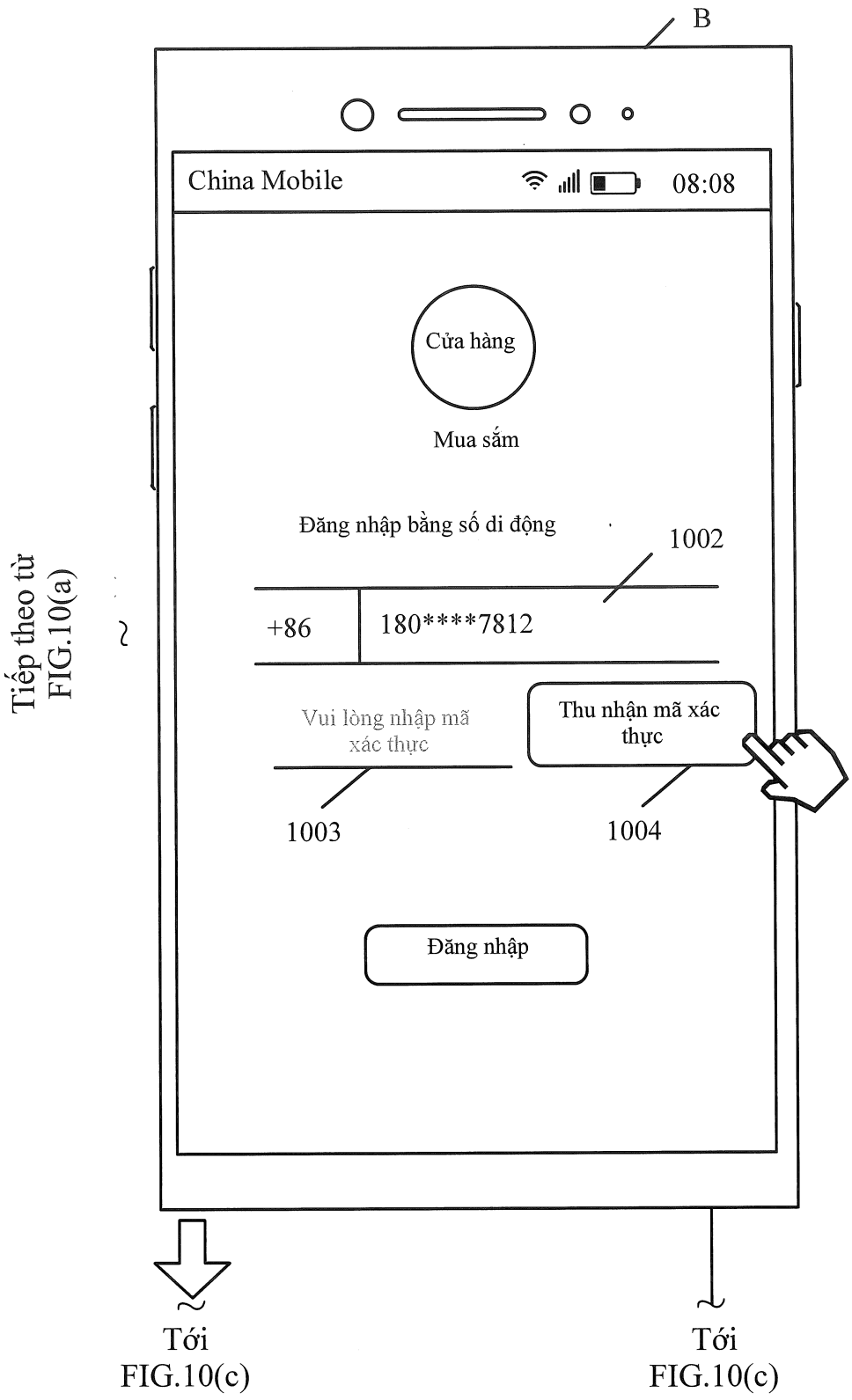
B
China Mobile
08:08
Cửa hàng
Mua sắm
Đăng nhập bằng số di động
1002
+86
180****7812
Vui lòng nhập mã xác thực
Thu nhận mã xác thực
1003
1004
Đăng nhập
Tiếp theo từ FIG.10(a)
Tới FIG.10(c)
Tới FIG.10(c)

FIG. 10(b)

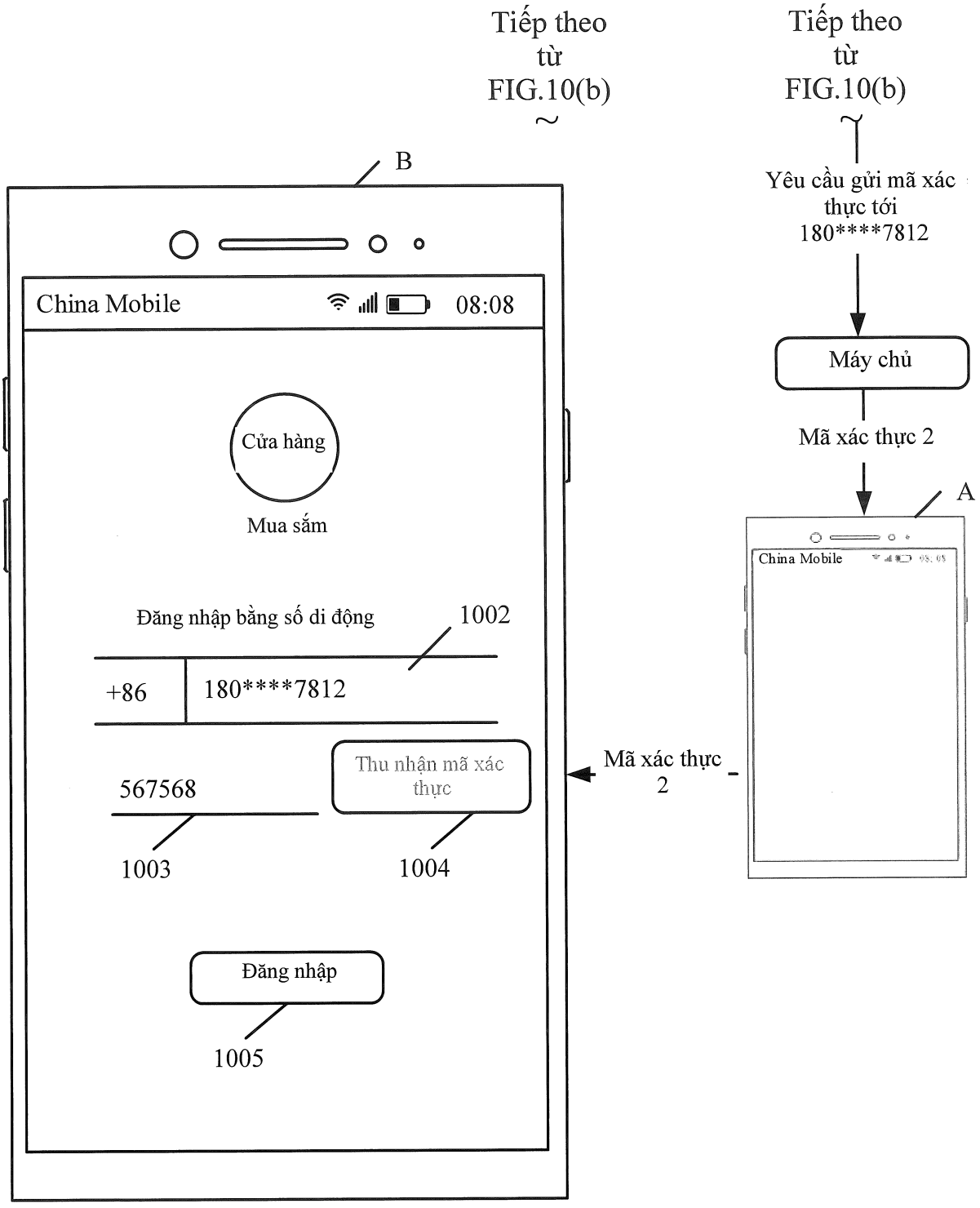
Tiếp theo từ FIG.10(b)
Tiếp theo từ FIG.10(b)
Yêu cầu gửi mã xác thực tới 180****7812
Máy chủ
Mã xác thực 2
A
B
China Mobile
08:08
Cửa hàng
Mua sắm
Đăng nhập bằng số di động
1002
+86
180****7812
Thu nhận mã xác thực
Mã xác thực 2
567568
1003
1004
Đăng nhập
1005

FIG. 10(c)

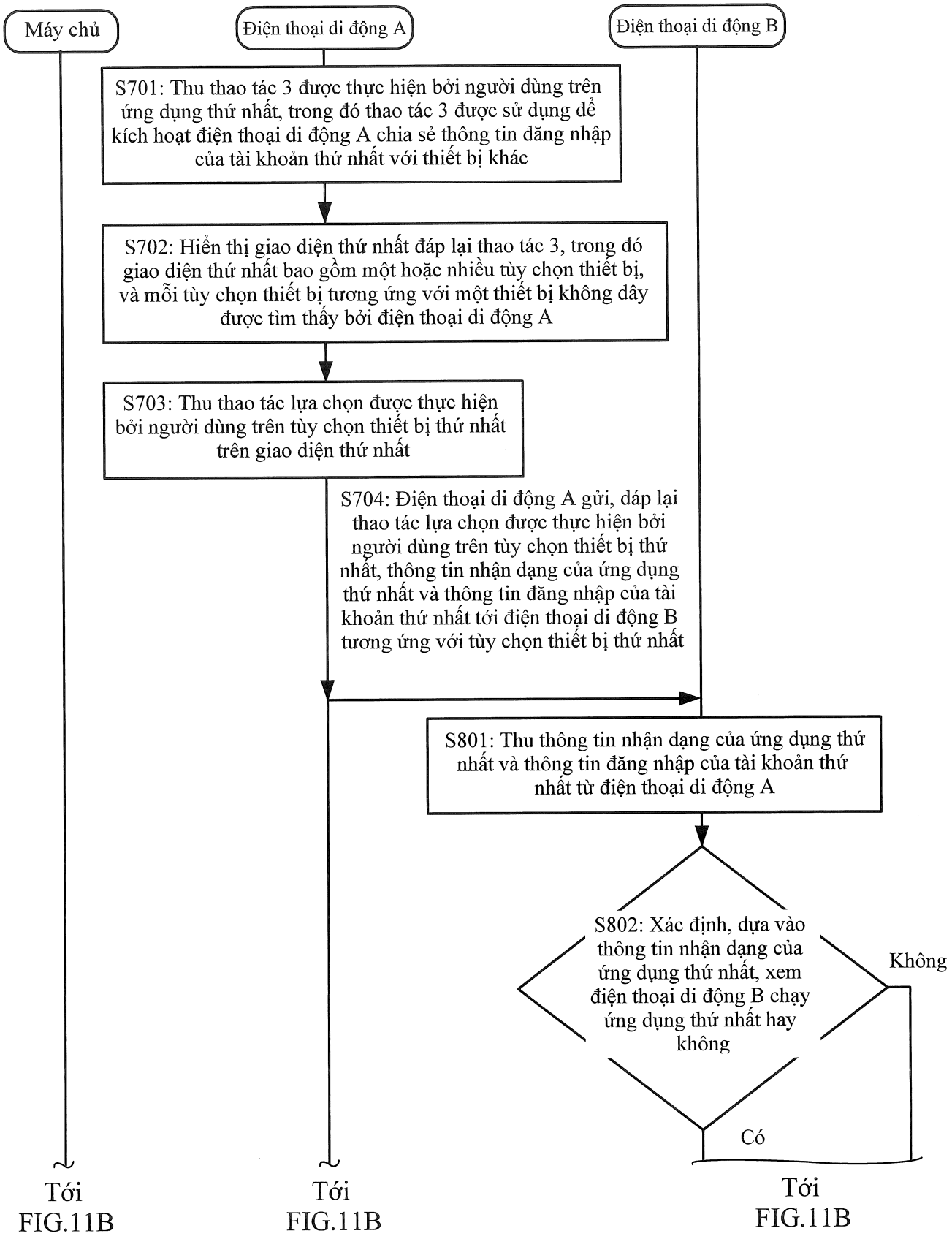
Máy chủ
Điện thoại di động A
Điện thoại di động B
S701: Thu thao tác 3 được thực hiện bởi người dùng trên ứng dụng thứ nhất, trong đó thao tác 3 được sử dụng để kích hoạt điện thoại di động A chia sẻ thông tin đăng nhập của tài khoản thứ nhất với thiết bị khác
S702: Hiển thị giao diện thứ nhất đáp lại thao tác 3, trong đó giao diện thứ nhất bao gồm một hoặc nhiều tùy chọn thiết bị, và mỗi tùy chọn thiết bị tương ứng với một thiết bị không dây được tìm thấy bởi điện thoại di động A
S703: Thu thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất trên giao diện thứ nhất
S704: Điện thoại di động A gửi, đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất, thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất tới điện thoại di động B tương ứng với tùy chọn thiết bị thứ nhất
S801: Thu thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất từ điện thoại di động A
S802: Xác định, dựa vào thông tin nhận dạng của ứng dụng thứ nhất, xem điện thoại di động B chạy ứng dụng thứ nhất hay không
Không
Có
Tới FIG.11B
Tới FIG.11B
Tới FIG.11B

FIG. 11A

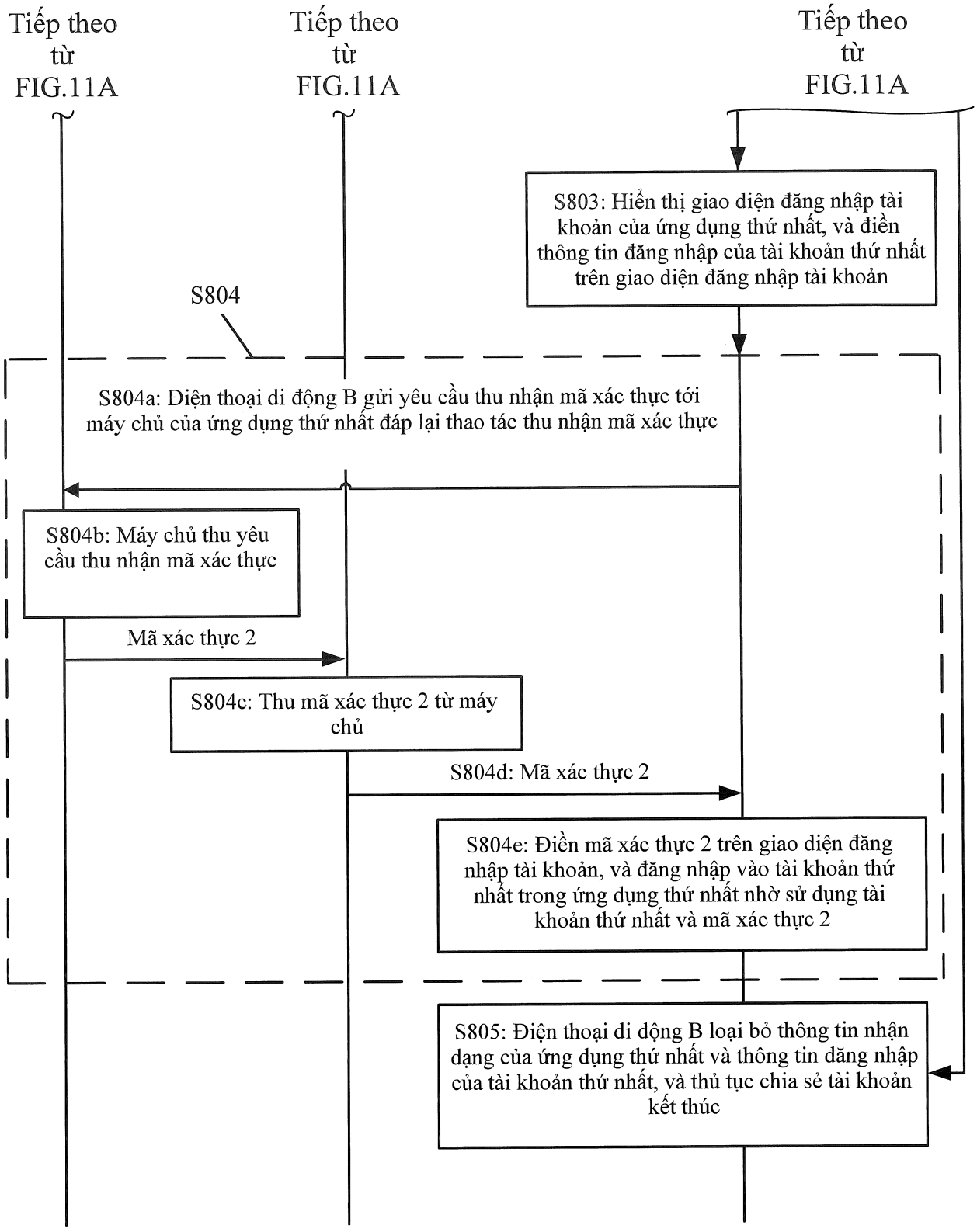
Tiếp theo từ FIG.11A
Tiếp theo từ FIG.11A
Tiếp theo từ FIG.11A
S803: Hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất, và điền thông tin đăng nhập của tài khoản thứ nhất trên giao diện đăng nhập tài khoản
S804
S804a: Điện thoại di động B gửi yêu cầu thu nhận mã xác thực tới máy chủ của ứng dụng thứ nhất đáp lại thao tác thu nhận mã xác thực
S804b: Máy chủ thu yêu cầu thu nhận mã xác thực
Mã xác thực 2
S804c: Thu mã xác thực 2 từ máy chủ
S804d: Mã xác thực 2
S804e: Điền mã xác thực 2 trên giao diện đăng nhập tài khoản, và đăng nhập vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng tài khoản thứ nhất và mã xác thực 2
S805: Điện thoại di động B loại bỏ thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất, và thủ tục chia sẻ tài khoản kết thúc

FIG. 11B

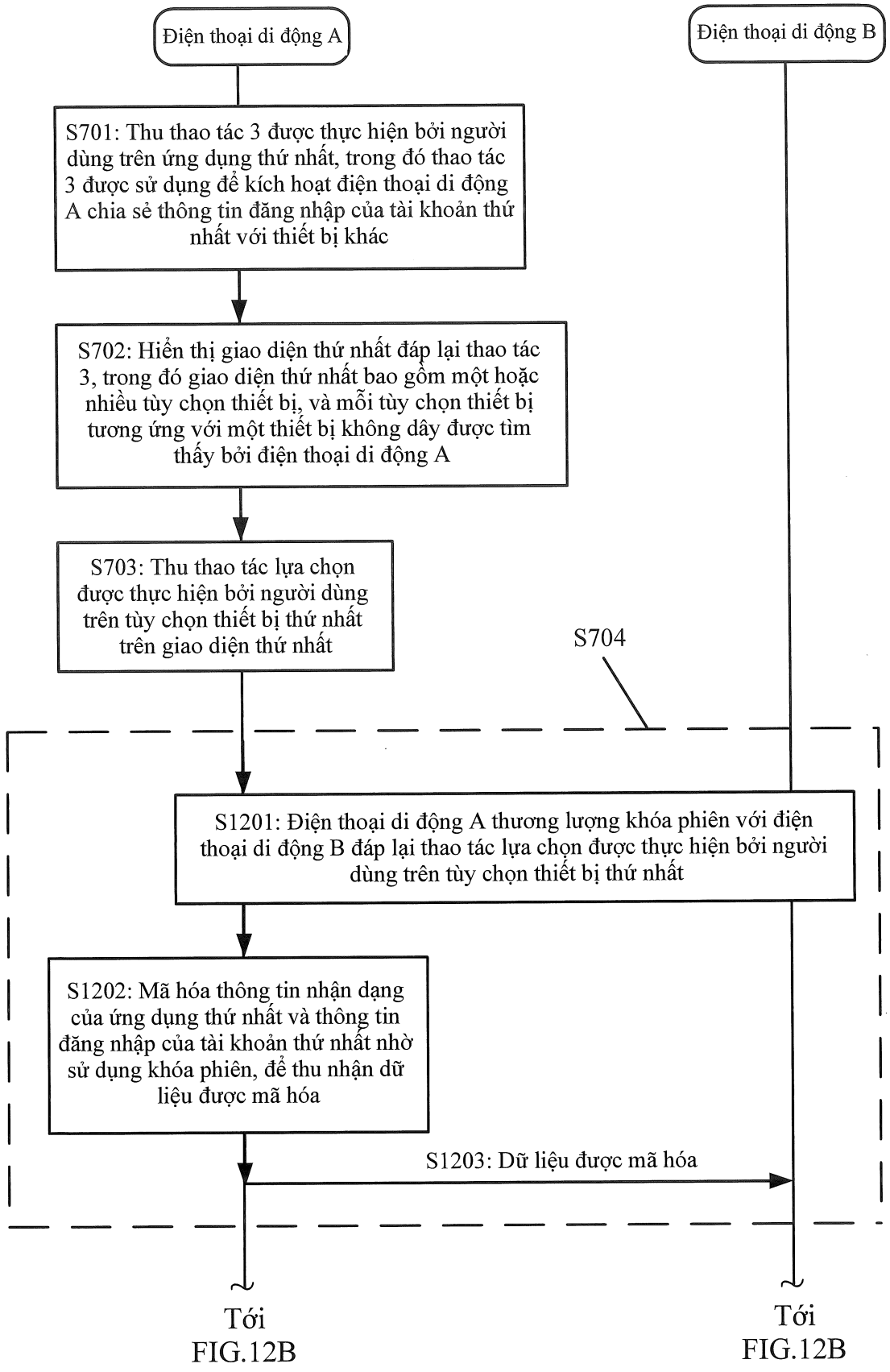
Điện thoại di động A
Điện thoại di động B
S701: Thu thao tác 3 được thực hiện bởi người dùng trên ứng dụng thứ nhất, trong đó thao tác 3 được sử dụng để kích hoạt điện thoại di động A chia sẻ thông tin đăng nhập của tài khoản thứ nhất với thiết bị khác
S702: Hiển thị giao diện thứ nhất đáp lại thao tác 3, trong đó giao diện thứ nhất bao gồm một hoặc nhiều tùy chọn thiết bị, và mỗi tùy chọn thiết bị tương ứng với một thiết bị không dây được tìm thấy bởi điện thoại di động A
S703: Thu thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất trên giao diện thứ nhất
S704
S1201: Điện thoại di động A thương lượng khóa phiên với điện thoại di động B đáp lại thao tác lựa chọn được thực hiện bởi người dùng trên tùy chọn thiết bị thứ nhất
S1202: Mã hóa thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất nhờ sử dụng khóa phiên, để thu nhận dữ liệu được mã hóa
S1203: Dữ liệu được mã hóa
Tới FIG.12B
Tới FIG.12B

FIG. 12A

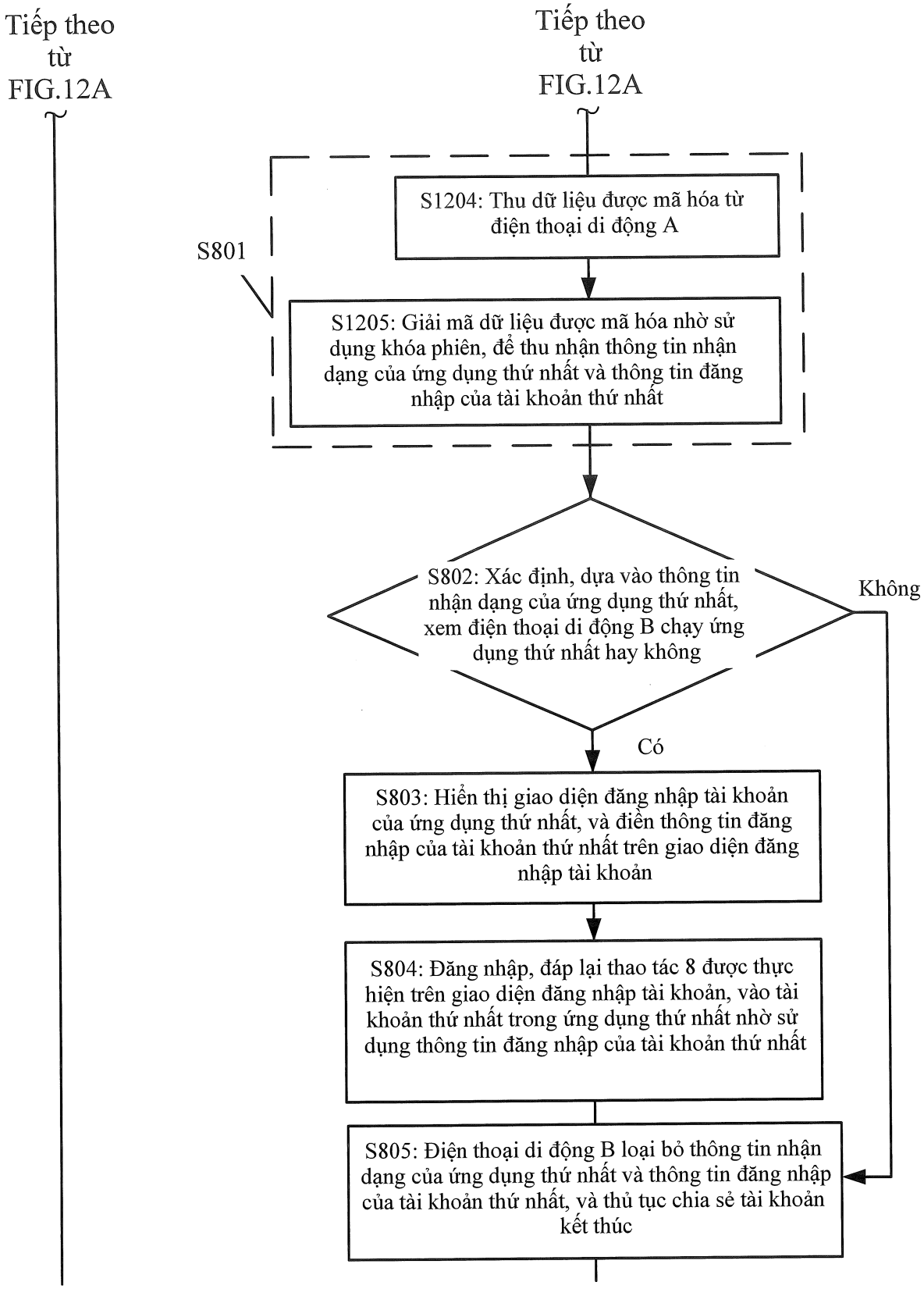
Tiếp theo từ FIG.12A
Tiếp theo từ FIG.12A
S801
S1204: Thu dữ liệu được mã hóa từ điện thoại di động A
S1205: Giải mã dữ liệu được mã hóa nhờ sử dụng khóa phiên, để thu nhận thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất
S802: Xác định, dựa vào thông tin nhận dạng của ứng dụng thứ nhất, xem điện thoại di động B chạy ứng dụng thứ nhất hay không
Không
Có
S803: Hiển thị giao diện đăng nhập tài khoản của ứng dụng thứ nhất, và điền thông tin đăng nhập của tài khoản thứ nhất trên giao diện đăng nhập tài khoản
S804: Đăng nhập, đáp lại thao tác 8 được thực hiện trên giao diện đăng nhập tài khoản, vào tài khoản thứ nhất trong ứng dụng thứ nhất nhờ sử dụng thông tin đăng nhập của tài khoản thứ nhất
S805: Điện thoại di động B loại bỏ thông tin nhận dạng của ứng dụng thứ nhất và thông tin đăng nhập của tài khoản thứ nhất, và thủ tục chia sẻ tài khoản kết thúc

FIG. 12B

27/27

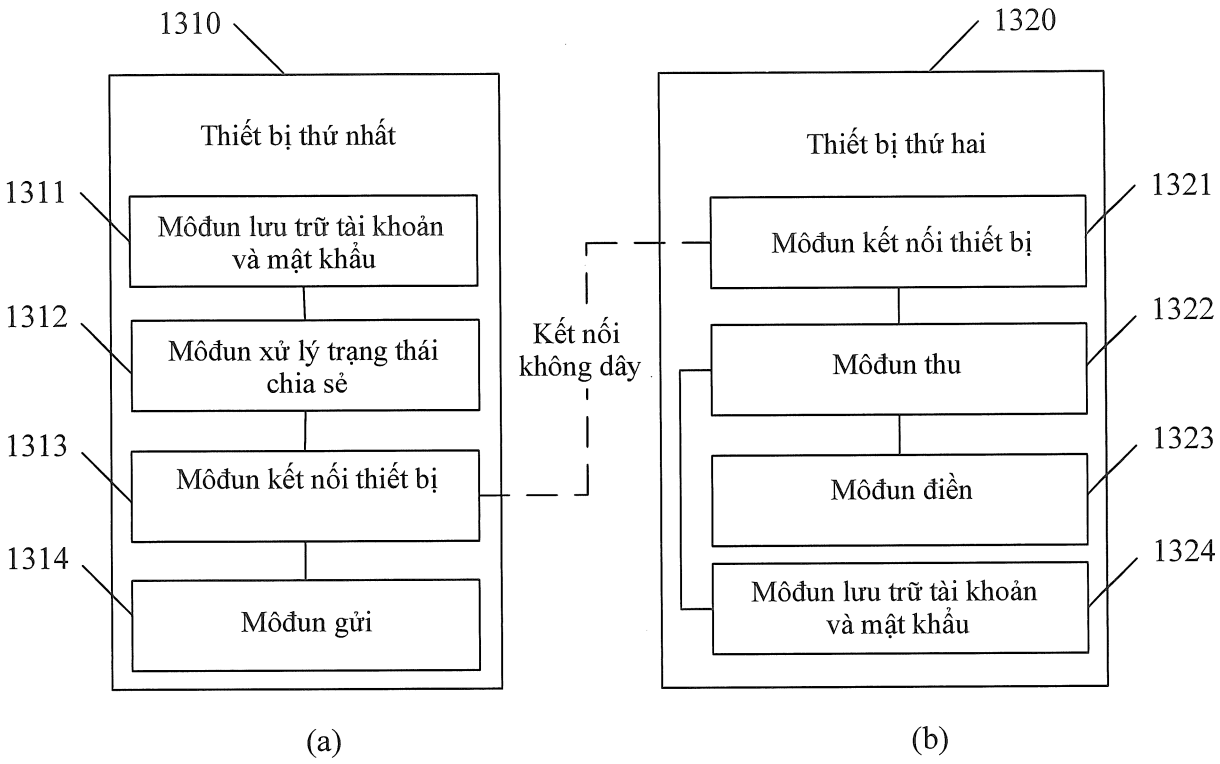

FIG. 13

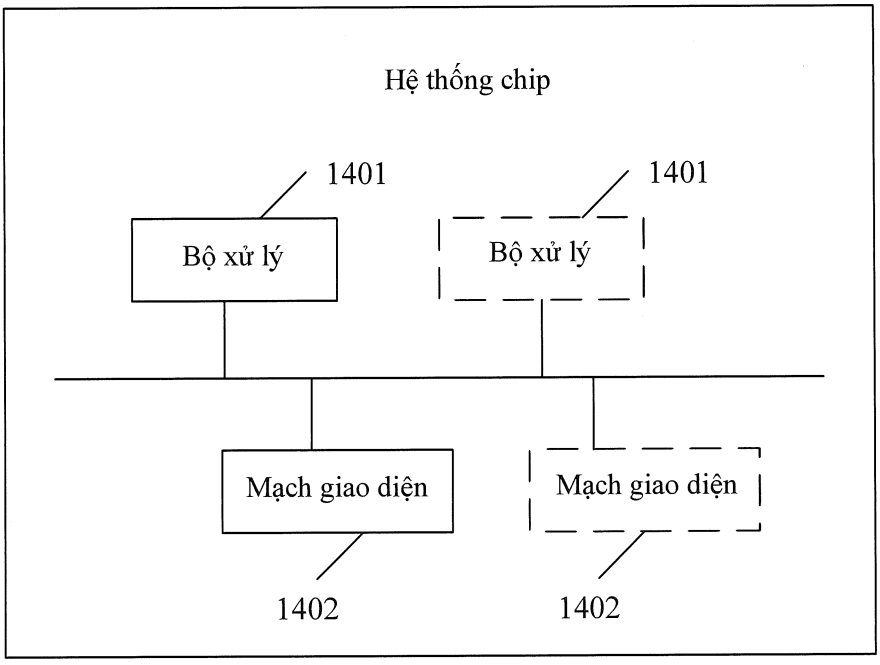

FIG. 14