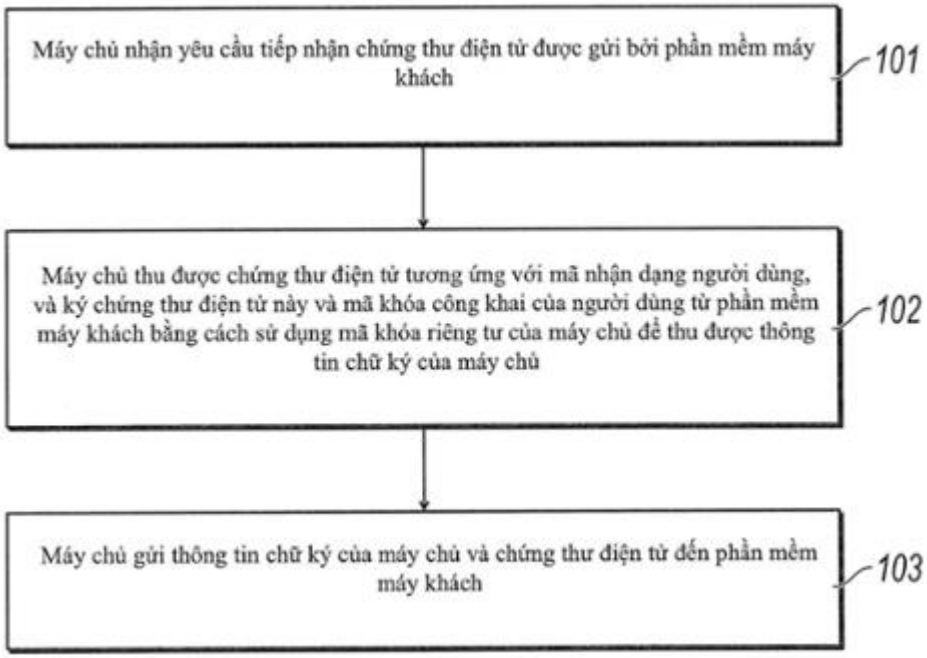
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0031024**
(51)[7] **H04L 29/06**
(13) **B**

(21) 1-2019-03432
(22) 04/12/2017
(86) PCT/CN2017/114382 04/12/2017
(87) WO 2018/107988 21/06/2018
(30) 201611154671.9 14/12/2016 CN
(45) 25/02/2022 407
(43) 25/09/2019 378A
(73) Advanced New Technologies Co., Ltd. (KY)
Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands
(72) SHEN, Lingnan (CN); CHEN, Ge (CN); LIU, Yanghui (CN); JIN, Huifeng (CN).
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP, THIẾT BỊ VÀ HỆ THỐNG XỬ LÝ CÁC MÃ VẠCH HAI CHIỀU

(57) Sáng chế đề cập đến phương pháp, thiết bị, và hệ thống xử lý các mã vạch hai chiều, liên quan đến lĩnh vực công nghệ xử lý thông tin, và chủ yếu nhằm giảm bớt vấn đề công nghệ hiện có là chứng thư điện tử được tạo dựa vào mã ngẫu nhiên tĩnh, và khi chứng thư điện tử bị sao chép hoặc bị đánh cắp thông qua chụp ảnh, tính bảo mật của chứng thư điện tử không thể được đảm bảo. Các giải pháp kỹ thuật của sáng chế gồm các bước sau: nhận, bởi máy chủ, yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, trong đó yêu cầu tiếp nhận chứng nhận điện tử gồm mã nhận dạng người dùng; nhận được chứng thư điện tử tương ứng với mã nhận dạng người dùng, và ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng của máy chủ để nhận được thông tin chữ ký của máy chủ; và gửi thông tin chữ ký của máy chủ và chứng thư điện tử tới phần mềm máy khách, để phần mềm máy khách xác minh thông tin chữ ký của máy chủ, và tạo mã vạch hai chiều dựa vào chứng thư điện tử để thiết bị đầu cuối xác minh chứng thư thực hiện xác minh chứng thư điện tử bao gồm trong mã vạch hai chiều, trong đó thiết bị đầu cuối xác minh chứng thư được tạo cấu hình để tạo chứng thư điện tử dựa vào mã nhận dạng người dùng.


Máy chủ nhận yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách
101
Máy chủ thu được chứng thư điện tử tương ứng với mã nhận dạng người dùng, và ký chứng thư điện tử này và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng tư của máy chủ để thu được thông tin chữ ký của máy chủ
102
Máy chủ gửi thông tin chữ ký của máy chủ và chứng thư điện tử đến phần mềm máy khách
103

Lĩnh vực kỹ thuật được đề cập

Sáng chế liên quan đến lĩnh vực công nghệ xử lý thông tin, và cụ thể, đến phương pháp, thiết bị, và hệ thống xử lý các mã vạch hai chiều.

Tình trạng kỹ thuật của sáng chế

Hiện tại, có một số trường hợp áp dụng xác minh chứng thư trong công việc và cuộc sống hàng ngày, ví dụ, thẻ căn cước, thẻ ngân hàng, vé xe buýt, vé buổi hòa nhạc, và thẻ kiểm soát truy cập. Trong một số trường hợp áp dụng, việc xác minh chứng thư chỉ cần được hoàn thành bằng cách sử dụng các thực thể xác định, ví dụ, vé xe buýt, vé buổi hòa nhạc, và thẻ kiểm soát truy cập. Đối với một số tình huống xác minh chứng thư với yêu cầu bảo mật tương đối cao, thực thể xác định và thông tin cá nhân cần được sử dụng cùng nhau để hoàn tất xác minh, ví dụ, thẻ ngân hàng và truy cập vân tay ở nhà/công ty.

Trên thực tế, trong trường hợp áp dụng với việc xác minh chứng thư chỉ cần được hoàn thành bằng cách sử dụng một thực thể xác định, xác minh chứng thư có thể được hoàn thành bằng cách nhận được thực thể xác định tương ứng. Ví dụ, người dùng có thể mua vé giấy xe buýt hoặc vé giấy buổi hòa nhạc từ cửa sổ vé, và có thể lên xe buýt hoặc đi đến buổi hòa nhạc sau khi hoàn tất xác minh tại nơi soát vé. Chế độ xác minh này phụ thuộc vào thực thể xác định (vé xe buýt hoặc vé buổi hòa nhạc), và yêu cầu người dùng mang theo thực thể xác định. Tuy nhiên, nếu thực thể xác định bị mất hoặc bị hư hỏng, quá trình hủy đăng ký hoặc đăng kí lại thực thể xác định là phức tạp.

Đối với trường hợp áp dụng có yêu cầu bảo mật tương đối cao, bảo mật có thể được đảm bảo bằng một thiết bị phụ trợ xác nhận bảo mật bổ sung, ví dụ, bàn phím bảo mật hoặc đơn vị nhận dạng vân tay. Như vậy, chi phí sử dụng tăng lên. Mặc dù phương pháp này có thể ngăn chặn rò rỉ thông tin cá nhân, mối đe dọa rò rỉ thông tin cá nhân vẫn tồn tại.

Trong cả hai trường hợp áp dụng đã nêu, có một vấn đề là việc xác minh chứng thư ít thuận tiện với sự bảo mật tương đối thấp, và chi phí của bên xuất bản chứng thư

tương đối cao. Để giảm bớt vấn đề đã nêu, người dùng trong công nghệ hiện nay có thể mua chứng thư điện tử trực tuyến. Một chuỗi mã ngẫu nhiên được ghi lại trong chứng thư điện tử, và trong quá trình xác minh chứng thư, có thể hoàn tất xác minh bằng cách xác minh mã ngẫu nhiên trong chứng thư điện tử, do đó nâng cao sự thuận tiện và bảo mật của việc xác minh chứng thư và giảm chi phí xuất bản của bên xuất bản chứng thư. Tuy nhiên, mã ngẫu nhiên tĩnh được sử dụng trong chứng thư điện tử, và nếu chứng thư điện tử bị sao chép hoặc đánh cắp thông qua chụp ảnh, sự bảo mật của chứng thư điện tử không thể được đảm bảo.

Bản chất kỹ thuật của sáng chế

Theo khắc phục vấn đề này, sáng chế đề xuất phương pháp, thiết bị, và hệ thống xử lý các mã vạch hai chiều, và chủ yếu nhằm giảm bớt vấn đề công nghệ hiện có mà chứng thư điện tử được tạo ra dựa trên mã ngẫu nhiên tĩnh, và khi chứng thư điện tử bị sao chép hoặc đánh cắp thông qua chụp ảnh, sự bảo mật của chứng thư điện tử không thể được đảm bảo.

Theo khía cạnh thứ nhất của sáng chế, sáng chế đề xuất phương pháp xử lý các mã vạch hai chiều, bao gồm bước: nhận, bởi máy chủ, yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, ở đây yêu cầu tiếp nhận chứng thư điện tử bao gồm mã nhận dạng người dùng; nhận được chứng thư điện tử tương ứng với mã nhận dạng người dùng, và ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng của máy chủ để nhận được thông tin chữ ký của máy chủ; và gửi thông tin chữ ký của máy chủ và chứng thư điện tử tới phần mềm máy khách, để phần mềm máy khách xác minh thông tin chữ ký của máy chủ, và tạo mã vạch hai chiều dựa trên chứng thư điện tử để thiết bị đầu cuối xác minh chứng thư thực hiện xác minh chứng thư điện tử bao gồm trong mã vạch hai chiều, ở đây thiết bị đầu cuối xác minh chứng thư được tạo cấu hình để tạo chứng thư điện tử dựa vào mã nhận dạng người dùng.

Theo khía cạnh thứ hai của sáng chế, sáng chế đề xuất phương pháp xử lý các mã vạch hai chiều, bao gồm bước: nhận, bởi phần mềm máy khách, thông tin chữ ký của máy chủ và chứng thư điện tử được gửi bởi máy chủ, ở đây thông tin chữ ký của máy chủ nhận được bởi máy chủ bằng cách ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng của

máy chủ; xác minh thông tin chữ ký của máy chủ để nhận được chứng thư điện tử; nhận được mã khóa công khai của người dùng tương ứng với mã khóa công khai của người dùng, và ký chứng thư điện tử bằng cách sử dụng mã khóa công khai của người dùng để nhận được thông tin chữ ký của phần mềm máy khách; và tạo mã vạch hai chiều dựa trên thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng, để thiết bị đầu cuối xác minh chứng thư thực hiện xác minh chứng thư điện tử bao gồm trong mã vạch hai chiều dựa vào thông tin bảo mật định trước và mã khóa công khai của người dùng, ở đây thông tin bảo mật định trước có thời hạn hiệu lực, và thiết bị đầu cuối xác minh chứng thư được tạo cấu hình để tạo chứng thư điện tử dựa vào mã nhận dạng người dùng.

Theo khía cạnh thứ ba của sáng chế, sáng chế đề xuất phương pháp xử lý các mã vạch hai chiều, bao gồm các bước sau: nhận được, bởi thiết bị đầu cuối xác minh chứng thư, mã vạch hai chiều trong phần mềm máy khách, ở đây mã vạch hai chiều được tạo bởi phần mềm máy khách dựa trên thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng, thông tin chữ ký của phần mềm máy khách nhận được bởi phần mềm máy khách bằng cách ký chứng thư điện tử, và thông tin chữ ký của máy chủ nhận được bởi máy chủ bằng cách ký chứng thư điện tử và mã khóa công khai của người dùng; xác minh khoảng thời gian hiệu lực của thông tin bảo mật định trước, và xác minh thông tin chữ ký của phần mềm máy khách và thông tin chữ ký của máy chủ; nếu việc xác minh mỗi thông tin trong số thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, và thông tin chữ ký của máy chủ thành công, nhận được thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử để xác minh; và nếu việc xác minh thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử thành công, xác định rằng sự xác minh chứng thư điện tử thành công.

Theo khía cạnh thứ tư của sáng chế, sáng chế đề xuất máy chủ, bao gồm: đơn vị nhận, được tạo cấu hình để nhận yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, ở đây yêu cầu tiếp nhận chứng thư điện tử gồm mã nhận dạng người dùng; đơn vị tiếp nhận thứ nhất, được tạo cấu hình để nhận được chứng thư điện tử tương ứng với mã nhận dạng của người dùng nhận được bởi đơn vị nhận; đơn vị ký, được tạo cấu hình để ký chứng thư điện tử và mã khóa công khai của người dùng từ

phần mềm máy khách bằng cách sử dụng mã khóa riêng của máy chủ để có được thông tin chữ ký của máy chủ; và đơn vị gửi, được tạo cấu hình để gửi thông tin chữ ký của máy chủ có được bởi đơn vị ký và chứng thư điện tử nhận được bởi đơn vị tiếp nhận thứ nhất tới phần mềm máy khách, để phần mềm máy khách xác minh thông tin chữ ký của máy chủ trong thời gian có hiệu lực của mã khóa công khai của người dùng, và tạo mã vạch hai chiều dựa vào chứng thư điện tử để thiết bị đầu cuối xác minh chứng thư thực hiện xác minh chứng thư điện tử bao gồm trong mã vạch hai chiều, ở đây thiết bị đầu cuối xác minh chứng thư được tạo cấu hình để tạo chứng thư điện tử dựa vào mã nhận dạng người dùng.

Theo khía cạnh thứ năm của sáng chế, sáng chế đề xuất phần mềm máy khách, bao gồm các phần sau: đơn vị nhận thứ nhất, được tạo cấu hình để nhận thông tin chữ ký của máy chủ và chứng thư điện tử được gửi bởi máy chủ, ở đây thông tin chữ ký của máy chủ nhận được bởi máy chủ bằng cách ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng của máy chủ; đơn vị xác minh chữ ký, được tạo cấu hình để xác minh thông tin chữ ký của máy chủ để thu được chứng thư điện tử; đơn vị tiếp nhận, được tạo cấu hình để nhận được mã khóa của người dùng tương ứng với mã khóa công khai của người dùng; đơn vị ký, được tạo cấu hình để ký chứng thư điện tử bằng cách sử dụng mã khóa của người dùng thu được bởi đơn vị tiếp nhận để có được thông tin chữ ký của phần mềm máy khách; và đơn vị kiến tạo, được tạo cấu hình để tạo mã vạch hai chiều dựa vào thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng, để thiết bị đầu cuối xác minh chứng thư thực hiện xác minh chứng thư điện tử bao gồm trong mã vạch hai chiều dựa vào thông tin bảo mật định trước và mã khóa công khai của người dùng, ở đây thông tin bảo mật định trước có thời hạn hiệu lực, và thiết bị đầu cuối xác minh chứng thư được tạo cấu hình để tạo chứng thư điện tử dựa vào mã nhận dạng người dùng.

Theo khía cạnh thứ sáu của sáng chế, sáng chế đề xuất thiết bị đầu cuối xác minh chứng thư, gồm các phần sau: đơn vị tiếp nhận thứ nhất, được tạo cấu hình để nhận được mã vạch hai chiều trong phần mềm máy khách, ở đây mã vạch hai chiều được tạo bởi phần mềm máy khách dựa vào thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và

mã khóa công khai của người dùng, thông tin chữ ký của phần mềm máy khách có được bởi phần mềm máy khách bằng cách ký chứng thư điện tử, và thông tin chữ ký của máy chủ có được bởi máy chủ bằng cách ký chứng thư điện tử và mã khóa công khai của người dùng; đơn vị xác minh thứ nhất, được tạo cấu hình để xác minh khoảng thời gian hiệu lực của thông tin bảo mật định trước nhận được bởi đơn vị tiếp nhận thứ nhất; đơn vị xác minh thứ hai, được tạo cấu hình để xác minh thông tin chữ ký của phần mềm máy khách và thông tin chữ ký của máy chủ; đơn vị xác minh thứ ba, được tạo cấu hình để có được thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử để xác minh khi việc xác minh của đơn vị xác minh thứ nhất về mỗi thông tin trong số thông tin chữ ký của phần mềm máy khách và thông tin chữ ký của máy chủ thành công; và đơn vị xác định, được tạo cấu hình để xác định rằng sự xác minh chứng thư điện tử thành công khi việc xác minh của đơn vị xác minh thứ ba về thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử thành công.

Theo khía cạnh thứ bảy của sáng chế, sáng chế đề xuất hệ thống xử lý các mã vạch hai chiều, và hệ thống bao gồm các phần sau: phần mềm máy khách, được tạo cấu hình để gửi yêu cầu tiếp nhận chứng thư điện tử đến máy chủ, trong đó yêu cầu tiếp nhận chứng thư điện tử bao gồm mã nhận dạng người dùng; máy chủ, được tạo cấu hình để nhận yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, và nhận chứng thư điện tử từ thiết bị đầu cuối xác minh chứng thư dựa vào mã nhận dạng người dùng; và thiết bị đầu cuối xác minh chứng thư, được tạo cấu hình để nhận và trả lời thông tin yêu cầu tiếp nhận chứng thư điện tử được gửi bởi máy chủ, và gửi chứng thư điện tử đến máy chủ, ở đây máy chủ còn được tạo cấu hình để nhận chứng thư điện tử được gửi bởi thiết bị đầu cuối xác minh chứng thư, ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách để có được thông tin chữ ký của máy chủ, và gửi thông tin chữ ký của máy chủ và chứng thư điện tử tới phần mềm máy khách; phần mềm máy khách được định cầu hình để nhận thông tin chữ ký của máy chủ và chứng thư điện tử được gửi bởi máy chủ, xác minh thông tin chữ ký của máy chủ để thu được chứng thư điện tử, thu được mã khóa của người dùng tương ứng với mã khóa công khai của người dùng, ký chứng thư điện tử bằng cách sử dụng mã khóa của người dùng để có được thông tin chữ ký của phần mềm máy khách, và tạo mã vạch hai chiều dựa vào thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và

mã khóa công khai của người dùng; và thiết bị đầu cuối xác minh chứng thư được tạo cấu hình để nhận được mã vạch hai chiều trong phần mềm máy khách, xác minh khoảng thời gian hiệu lực của thông tin bảo mật định trước, và xác minh thông tin chữ ký của phần mềm máy khách và thông tin chữ ký của máy chủ; và nếu việc xác minh mỗi thông tin trong số thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, và thông tin chữ ký của máy chủ thành công, nhận được thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử để xác minh, và nếu việc xác minh thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử thành công, xác định rằng sự xác minh chứng thư điện tử thành công.

Theo các giải pháp kỹ thuật trước, và theo phương pháp, thiết bị, và hệ thống xử lý các mã vạch hai chiều được đề xuất theo sáng chế, sau khi nhận được yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, máy chủ ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng của máy chủ để có được thông tin chữ ký của máy chủ và gửi thông tin chữ ký của máy chủ và chứng thư điện tử đến phần mềm máy khách. Phần mềm máy khách nhận thông tin chữ ký của máy chủ và chứng thư điện tử được gửi bởi máy chủ, xác minh thông tin chữ ký của máy chủ, sau khi xác minh thông tin chữ ký thành công, ký chứng thư điện tử, và tạo mã vạch hai chiều dựa vào thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng. Sau khi có được mã vạch hai chiều, thiết bị đầu cuối xác minh chứng thư có thể xác minh thông tin chữ ký của máy chủ, thông tin chữ ký của phần mềm máy khách, và thông tin bảo mật định trước trong mã vạch hai chiều để xác định xem chứng thư điện tử có bị giả mạo trong quá trình truyền hay không, để đảm bảo tính bảo mật của chứng thư điện tử trong quá trình sử dụng.

Phần mô tả chỉ đơn thuần là tổng quan các giải pháp kỹ thuật của sáng chế. Để hiểu rõ hơn các phương tiện kỹ thuật của sáng chế để thực hiện nội dung của bản mô tả kỹ thuật và để làm cho, các mục đích đã nêu và các mục đích khác, các tính năng, và các thuận lợi của sáng chế dễ hiểu hơn, sau đây liệt kê các phương án cụ thể của sáng chế.

Mô tả vắn tắt các hình vẽ

Bằng cách đọc các phần mô tả chi tiết về các phương án ưu tiên sau đây, người có hiểu biết trung bình về lĩnh vực kỹ thuật này hiểu được các hiệu quả và lợi ích khác. Các hình vẽ kèm theo chỉ đơn thuần được sử dụng để thể hiện các mục đích của các phương án ưu tiên, nhưng không được coi là giới hạn đối với sáng chế. Ngoài ra, số chỉ dẫn giống nhau được sử dụng để biểu thị phần tương tự trên tất cả các hình vẽ kèm theo. Trong các hình vẽ kèm theo:

Fig.1 là sơ đồ khung minh họa sự tương tác giữa phần mềm máy khách, máy chủ, và thiết bị đầu cuối xác minh chứng thư, theo một phương án của sáng chế;

Fig.2 là lưu đồ minh họa phương pháp thứ nhất để xử lý các mã vạch hai chiều, theo một phương án của sáng chế;

Fig.3 là lưu đồ minh họa phương pháp thứ hai để xử lý các mã vạch hai chiều, theo một phương án của sáng chế;

Fig.4 là lưu đồ minh họa phương pháp thứ ba để xử lý các mã vạch hai chiều, theo một phương án của sáng chế;

Fig.5 là giản đồ minh họa bước ký và xác minh chữ ký, theo một phương án của sáng chế;

Fig.6 là lưu đồ minh họa phương pháp thứ tư để xử lý các mã vạch hai chiều, theo một phương án của sáng chế;

Fig.7 là lưu đồ minh họa phương pháp thứ năm để xử lý các mã vạch hai chiều, theo một phương án của sáng chế;

Fig.8 là sơ đồ khối minh họa máy chủ, theo một phương án của sáng chế;

Fig.9 là sơ đồ khối minh họa máy chủ khác, theo một phương án của sáng chế;

Fig.10 là sơ đồ khối minh họa phần mềm máy khách, theo một phương án của sáng chế;

Fig.11 là sơ đồ khối minh họa phần mềm máy khách khác, theo một phương án của sáng chế;

Fig.12 là sơ đồ khối minh họa thiết bị đầu cuối xác minh chứng thư, theo một phương án của sáng chế;

Fig.13 là sơ đồ khối minh họa thiết bị đầu cuối xác minh chứng thư khác, theo một phương án của sáng chế; và

Fig.14 là một sơ đồ khối minh họa hệ thống xử lý các mã vạch hai chiều, theo một phương án của sáng chế.

Mô tả chi tiết sáng chế

Phần sau đây mô tả chi tiết hơn các phương án ví dụ của sáng chế có tham chiếu đến các hình vẽ kèm theo. Mặc dù các hình vẽ kèm theo thể hiện các phương án ví dụ của sáng chế, cần hiểu rằng sáng chế có thể được thực hiện theo nhiều hình thức khác nhau và không bị giới hạn bởi các phương án được mô tả ở đây. Thay vào đó, những phương án này được đưa ra để người có hiểu biết trung bình về lĩnh vực kỹ thuật này hiểu rõ hơn về sáng chế và phạm vi của sáng chế.

Để giảm bớt vấn đề công nghệ hiện có mà thông tin chứng thư điện tử trong mã vạch hai chiều có thể dễ dàng bị rò rỉ, các phương án của sáng chế đề xuất phương pháp xử lý các mã vạch hai chiều. Phương pháp được thực hiện nhờ sự vận hành của máy chủ, phần mềm máy khách và thiết bị đầu cuối xác minh chứng thư. Thiết bị đầu cuối xác minh chứng thư ít nhất có thể tạo và truyền dữ liệu, để truyền chứng thư điện tử đã tạo đến máy chủ, và có thể nhận được dữ liệu, và xác minh dữ liệu, để nhận được chứng thư điện tử từ mã vạch hai chiều trong phần mềm máy khách và xác minh xem liệu chứng thư điện tử có đúng hay không. Máy chủ ít nhất có thể truyền và nhận dữ liệu, để nhận chứng thư điện tử được gửi bởi thiết bị đầu cuối xác minh chứng thư, và gửi chứng thư điện tử đến phần mềm máy khách, thực hiện truyền dữ liệu. Phần mềm máy khách ít nhất có thể trao đổi dữ liệu với máy chủ, để nhận chứng thư điện tử được gửi bởi máy chủ và có thể tạo hình ảnh, để tạo mã vạch hai chiều, v.v. dựa trên thông tin chứng thư điện tử.

Trước khi phương pháp trong các phương án được mô tả, để dễ hiểu, sơ đồ khung minh họa sự tương tác giữa phần mềm máy khách, máy chủ, và thiết bị đầu cuối xác minh chứng thư, theo một phương án của sáng chế được cung cấp trước tiên, như được thể hiện trên Fig.1. Theo phương án của sáng chế, sau khi tạo chứng thư điện tử dựa trên mã nhận dạng người dùng (như số thẻ căn cước, số điện thoại di động, hoặc địa chỉ email), thiết bị đầu cuối xác minh chứng thư gửi chứng thư điện tử đến máy chủ và máy chủ có quyền truy cập vào chứng thư điện tử được tạo bởi thiết bị đầu cuối

xác minh chứng thư. Sau khi nhận được yêu cầu tiếp nhận chứng thư điện tử từ phần mềm máy khách, máy chủ gửi chứng thư điện tử cho phần mềm máy khách để phần mềm máy khách tạo mã vạch hai chiều dựa trên chứng thư điện tử để thiết bị đầu cuối xác minh chứng thư thực hiện xác minh.

Cần lưu ý là, theo phương án này của sáng chế, mô tả được thực hiện bằng cách sử dụng ví dụ rằng chứng thư điện tử được mang trong trong mã vạch hai chiều. Tuy nhiên, về mặt lý thuyết, chứng thư điện tử cũng có thể phụ thuộc vào một phương tiện khác, ví dụ, phần mềm máy khách có khả năng NFC ví dụ như khả năng SE hoặc khả năng HCE. Theo phương án của sáng chế, mô tả được thực hiện bằng cách sử dụng một ví dụ là chứng thư điện tử được mang trong mã vạch hai chiều, bởi vì đối với người dùng chứng thư điện tử và thiết bị đầu cuối xác minh chứng thư, mã vạch hai chiều có các yêu cầu tương đối thấp về các thiết bị phần cứng được sử dụng và các thiết bị phần cứng tương đối phổ biến. Tuy nhiên, cần phải rõ ràng rằng phương pháp mô tả như vậy không nhằm áp đặt một giới hạn rằng chứng thư điện tử chỉ có thể được mang bằng cách sử dụng mã vạch hai chiều.

Phần sau đây trước hết đề cập đến phương pháp xử lý các mã vạch hai chiều được thực hiện ở phía máy chủ dựa trên giản đồ được thể hiệnị trên Fig.1. Như được thể hiện trên Fig.2, phương pháp bao gồm các bước sau.

101. Máy chủ nhận yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách.

Sau khi đăng nhập thành công vào máy chủ, phần mềm máy khách gửi yêu cầu tiếp nhận chứng thư điện tử đến máy chủ, trong đó yêu cầu tiếp nhận chứng thư điện tử bao gồm mã nhận dạng người dùng, để máy chủ tìm kiếm thông tin chứng thư điện tử tương ứng dựa trên mã nhận dạng người dùng. Trong quy trình thực hiện cụ thể, chứng thư điện tử có thể bao gồm nhưng không giới hạn các nội dung sau: chứng thư điện tử tương ứng với vé máy bay, vé xe buýt, vé tàu, vé hòa nhạc, thẻ ngân hàng, thẻ kiểm soát truy cập, vé vào cổng công viên, thẻ căn cước, phiếu giảm giá của thương gia, thẻ thành viên, bằng lái xe, thẻ kiểm soát truy cập giấy phép lái xe, hoặc thẻ xe buýt.

Trong quy trình thực hiện cụ thể, phần mềm máy khách là một ứng dụng (APP) được cài đặt trong một thiết bị điện tử hoặc trang web. Trước khi phần mềm máy khách tương tác với máy chủ, phần mềm máy khách có thể đăng ký với máy chủ dựa

trên mã nhận dạng người dùng và mã nhận dạng người dùng có thể bao gồm nhưng không giới hạn ở thẻ căn cước, tên thật phù hợp với thẻ căn cước, số điện thoại di động, địa chỉ email, tên tài khoản, v.v. Trong quá trình đăng ký, có thể đặt mật khẩu đăng nhập để đăng nhập vào máy chủ, và sau khi đăng ký và đăng nhập thành công, phần mềm máy khách có thể được kết nối và giao tiếp với máy chủ.

102. Máy chủ nhận được chứng thư điện tử tương ứng với mã nhận dạng người dùng, và ký chứng thư điện tử và mã khóa công khai của phần mềm máy khách bằng cách sử dụng mã khóa riêng của máy chủ để có được thông tin chữ ký của máy chủ.

Máy chủ được mô tả theo phương án này không tạo ra chứng thư điện tử. Sau khi nhận yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, máy chủ nhận được chứng thư điện tử tương ứng với mã nhận dạng người dùng từ thiết bị đầu cuối xác minh chứng thư mà tạo chứng thư điện tử. Máy chủ đóng vai trò là cầu nối giữa bên sử dụng chứng thư điện tử (phần mềm máy khách) và thiết bị đầu cuối xác minh chứng thư điện tử (thiết bị đầu cuối xác minh chứng thư) và chịu trách nhiệm chuyển tiếp chứng thư điện tử được tạo bởi thiết bị đầu cuối xác minh chứng thư đến bên sử dụng chứng thư điện tử. Điều cần lưu ý là, giả thuyết rằng máy chủ được mô tả theo phương án này của sáng chế đáp ứng các yêu cầu quy định quốc gia, máy chủ cần phải được cấp phép bởi thiết bị đầu cuối xác minh chứng thư để truy cập thiết bị đầu cuối xác minh chứng thư.

Để ngăn chặn chứng thư điện tử bị giả mạo trong quá trình truyền của máy chủ và phần mềm máy khách, trước khi máy chủ phản hồi yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, máy chủ cần phải ký mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng của máy chủ để có thông tin chữ ký của máy chủ. Theo phương án này của sáng chế, mã khóa công khai của người dùng từ phần mềm máy khách được ký để phần mềm máy khách và máy chủ có thể xác minh các tính đồng nhất của nhau, thực hiện xác thực bảo mật trên thông tin nhận dạng, và đảm bảo rằng thông tin trong quá trình truyền dữ liệu không bị giả mạo. Máy chủ ký chứng thư điện tử bằng cách sử dụng mã khóa riêng của máy chủ để tính toàn vẹn của chứng thư điện tử ban đầu có thể được xác định.

Ngoài ra, khi ký mã khóa công khai của người dùng và chứng thư điện tử, máy chủ có thể sử dụng thêm thông tin chữ ký của máy chủ thu được khi máy chủ ký chứng

thư điện tử và mã khóa công khai của người dùng là thông tin thuộc tính của mã vạch hai chiều được tạo khi phần mềm máy khách tạo mã vạch hai chiều sau đó, để đảm bảo rằng chứng thư điện tử được truyền bởi phần mềm máy khách được gửi bởi máy chủ, được xác minh bởi phần mềm máy khách, và được cấp quyền và đáng tin cậy. Như vậy, chứng thư điện tử không thể bị giả mạo hoặc từ chối.

103. Máy chủ gửi thông tin chữ ký của máy chủ và chứng thư điện tử tới phần mềm máy khách.

Như vậy, phần mềm máy khách xác minh chứng thư điện tử đã được ký, và tạo mã vạch hai chiều dựa trên chứng thư điện tử, để thiết bị đầu cuối xác minh chứng thư thực hiện xác minh chứng thư điện tử bao gồm trong mã vạch hai chiều. Thiết bị đầu cuối xác minh chứng thư được tạo cấu hình để tạo ra chứng thư điện tử dựa trên mã nhận dạng người dùng.

Theo phương pháp xử lý mã vạch hai chiều được đề xuất theo phương án này của sáng chế, sau khi nhận được yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, máy chủ ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng của máy chủ để có được thông tin chữ ký của máy chủ, và gửi thông tin chữ ký của máy chủ và chứng thư điện tử đến phần mềm máy khách. Phần mềm máy khách nhận thông tin chữ ký của máy chủ và chứng thư điện tử được gửi bởi máy chủ, xác minh thông tin chữ ký của máy chủ, sau khi xác minh về thông tin chữ ký thành công, ký chứng thư điện tử, và tạo mã vạch hai chiều dựa vào thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử và mã khóa công khai của người dùng. Sau khi có được mã vạch hai chiều, thiết bị đầu cuối xác minh chứng thư có thể xác minh thông tin chữ ký của máy chủ, thông tin chữ ký của phần mềm máy khách, và thông tin bảo mật định trước trong mã vạch hai chiều để xác định xem chứng thư điện tử có bị giả mạo trong quá trình truyền hay không, để đảm bảo tính bảo mật của chứng thư điện tử trong quá trình sử dụng.

Mô tả thêm về phương pháp được thể hiện trên Fig.1, để đảm bảo tính hợp lệ của mã nhận dạng người dùng của phần mềm máy khách và đảm bảo rằng mã nhận dạng người dùng của phần mềm máy khách không bị giả mạo trong quá trình truyền nội dung, trong bước 102, chứng thư điện tử và mã khóa công khai của người dùng từ

phần mềm máy khách có thể được ký bằng cách sử dụng mã khóa riêng của máy chủ trong các phương pháp sau, v.v.. Ví dụ:

Phương pháp 1: Máy chủ gán mã khóa chữ ký người dùng vào chứng thư điện tử, và ký chứng thư điện tử và mã khóa công khai thứ nhất của người dùng bằng cách sử dụng mã khóa riêng của máy chủ, trong đó mã khóa chữ ký người dùng được gán bao gồm mã khóa công khai thứ nhất của người dùng.

Khi máy chủ nhận được yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, nếu không có mã khóa công khai của người dùng từ phần mềm máy khách thu được từ yêu cầu tiếp nhận chứng thư điện tử, máy chủ sẽ tạm thời gán một cặp mã khóa chữ ký người dùng cho chứng thư điện tử để xác thực mã nhận dạng người dùng của phần mềm máy khách và do đó đảm bảo rằng chứng thư điện tử không bị giả mạo, trong đó các mã khóa chữ ký người dùng được gán bao gồm một mã khóa công khai thứ nhất của người dùng và một mã khóa riêng của người dùng thứ nhất; và ký mã khóa riêng của người dùng thứ nhất bằng cách sử dụng mã khóa riêng của máy chủ để thực hiện xác thực bảo mật trên thông tin chữ ký của máy chủ sau khi nhận được thông tin chữ ký của máy chủ.

Vì các mã khóa chữ ký người dùng được máy chủ gán tạm thời cho chứng thư điện tử, nếu các mã khóa chữ ký người dùng không thu được bởi phần mềm máy khách, thông tin chữ ký của máy chủ trong máy chủ không thể được xác minh. Để giảm bớt vấn đề đã nêu, nếu máy chủ ký chứng thư điện tử và mã khóa công khai thứ nhất của người dùng của phần mềm máy khách bằng cách sử dụng phương pháp 1, khi máy chủ gửi thông tin chữ ký của máy chủ và chứng thư điện tử đến phần mềm máy khách, máy chủ cần gửi đồng bộ các mã khóa chữ ký người dùng được gán cho chứng thư điện tử tới phần mềm máy khách để phần mềm máy khách có thể xác minh thông tin chữ ký của máy chủ dựa trên các mã khóa chữ ký người dùng.

Theo một quy trình thực hiện cụ thể, sau khi nhận được mã khóa chữ ký người dùng được máy chủ gán tạm thời cho chứng thư điện tử, và xác minh thông tin chữ ký của máy chủ dựa vào các mã khóa chữ ký người dùng, phần mềm máy khách có thể trực tiếp loại bỏ các mã khóa chữ ký người dùng, hoặc có thể sử dụng mã khóa chữ ký người dùng như mã khóa của người dùng thông thường và mã khóa công khai của

người dùng từ phần mềm máy khách. Các phương án không bị giới hạn ở phương án này của sáng chế.

Phương pháp 2: Máy chủ nhận được mã khóa công khai thứ hai của người dùng được gửi bởi phần mềm máy khách, và ký mã khóa công khai thứ hai của người dùng và chứng thư điện tử bằng cách sử dụng mã khóa riêng của máy chủ.

Theo phương án này, để nhận biết danh tính của phần mềm máy khách, khi gửi yêu cầu tiếp nhận chứng thư điện tử đến máy chủ, phần mềm máy khách sẽ gửi đồng bộ mã khóa công khai thứ hai của người dùng của phần mềm máy khách đến máy chủ, để máy chủ thực hiện xác thực danh tính trên phần mềm máy khách, và máy chủ ký mã khóa công khai thứ hai của người dùng và chứng thư điện tử của phần mềm máy khách bằng cách sử dụng mã khóa riêng của máy chủ. Sau khi nhận mã khóa công khai thứ hai của người dùng và chứng thư điện tử đã được ký, phần mềm máy khách chỉ có thể nhận được thông tin chứng thư điện tử sau khi xác minh chữ ký thành công để đảm bảo rằng chứng thư điện tử không bị giả mạo.

Cần lưu ý là, mã khóa công khai thứ nhất của người dùng và mã khóa công khai thứ hai của người dùng được mô tả theo phương án này của sáng chế được sử dụng để phân biệt các mã khóa công khai của người dùng khác nhau của phần mềm máy khách. "Thứ nhất" và "thứ hai" không có các ý nghĩa khác và không nhằm mục đích giới hạn số lượng, mức độ ưu tiên, v.v. của các mã khóa công khai của người dùng. Phương pháp đặt tên mã khóa công khai của người dùng trong phần mềm máy khách không bị giới hạn ở phương án này của sáng chế.

Để dễ mô tả, trong phần mô tả sau theo phương án của sáng chế, mô tả được thực hiện bằng cách sử dụng một ví dụ là mã khóa công khai của người dùng và mã khóa riêng của người dùng là các khóa mã bất đối xứng. Tuy nhiên, cần phải rõ ràng rằng mã khóa công khai của người dùng và mã khóa riêng của người dùng không bị giới hạn ở các khóa mã bất đối xứng, mà có thể là các khóa mã đối xứng. Các phương án không bị giới hạn ở phương án này của sáng chế.

Để hỗ trợ việc hiểu về quá trình ký của máy chủ, sau đây sử dụng một ví dụ là máy chủ ký mã khóa công khai của người dùng và chứng thư điện tử để mô tả. Quy trình cụ thể bao gồm các bước sau: sau khi thu được mã khóa công khai của người dùng và chứng thư điện tử, máy chủ có thể thực hiện hoạt động băm trên mã khóa

công khai của người dùng và chứng thư điện tử bằng cách sử dụng giải thuật băm để lấy giá trị băm, và sau đó ký giá trị băm bằng cách sử dụng mã khóa riêng của máy chủ để có được thông tin chữ ký của máy chủ. Một giải thuật (như hoạt động băm) được sử dụng trong quá trình ký không bị giới hạn ở phương án này của sáng chế.

Sau khi ký chứng thư điện tử và mã khóa công khai của người dùng, máy chủ gửi chứng thư điện tử, mã khóa công khai của người dùng đã ký, và chứng thư điện tử đã ký cho phần mềm máy khách, để phần mềm máy khách xác minh thông tin chữ ký của máy chủ và đảm bảo rằng chứng thư điện tử không bị giả mạo bởi người dùng cố tình làm hại trong quá trình truyền dữ liệu. Ngoài ra, máy chủ cần phát đi thêm mã khóa công khai tương ứng với mã khóa riêng của máy chủ mà được sử dụng khi máy chủ có được thông tin chữ ký, để phần mềm máy khách và thiết bị đầu cuối xác minh chứng thư nhận mã khóa công khai được phát đi bởi máy chủ, và sử dụng mã khóa công khai của máy chủ để xác minh thông tin chữ ký.

Hơn nữa, máy chủ được mô tả theo phương án này của sáng chế đóng vai trò là cầu nối mang phần mềm máy khách và bên xác minh thông tin chứng thư. Máy chủ chịu trách nhiệm xác thực tính hợp lệ của người dùng, và ngoài ra, máy chủ có thể xác minh thêm tính hợp lệ của việc sử dụng chứng thư điện tử. Trong các quy trình sử dụng cụ thể, các chứng thư điện tử tương ứng với các loại dịch vụ khác nhau, và các loại dịch vụ khác nhau được giới hạn bằng cách sử dụng các tiêu chuẩn dịch vụ khác nhau. Ví dụ, khi chứng thư điện tử là vé máy bay, dịch vụ vé máy bay bao gồm thời gian khởi hành của máy bay (trường hợp áp dụng này chỉ có thể là tình huống với một máy bay cất cánh đúng giờ mà không bị chậm trễ). Ngoài ra, khi chứng thư điện tử là vé buổi hòa nhạc, dịch vụ vé cũng bao gồm thời gian bắt đầu, thời gian vào cửa, v.v. của buổi hòa nhạc. Do đó, theo phương án này của sáng chế, trước khi thu được chứng thư điện tử tương ứng dựa trên mã nhận dạng người dùng, máy chủ cần phân tích cú pháp yêu cầu tiếp nhận chứng thư điện tử, có được thời gian hiệu lực của dịch vụ bao gồm trong yêu cầu tiếp nhận chứng thư điện tử, và xác minh xem thời gian hiệu lực của dịch vụ có tuân thủ với tiêu chuẩn dịch vụ hay không. Khi thời gian hiệu lực của dịch vụ tuân thủ tiêu chuẩn dịch vụ, máy chủ thu được chứng thư điện tử tương ứng với mã nhận dạng người dùng. Khi thời gian hiệu lực của dịch vụ không tuân thủ tiêu chuẩn dịch vụ, máy chủ sẽ trả về phần mềm máy khách, thông tin nhắc nhở cho biết rằng không có chứng thư điện tử tương ứng.

Để hiểu rõ hơn, phần sau đây mô tả thời gian hiệu lực của dịch vụ và tiêu chuẩn dịch vụ với các ví dụ. Ví dụ, giả sử rằng chứng thư điện tử là dịch vụ vé xe buýt, thời gian để thiết bị đầu cuối xác minh chứng thư để bán các vé xe buýt trước 7 ngày, và ngày hiện tại là ngày 1 tháng 11, năm 2016. Người dùng gửi yêu cầu tiếp nhận chứng thư điện tử đến máy chủ bằng cách sử dụng phần mềm máy khách vào ngày 1 tháng 11, năm 2016, thời gian hiệu lực của dịch vụ bao gồm trong yêu cầu là đến ngày 20 tháng 11, năm 2016, và thời gian hiệu lực tối đa của chứng thư điện tử được tạo bởi thiết bị đầu cuối xác minh chứng thư là đến ngày 8 tháng 11, năm 2016. Do đó, máy chủ có thể xác định rằng thời gian hiệu lực của dịch vụ không tuân thủ với tiêu chuẩn dịch vụ. Mô tả đã nêu chỉ là một ví dụ. Phương án này của sáng chế không đặt giới hạn về loại dịch vụ của chứng thư điện tử, thời gian hiệu lực của dịch vụ, tiêu chuẩn dịch vụ, v.v.

Hơn nữa, trong bước 102, chứng thư điện tử tương ứng với mã nhận dạng người dùng có thể thu được theo các phương pháp sau nhưng không giới hạn ở các phương pháp này. Ví dụ:

Phương pháp 1: Sau khi thiết bị đầu cuối xác minh chứng thư tạo chứng thư điện tử dựa trên mã nhận dạng người dùng, chứng thư điện tử được đồng bộ hóa bởi thiết bị đầu cuối xác minh chứng thư được nhận.

Theo phương án này, sau khi tạo chứng thư điện tử, thiết bị đầu cuối xác minh chứng thư chủ động gửi chứng thư điện tử đã tạo đến máy chủ. Trong một quy trình thực hiện cụ thể, để giúp quản lý số lượng chứng thư điện tử, máy chủ có thể tạo cục bộ danh sách định trước, ở đây danh sách định trước được sử dụng để ghi lại mối quan hệ ánh xạ giữa mã nhận dạng người dùng và chứng thư điện tử. Sau khi nhận được chứng thư điện tử được đồng bộ hóa bởi thiết bị đầu cuối xác minh chứng thư, máy chủ sẽ ghi lại mối quan hệ ánh xạ mới nhận được giữa chứng thư điện tử và mã nhận dạng người dùng trong danh sách định trước. Sau khi gửi chứng thư điện tử đến phần mềm máy khách, máy chủ có thể xóa chứng thư điện tử đã được gửi thành công ra khỏi danh sách định trước, để giảm tài nguyên bị chiếm giữ bởi máy chủ.

Phương pháp 2: thông tin yêu cầu để thu được chứng thư điện tử được gửi đến thiết bị đầu cuối xác minh chứng thư được dựa trên mã nhận dạng người dùng, để thu được chứng thư điện tử.

Theo phương án này, máy chủ được sử dụng để chuyển tiếp. Máy chủ yêu cầu chứng thư điện tử từ thiết bị đầu cuối xác minh chứng thư dựa trên mã nhận dạng người dùng trong yêu cầu tiếp nhận chứng thư điện tử chỉ khi nhận được yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, và sau đó chuyển tiếp chứng thư điện tử có được cho phần mềm máy khách. Phương pháp để thu được chứng thư điện tử của máy chủ không bị giới hạn ở phương án này của sáng chế.

Hơn nữa, như một phần mô tả thêm và một phần mở rộng của phương pháp đã nêu, phương án của sáng chế còn đề xuất phương pháp xử lý mã vạch hai chiều. Theo phương pháp này, để dễ mô tả, mô tả chủ yếu được thực hiện bằng cách sử dụng ví dụ rằng phần mềm máy khách là ALIPAY và chứng thư điện tử là vé xem hòa nhạc điện tử. Cần phải rõ ràng rằng một phương pháp mô tả như vậy không nhằm áp đặt một giới hạn mà phần mềm máy khách được mô tả theo phương án này của sáng chế chỉ có thể là ALIPAY. Như được thể hiện trên Fig.3, phương pháp này bao gồm các bước sau:

201. Máy chủ nhận được yêu cầu tiếp nhận vé xem hòa nhạc điện tử được gửi bởi ALIPAY, trong đó yêu cầu tiếp nhận vé xem hòa nhạc điện tử bao gồm số điện thoại di động và thời gian hiệu lực của dịch vụ.

Trong thực tế, thời gian hiệu lực của dịch vụ có thể là thời gian đặt vé xem hòa nhạc điện tử hoặc có thể là thời gian bắt đầu của vé xem hòa nhạc điện tử hoặc có thể là bất kỳ lúc nào không liên quan đến vé xem hòa nhạc điện tử. Thời gian hiệu lực của dịch vụ không bị giới hạn ở phương án này của sáng chế.

202a. Máy chủ phân tích cú pháp yêu cầu tiếp nhận vé xem hòa nhạc điện tử và có được thời gian hiệu lực của dịch vụ bao gồm trong yêu cầu tiếp nhận vé xem hòa nhạc điện tử.

Ví dụ, thời gian hiệu lực của dịch vụ trong yêu cầu là thời gian bắt đầu buổi hòa nhạc: 16:00 ngày 20 tháng 9, năm 2016, và ngày hiện tại là ngày 1 tháng 9, năm 2016.

203a. Xác minh xem thời gian hiệu lực của dịch vụ có tuân thủ tiêu chuẩn dịch vụ hay không.

Nếu thời gian hiệu lực của dịch vụ tuân thủ tiêu chuẩn dịch vụ, bước 204 được thực hiện. Nếu thời gian hiệu lực của dịch vụ không tuân thủ tiêu chuẩn dịch vụ, bước 205 được thực hiện.

Theo phương án này của sáng chế, vé xem hòa nhạc điện tử được nhận theo kịch bản sau: khi vé giấy cho buổi hòa nhạc bị mất hoặc bị hỏng, có thể vào buổi hòa nhạc bằng cách xác minh vé xem hòa nhạc điện tử, mà không cần đăng kí lại vé xem hòa nhạc bằng giấy. Nó làm giảm quá trình đăng kí lại vé mệt mỏi. Trong ví dụ này, có thể chỉ định rằng tiêu chuẩn dịch vụ là có thể lấy vé xem hòa nhạc điện tử trong vòng 30 ngày trước khi mở buổi hòa nhạc, hoặc có thể lấy vé xem hòa nhạc điện tử trong vòng nửa giờ sau khi bắt đầu buổi hòa nhạc. Bước 202b có thể được thực hiện miễn là thời gian hiệu lực của dịch vụ tuân thủ tiêu chuẩn dịch vụ. Thời gian hiệu lực được mô tả trong bước 201 là thời gian bắt đầu buổi hòa nhạc vào ngày 20 tháng 9, năm 2016 là tuân thủ quy cách dịch vụ, vì vậy bước 202b được thực hiện.

202b. Máy chủ phân tích cú pháp yêu cầu tiếp nhận vé xem hòa nhạc điện tử, và nhận được số điện thoại trong yêu cầu tiếp nhận vé xem hòa nhạc điện tử.

203b. Xác nhận tính hợp lệ của số điện thoại di động.

Nếu số điện thoại di động hợp lệ, bước 204 được thực hiện. Nếu số điện thoại di động không hợp lệ, bước 205 được thực hiện.

Trong bước hiện tại, xác minh xem số điện thoại di động trong yêu cầu có phù hợp với số điện thoại di động trong máy chủ hay không.

Cần lưu ý là, khi bước 202a và bước 202b được thực hiện, không có trình tự giữa hai bước. Ngoài ra, các bước tiếp theo chỉ tiếp tục được thực hiện sau khi việc xác minh thời gian hiệu lực của dịch vụ và xác minh mã nhận dạng người dùng (số điện thoại di động) thành công.

204. Máy chủ có được vé xem hòa nhạc điện tử tương ứng với số điện thoại di động, và ký mã khóa công khai của người dùng của ALIPAY và chứng thư điện tử bằng cách sử dụng mã khóa riêng của máy chủ để thu được thông tin chữ ký của máy chủ.

Dựa vào các loại dịch vụ khác nhau, chứng thư điện tử có các chi tiết tương ứng. Vé xem hòa nhạc điện tử được sử dụng là một ví dụ. Vé xem hòa nhạc điện tử bao gồm địa điểm tổ chức buổi hòa nhạc, chỗ đứng, số chỗ ngồi cụ thể, tên buổi hòa nhạc, giá cả, v.v. Các phương án không bị giới hạn ở phương án này của sáng chế.

205. Chặn yêu cầu tiếp nhận vé xem hòa nhạc điện tử, và gửi lời nhắc lỗi yêu cầu tới ALIPAY.

206. Gửi thông tin chữ ký của máy chủ và vé xem hòa nhạc điện tử tới ALIPAY.

207. Phát đi mã khóa công khai tương ứng với mã khóa riêng của máy chủ, để ALIPAY xác minh thông tin chữ ký dựa trên mã khóa công khai của máy chủ.

Như phần mở rộng cho phương pháp được thể hiện trên Fig.3, sau khi thiết bị điện tử (ví dụ, điện thoại di động) được cài đặt ALIPAY bị mất, người dùng có thể chuyển đổi điện thoại di động và sau khi đăng nhập thành công vào ALIPAY, tiếp tục sử dụng chứng thư điện tử, ngăn chặn việc hủy đăng ký, đăng ký lại, v.v. sau khi chứng thư giấy bị mất. Trường hợp áp dụng như vậy chỉ có thể được áp dụng sau khi ALIPAY thực hiện xác minh chữ ký thành công bằng cách sử dụng mã khóa riêng của người dùng, mã khóa công khai của máy chủ, và chứng thư điện tử. Nếu ALIPAY chưa xác minh thông tin chữ ký của máy chủ, ALIPAY cần xác minh thông tin chữ ký của máy chủ dựa trên mã khóa công khai của máy chủ và thu được chứng thư điện tử sau khi xác minh thành công. Theo phương án tùy chọn của sáng chế, để xác định thêm rằng chứng thư điện tử không bị rò rỉ, sau khi máy chủ gửi thông tin chữ ký của máy chủ và chứng thư điện tử đến phần mềm máy khách, khoảng thời gian hiệu lực xác minh đối với mã khóa công khai của máy chủ có thể được cài đặt. Như vậy, phần mềm máy khách phải hoàn tất xác minh thông tin chữ ký của máy chủ trong một thời gian nhất định. Nếu khoảng thời gian hiệu lực xác minh đối với mã khóa công khai của máy chủ hết hạn, thông tin chữ ký của máy chủ không thể được xác minh.

Hơn nữa, phương án của sáng chế còn đề xuất phương pháp xử lý các mã vạch hai chiều. Phương pháp được áp dụng cho phía phần mềm máy khách được thể hiện trên Fig.1. Như được thể hiện trên Fig.4, phương pháp bao gồm các bước sau.

301. Phần mềm máy khách nhận thông tin chữ ký của máy chủ và chứng thư điện tử được gửi bởi máy chủ.

Sau khi phần mềm máy khách đăng nhập thành công vào máy chủ bằng cách sử dụng tên tài khoản người dùng và mật khẩu đăng nhập, phần mềm máy khách gửi yêu cầu tiếp nhận chứng thư điện tử đến máy chủ. Máy chủ trả lời yêu cầu tiếp nhận chứng thư điện tử. Để ngăn chứng thư điện tử bị giả mạo trong quá trình truyền, máy chủ gửi

thông tin chữ ký của máy chủ và thông tin điện tử đến phần mềm máy khách, để xác minh tính hợp lệ của danh tính của phần mềm máy khách. Thông tin chữ ký của máy chủ được máy chủ có được bằng cách ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng của máy chủ. Đối với các mô tả liên quan về việc lấy thông tin chữ ký của máy chủ, có thể tham khảo các phần mô tả chi tiết theo phương án đã nêu. Các chi tiết được bỏ qua để đơn giản theo phương án này của sáng chế.

302. Phần mềm máy khách xác minh thông tin chữ ký của máy chủ để thu được chứng thư điện tử.

Ví dụ, thông tin chữ ký của máy chủ có được bằng cách ký mã khóa công khai của người dùng và chứng thư điện tử bởi máy chủ, và việc xác minh thông tin chữ ký của máy chủ được thực hiện bởi phần mềm máy khách được sử dụng làm ví dụ cho phân mô tả chi tiết. Fig.5 là giản đồ minh họa quá trình ký và xác minh chữ ký, theo một phương án của sáng chế. Sau khi nhận được mã khóa công khai của người dùng và chứng thư điện tử, máy chủ thực hiện thao tác băm trên mã khóa công khai của người dùng và chứng thư điện tử bằng cách sử dụng thuật toán băm để lấy giá trị băm thứ nhất, và mã hóa giá trị băm thứ nhất bằng cách sử dụng mã khóa riêng của máy chủ để có được thông tin chữ ký của máy chủ. Máy chủ gửi thông tin chữ ký của máy chủ và chứng thư điện tử đến phần mềm máy khách. Sau khi nhận thông tin chữ ký của máy chủ và chứng thư điện tử, phần mềm máy khách trích xuất chứng thư điện tử, và thực hiện thao tác băm trên chứng thư điện tử để có được giá trị băm thứ hai. Ngoài ra, phần mềm máy khách sử dụng mã khóa công khai của máy chủ để giải mã thông tin chữ ký của máy chủ để có được giá trị băm thứ nhất, và so sánh giá trị băm thứ nhất thu được thông qua việc giải mã với giá trị băm thứ hai có được thông qua tính toán. Nếu giá trị băm thứ nhất giống với giá trị băm thứ hai, điều đó cho thấy rằng chứng thư điện tử không bị giả mạo trong quá trình truyền, và chứng thư điện tử có thể được sử dụng trực tiếp sau khi thu được chứng thư điện tử. Nếu giá trị băm thứ nhất khác với giá trị băm thứ hai, điều đó cho thấy rằng thông tin điện tử bị giả mạo trong quá trình truyền dữ liệu và có thể có nguy cơ rò rỉ thông tin. Cần lưu ý là Fig.5 chỉ là một ví dụ, và nội dung cụ thể của thông tin chữ ký của máy chủ không bị giới hạn.

303. Phần mềm máy khách thu được mã khóa của người dùng tương ứng với mã khóa công khai của người dùng, và ký chứng thư điện tử bằng cách sử dụng mã khóa của người dùng để có được thông tin chữ ký của phần mềm máy khách.

Phần mềm máy khách tạo chứng thư điện tử được mang trong mã vạch hai chiều. Để ngăn chặn chứng thư điện tử bị giả mạo bất hợp pháp và để ngăn không cho thông tin chứng thư điện tử bị rò rỉ, phần mềm máy khách cần phải ký chứng thư điện tử bằng cách sử dụng mã khóa riêng của người dùng, để có được thông tin chữ ký của phần mềm máy khách. Khi phần mềm máy khách sử dụng thông tin chữ ký của phần mềm máy khách làm thông tin thuộc tính của mã vạch hai chiều được tạo ra, thiết bị đầu cuối xác minh chứng thư có thể xác minh thông tin chữ ký của phần mềm máy khách, và xác thực thêm tính hợp lệ của phần mềm máy khách.

Về phương pháp triển khai chữ ký cụ thể, có thể tham chiếu đến mô tả chi tiết trên Fig.5. Các chi tiết được bỏ qua để đơn giản hóa theo phương án này của sáng chế.

304. Phần mềm máy khách tạo mã vạch hai chiều dựa trên thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng.

Khi phần mềm máy khách và bên xác minh chứng thư điện tử thực hiện truyền dữ liệu (chứng thư điện tử) khoảng cách ngắn, để đảm bảo an toàn của việc truyền chứng thư điện tử, thông tin xác thực có thể được thêm vào mã vạch hai chiều được tạo ra, và thông tin xác thực có thể bao gồm nhưng không giới hạn ở thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, và thông tin bảo mật định trước. Thiết bị đầu cuối xác minh chứng thư có thể xác minh thông tin chữ ký của phần mềm máy khách, để xác định rằng chứng thư điện tử cần xác minh được gửi bởi phần mềm máy khách. Ngoài ra, thiết bị đầu cuối xác minh chứng thư có thể xác minh thông tin chữ ký của máy chủ để xác định rằng chứng thư điện tử trong mã vạch hai chiều được gửi bởi máy chủ, để đảm bảo rằng chứng thư điện tử không bị giả mạo.

Theo phương án này của sáng chế, thông tin bảo mật định trước được sử dụng làm cài đặt động của mã vạch hai chiều, và được sử dụng làm chứng thư để thiết lập sự truyền dữ liệu "đáng tin cậy" giữa phần mềm máy khách và thiết bị đầu cuối xác minh chứng thư. Trước khi nhận được mã vạch hai chiều được gửi bởi phần mềm máy khách, thiết bị đầu cuối xác minh chứng thư thực hiện xác minh tính hợp lệ và bảo mật

của thông tin bảo mật định trước để đảm bảo tính bảo mật của chứng thư điện tử được gửi bởi phần mềm máy khách. Thông tin bảo mật định trước có thể bao gồm nhưng không giới hạn ở các nội dung sau: thông tin mật khẩu động, thông tin thời gian, thông tin mã ngẫu nhiên, v.v. Các` phương án không bị giới hạn ở phương án này của sáng chế.

Ví dụ, như được mô tả ở đây, thời gian hệ thống hiện tại được sử dụng đối với thông tin bảo mật định trước. Nếu phần mềm máy khách tạo mã vạch hai chiều lúc 08:00, có thể xác định rằng thông tin bảo mật định trước là 08/00. Nếu phần mềm máy khách tạo mã vạch hai chiều lúc 10:21, có thể xác định rằng thông tin bảo mật định trước là 10/21. Ví dụ đã nêu được mô tả bằng cách sử dụng thông tin bảo mật định trước dưới dạng thời gian hệ thống hiện tại. Tuy nhiên, rõ ràng là phương pháp mô tả như vậy không nhằm áp đặt giới hạn rằng thông tin bảo mật định trước được mô tả theo phương án này của sáng chế chỉ có thể là thời gian hệ thống hiện tại của phần mềm máy khách.

Cần lưu ý là, khi mã vạch hai chiều được tạo ra, mã khóa công khai của người dùng từ phần mềm máy khách không được phát rộng, và thay vào đó, mã khóa công khai của người dùng được sử dụng trực tiếp làm thông tin thuộc tính của mã vạch hai chiều được tạo ra. Điều này có thể có hiệu quả giảm tổng chi phí thêm và chi phí của phần mềm máy khách.

Theo phương pháp xử lý mã vạch hai chiều được đề xuất theo phương án này của sáng chế, sau khi nhận được yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, máy chủ ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng của máy chủ để có được thông tin chữ ký của máy chủ, và gửi thông tin chữ ký của máy chủ và chứng thư điện tử đến phần mềm máy khách. Phần mềm máy khách nhận thông tin chữ ký của máy chủ và chứng thư điện tử được gửi bởi máy chủ, xác minh thông tin chữ ký của máy chủ, sau khi xác minh thông tin chữ ký thành công, ký chứng thư điện tử, và tạo mã vạch hai chiều dựa vào thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng. Sau khi có được mã vạch hai chiều, thiết bị đầu cuối xác minh chứng thư có thể xác minh thông tin chữ ký của máy chủ, thông tin chữ ký của phần mềm máy khách, và thông tin bảo mật định trước trong mã vạch hai chiều để xác định

xem chứng thư điện tử có bị giả mạo trong quá trình truyền hay không, để đảm bảo tính bảo mật của chứng thư điện tử trong quá trình sử dụng.

Theo phương án này của sáng chế, khi đạt được mã khóa của người dùng tương ứng với mã khóa công khai của người dùng, phần mềm máy khách nhận mã khóa chữ ký người dùng mà được gửi bởi máy chủ và được gán cho chứng thư điện tử, ở đây mã khóa chữ ký người dùng bao gồm mã khóa công khai thứ nhất của người dùng và mã khóa thứ nhất của người dùng, mã khóa của người dùng và mã khóa công khai của người dùng là các khóa mã bất đối xứng, và phần mềm máy khách nhận được mã khóa công khai thứ nhất của người dùng trong mã khóa chữ ký người dùng mà được máy chủ gán cho chứng thư điện tử. Trong một phương án khác của sáng chế, khi thu được mã khóa của người dùng tương ứng với mã khóa công khai của người dùng, phần mềm máy khách có thể thu được mã khóa thứ hai của người dùng được tạo ra bởi phần mềm máy khách và tương ứng với mã khóa công khai của người dùng. Phương pháp để phần mềm máy khách thu được mã khóa của người dùng không bị giới hạn ở phương án này của sáng chế.

Hơn nữa, khi xác minh thông tin chữ ký của máy chủ, phương pháp bao gồm các bước sau: nhận và lưu trữ mã khóa công khai của máy chủ được phát quảng bá bởi máy chủ, và xác minh thông tin chữ ký của máy chủ dựa trên mã khóa công khai của máy chủ và chứng thư điện tử.

Khi xác định rằng máy chủ ký mã khóa công khai thứ hai của người dùng được tạo bởi phần mềm máy khách, phần mềm máy khách xác minh thông tin chữ ký của máy chủ dựa trên mã khóa công khai của máy chủ, chứng thư điện tử, và mã khóa công khai thứ nhất của người dùng.

Khi xác định rằng máy chủ ký mã khóa công khai thứ nhất của người dùng được gán bởi máy chủ cho chứng thư điện tử, phần mềm máy khách xác minh thông tin chữ ký của máy chủ dựa vào mã khóa công khai của máy chủ, chứng thư điện tử và mã khóa công khai thứ hai của người dùng. Đối với quy trình mà phần mềm máy khách xác minh thông tin chữ ký của máy chủ, có thể tham chiếu đến mô tả chi tiết trên Fig.5. Các phương án không bị giới hạn ở phương án này của sáng chế.

Cần lưu ý là, khi gửi chứng thư điện tử đến phần mềm máy khách, máy chủ cần ký chứng thư điện tử và mã khóa công khai của người dùng để có được thông tin

chữ ký của máy chủ, để khi phần mềm máy khách tạo ra mã vạch hai chiều sau đó, thông tin chữ ký của máy chủ có thể được sử dụng làm thông tin thuộc tính của mã vạch hai chiều được tạo ra. Người dùng sử dụng mã khóa riêng của người dùng để đăng ký thông tin được gửi bởi máy chủ, để đảm bảo tính chính xác của thông tin gốc của chứng thư điện tử, và đảm bảo rằng mã khóa công khai của người dùng là hợp lệ và đáng tin cậy khi được xác minh và không thể bị giả mạo hoặc từ chối.

Hơn nữa, có thể có nhiều mã khóa chữ ký người dùng (bao gồm mã khóa thứ nhất của người dùng được tạo bởi phần mềm máy khách, và mã khóa thứ hai của người dùng được máy chủ gán cho chứng thư điện tử) trong phần mềm máy khách. Do đó, phần mềm máy khách có thể ký chứng thư điện tử bằng cách sử dụng bất kỳ mã khóa riêng nào của người dùng mà khớp với phần mềm máy khách. Ví dụ, phần mềm máy khách có thể ký chứng thư điện tử bằng cách sử dụng mã khóa thứ nhất của người dùng, hoặc có thể ký chứng thư điện tử bằng cách sử dụng mã khóa thứ hai của người dùng. Các phương án không bị giới hạn ở phương án này của sáng chế.

Để đảm bảo hơn tính bảo mật của chứng thư điện tử, khi phần mềm máy khách tạo mã vạch hai chiều, phần mềm máy khách cũng sử dụng thông tin chữ ký của phần mềm máy khách trong quy trình. Do đó, thiết bị đầu cuối xác minh chứng thư thực hiện xác minh thông tin chữ ký của phần mềm máy khách, để đảm bảo rằng chứng thư điện tử được tạo bởi phần mềm máy khách và phần mềm máy khách được cấp quyền và đáng tin cậy để sử dụng chứng thư điện tử, và chứng thư điện tử không thể bị giả mạo hoặc bị từ chối. Mã vạch hai chiều có thể được tạo dựa vào thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng theo phương pháp sau: cài đặt khoảng thời gian hiệu lực của thông tin bảo mật định trước, và tạo ra mã vạch hai chiều dựa vào thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, mã khóa công khai của người dùng, thời gian có hiệu lực của thông tin bảo mật định trước, và mã nhận dạng người dùng.

Cần lưu ý là, theo phương án này của sáng chế, khi tạo mã vạch hai chiều, phần mềm máy khách cần sử dụng mã nhận dạng người dùng làm thông tin thuộc tính của mã vạch hai chiều được tạo ra. Điều này có thể được áp dụng cho trường hợp áp dụng với thiết bị đầu cuối xác minh chứng thư yêu cầu hệ thống tên thật của người

dùng. Ví dụ, khi chứng thư điện tử là chứng thư tương ứng với vé máy bay, vé xe buýt, vé tàu, thẻ ngân hàng, v.v., khi thiết bị đầu cuối xác minh chứng thư thực hiện xác minh chứng thư điện tử như vậy, thẻ nhận dạng người dùng có thể được sử dụng để kiểm tra điều kiện hệ thống tên thật, để hỗ trợ hoàn thành xác minh, thỏa mãn yêu cầu trong một số trường hợp áp dụng yêu cầu hệ thống tên thật.

Với giải pháp tùy chọn theo phương án này của sáng chế, trong một số trường hợp bảo mật cao, khi mã vạch hai chiều được tạo ra, để ngăn không cho mã vạch hai chiều bị sử dụng bởi người dùng có dã tâm khi điện thoại di động hoặc máy tính bảng bị mất hoặc trong một khoảng thời gian ngắn khi mã vạch hai chiều bị bẻ khóa, dấu hiệu sinh trắc học của người sử dụng chứng thư điện tử có thể được thêm vào mã vạch hai chiều. Ví dụ, một dấu hiệu sinh trắc học như dấu vân tay của người sử dụng chứng thư điện tử bao gồm trong mã vạch hai chiều. Khi thiết bị đầu cuối xác minh chứng thư thực hiện xác minh mã vạch hai chiều, việc xác minh trên dấu hiệu sinh trắc học của người đó là cần thiết để đảm bảo hơn tính bảo mật của chứng thư điện tử.

Hơn nữa, theo phương án đã nêu, các chức năng cụ thể và các phương án cụ thể của máy chủ và phần mềm máy khách để xử lý mã vạch hai chiều đã được mô tả chi tiết. Thiết bị đầu cuối xác minh chứng thư được thể hiện trên Fig.1 cần thực hiện sự xác minh trên chứng thư điện tử được tạo ra phụ thuộc vào mã vạch hai chiều. Phần sau đây đề cập đến phương pháp xử lý các mã vạch hai chiều. Phương pháp được áp dụng cho thiết bị đầu cuối xác minh chứng thư. Như được thể hiện trên Fig.6, phương pháp bao gồm các bước sau.

401. Thiết bị đầu cuối xác minh chứng thư có được mã vạch hai chiều trong phần mềm máy khách.

Mã vạch hai chiều được tạo bởi phần mềm máy khách dựa trên thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng, thông tin chữ ký của phần mềm máy khách có được bởi phần mềm máy khách bằng cách ký chứng thư điện tử, và thông tin chữ ký của máy chủ có được bởi máy chủ bằng cách ký chứng thư điện tử và mã khóa công khai của người dùng.

Thiết bị đầu cuối xác minh chứng thư có thể nhận được mã vạch hai chiều trong phần mềm máy khách theo phương pháp sau, v.v. Ví dụ, mã vạch hai chiều có được

bằng cách sử dụng chỉ dẫn thu thập dữ liệu định trước. Các phương pháp liên quan đến chỉ dẫn thu thập dữ liệu định trước bao gồm phương pháp quét, phương pháp dao động đầu truyền dữ liệu, phương pháp kích hoạt khóa, phương pháp kích hoạt giọng nói,và phương pháp trượt dọc theo dấu.

Theo phương pháp chỉ dẫn thu thập dữ liệu định trước theo phương án này của sáng chế, các phương pháp chỉ dẫn thu thập dữ liệu định trước khác với phương pháp quét cần được thiết đặt trước khi truyền dữ liệu. Ví dụ, phương pháp lắc đầu truyền dữ liệu được thiết đặt như sau: lắc hai lần theo cùng một hướng, lắc trái và phải hai lần, và lắc lên xuống ba lần. Phương pháp kích hoạt khóa mã bao gồm các cách sau: thiết bị đầu cuối xác minh chứng thư giám sát trạng thái kích hoạt của khóa mã định trước và khóa mã định trước có thể là khóa mã vật lý, hoặc có thể là khóa mã ảo. Khi phần mềm máy khách kích hoạt khóa mã định trước, thiết bị đầu cuối xác minh chứng thư có thể thu được mã vạch hai chiều được hiển thị trong phần mềm máy khách. Nếu phần mềm máy khách là phần mềm máy khách màn hình cảm ứng, sau khi thiết bị đầu cuối xác minh chứng thư xác định trước phương pháp trượt dọc theo dấu, thiết bị đầu cuối xác minh chứng thư sẽ theo dõi trạng thái trượt của màn hình cảm ứng trong phần mềm máy khách và khi người dùng phần mềm máy khách kích hoạt hoạt động trượt trên màn hình, có được mã vạch hai chiều. Chỉ dẫn thu thập dữ liệu định trước được mô tả ở trên, và loại chỉ dẫn thu thập dữ liệu định trước trong thực tế không bị giới hạn ở phương án này của sáng chế.

402. Thiết bị đầu cuối xác minh chứng thư thực hiện xác minh khoảng thời gian hiệu lực của thông tin bảo mật định trước, và xác minh thông tin chữ ký của phần mềm máy khách và thông tin chữ ký của máy chủ.

Thiết bị đầu cuối xác minh chứng thư phân tích cú pháp mã vạch hai chiều nhận được, có được thông tin bảo mật định trước và chứng thư điện tử bao gồm trong mã vạch hai chiều, và xác minh khoảng thời gian hiệu lực của thông tin bảo mật định trước và tính hợp lệ của khoảng thời gian hiệu lực của dịch vụ trong chứng thư điện tử. Ví dụ, giả sử rằng thông tin bảo mật định trước là thời gian hệ thống hiện tại của phần mềm máy khách, thông tin bảo mật định trước là 10/21, và khoảng thời gian hiệu lực của thông tin bảo mật định trước là 60 giây. Thiết bị đầu cuối xác minh chứng thư có được sự khác biệt thời gian giữa thời gian hệ thống hiện tại và thông tin bảo mật định trước, và xác định xem khoảng thời gian hiệu lực có lớn hơn 60 giây hay không. Nếu

xác định được rằng khoảng thời gian hiệu lực lớn hơn 60 giây, thiết bị đầu cuối xác minh chứng thư xác định rằng mã vạch hai chiều không hợp lệ. Mô tả đã nêu là một ví dụ. Ngoài ra, khoảng thời gian hiệu lực của thông tin bảo mật định trước có thể được đặt thành hai phút, v.v. Khoảng thời gian hiệu lực của thông tin bảo mật định trước không bị giới hạn ở phương án này của sáng chế.

Các phương án về thiết bị đầu cuối xác minh chứng thư để xác minh thông tin chữ ký của phần mềm máy khách và thông tin chữ ký của máy chủ, các tham chiếu có thể được thực hiện theo phương pháp được thể hiện trên Fig.5. Các chi tiết được bỏ qua để đơn giản theo phương án này của sáng chế.

403. Nếu việc xác minh mỗi thông tin trong số thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, và thông tin chữ ký của máy chủ thành công, nhận được thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử để xác minh.

Về việc xác minh thời gian hiệu lực của dịch vụ, có thể tham khảo các phần mô tả liên quan trong các phương án đã nêu. Các chi tiết được bỏ qua để đơn giản theo phương án này của sáng chế.

404. Nếu việc xác minh về thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử thành công, xác định rằng sự xác minh chứng thư điện tử thành công.

Theo phương pháp xử lý mã vạch hai chiều được đề xuất theo phương án này của sáng chế, sau khi nhận yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, máy chủ ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng của máy chủ để có được thông tin chữ ký của máy chủ, và gửi thông tin chữ ký của máy chủ và chứng thư điện tử đến phần mềm máy khách. Phần mềm máy khách nhận thông tin chữ ký của máy chủ và chứng thư điện tử được gửi bởi máy chủ, xác minh thông tin chữ ký của máy chủ, sau khi xác minh thông tin chữ ký thành công, ký chứng thư điện tử, và tạo mã vạch hai chiều dựa trên thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng. Sau khi nhận được mã vạch hai chiều, thiết bị đầu cuối xác minh chứng thư có thể xác minh thông tin chữ ký của máy chủ, thông tin chữ ký của phần mềm máy khách, và thông tin bảo mật định trước trong mã vạch hai chiều để xác định

xem chứng thư điện tử có bị giả mạo trong quá trình truyền hay không, để đảm bảo tính bảo mật của chứng thư điện tử trong quá trình sử dụng.

Hơn nữa, như một phần mở rộng cho phương pháp được thể hiện trên Fig.6, theo phương án này của sáng chế, tất cả các bước của phương pháp đều được thực hiện dựa trên chứng thư điện tử được tạo bởi thiết bị đầu cuối xác minh chứng thư. Do đó, theo phương án này của sáng chế, trước khi mã vạch hai chiều trong phần mềm máy khách có được, thiết bị đầu cuối xác minh chứng thư điện tử tạo ra chứng thư điện tử dựa trên mã nhận dạng người dùng, và nhu cầu tạo ra chứng thư điện tử có thể bao gồm nhưng không giới hạn ở nội dung sau. Ví dụ, sau khi người dùng mua vé từ cửa sổ vé, hệ thống vé tạo ra thông tin chứng thư điện tử bên cạnh việc tạo chứng thư giấy, và phản hồi thông tin chứng thư điện tử đến máy chủ. Như vậy, máy chủ có thể gửi chứng thư điện tử đến phần mềm máy khách. Ngoài ra, sau khi người dùng mua vé điện tử trên trang web bán vé, chứng thư điện tử tương ứng với vé điện tử được tạo và sau đó được gửi đến máy chủ. Theo phương án này của sáng chế, không có hạn chế về việc liệu thiết bị đầu cuối xác minh chứng thư có cung cấp vé giấy sau khi tạo chứng thư điện tử hay không. Theo phương án này của sáng chế, chứng thư điện tử nhằm ngăn chặn các hoạt động đăng kí lại phức tạp đối với chứng thư giấy sau khi chứng thư giấy bị mất hoặc bị hỏng. Ngoài ra, tính bảo mật của chứng thư điện tử có thể được đảm bảo khi thiết bị đầu cuối xác minh chứng thư thu được chứng thư điện tử được mang theo trong mã vạch hai chiều động.

Sau khi thiết bị đầu cuối xác minh chứng thư tạo chứng thư điện tử, chứng thư điện tử tương ứng có thể được đồng bộ hóa với máy chủ dựa trên thông tin nhận dạng người dùng để phần mềm máy khách có thể thu được chứng thư điện tử từ máy chủ. Theo một phương án khác của sáng chế, sau khi nhận được thông tin yêu cầu lấy chứng thư điện tử được gửi bởi máy chủ, thiết bị đầu cuối xác minh chứng thư gửi chứng thư điện tử đến máy chủ, trong đó thông tin yêu cầu để thu được chứng thư điện tử bao gồm mã nhận dạng người dùng.

Ngoài ra, thiết bị đầu cuối xác minh chứng thư có thể xác minh thông tin chữ ký của phần mềm máy khách và thông tin chữ ký của máy chủ theo phương pháp sau, v.v.. Ví dụ, thiết bị đầu cuối xác minh chứng thư nhận được mã khóa công khai của người dùng trong mã vạch hai chiều, và xác minh thông tin chữ ký của phần mềm máy khách dựa trên mã khóa công khai của người dùng và chứng thư điện tử. Thiết bị đầu

cuối xác minh chứng thư nhận và lưu trữ mã khóa công khai của máy chủ tương ứng với mã khóa riêng của máy chủ và được phát bởi máy chủ; và xác minh thông tin chữ ký của máy chủ dựa trên mã khóa công khai của máy chủ và chứng thư điện tử.

Ngoài ra, trong một số trường hợp áp dụng có yêu cầu bảo mật tương đối cao, phần mềm máy khách sử dụng thông tin mã nhận dạng người dùng làm thông tin thuộc tính của mã vạch hai chiều được tạo, để thiết bị đầu cuối xác minh chứng thư xác nhận thông tin nhận dạng người dùng. Ví dụ, phần mềm máy khách sử dụng thẻ căn cước người dùng làm thông tin thuộc tính của mã vạch hai chiều được tạo. Thiết bị đầu cuối xác minh chứng thư phân tích cú pháp mã vạch hai chiều, có được mã nhận dạng người dùng bao gồm trong thiết bị đầu cuối xác minh chứng thư. và xác minh mã nhận dạng người dùng. Nếu thiết bị đầu cuối xác minh chứng thư xác định rằng việc xác minh mã nhận dạng người dùng thành công, thiết bị đầu cuối xác minh chứng thư xác định rằng sự xác minh chứng thư điện tử thành công. Ví dụ, khi chứng thư điện tử trong mã vạch hai chiều là vé tàu, khi người dùng sử dụng vé tàu điện tử để đi qua cửa quay của nhà ga, thẻ căn cước người dùng có thể được xác minh cùng lúc, để hoàn thành việc xác minh chứng thư điện tử.

Hơn nữa, khi thiết bị đầu cuối xác minh chứng thư thực hiện xác minh nội dung trong mã vạch hai chiều, bất kể số lượng nội dung có trong mã vạch hai chiều, miễn là nội dung bao gồm trong mã vạch hai chiều được xác minh thành công bởi thiết bị đầu cuối xác minh chứng thư, nó chỉ ra rằng xác minh chứng thư điện tử thành công. Nếu một mục hoặc một số mục có trong mã vạch hai chiều không được xác minh, điều đó cho thấy rằng xác minh chứng thư điện tử không thành công. Ví dụ, giả sử rằng khi mã vạch hai chiều bao gồm thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, và mã nhận dạng người dùng, có thể xác định rằng chứng thư điện tử chỉ được xác minh thành công sau khi việc xác minh mỗi thông tin trong số thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, và mã nhận dạng người dùng thành công.

Như được mô tả ở trên, thiết bị đầu cuối xác minh chứng thư thực hiện xác minh chứng thư điện tử được mang theo mã vạch hai chiều, và có thể thấy sự thuận tiện và bảo mật của chứng thư điện tử trong công việc và cuộc sống hàng ngày. Mô tả đã nêu được mô tả bằng cách sử dụng một ví dụ là phần mềm máy khách bao gồm một loại chứng thư điện tử. Trong thực tế, phần mềm máy khách có thể bao gồm nhiều loại

chứng thư điện tử. Các chứng thư điện tử có thể được ghi riêng trong các mã vạch hai chiều động khác nhau, hoặc có thể được ghi trong cùng mã vạch hai chiều. Các phương án không bị giới hạn ở phương án này của sáng chế. Chứng thư điện tử có thể thay thế thông tin chứng nhận thực thể trong công nghệ hiện có, ngăn chặn rò rỉ thông tin trong chứng nhận thực thể, và giảm bớt các bước đăng kí lại hoặc hủy đăng ký rườm rà khi chứng nhận thực thể bị mất. Theo phương pháp trong phương án này của sáng chế, người dùng chỉ cần mang theo một thiết bị đầu cuối (điện thoại di động) được cài đặt với phần mềm máy khách khi đi ra ngoài, và không cần mang theo bất kỳ chứng nhận thực thể nào.

Ví dụ, người dùng A chỉ mang theo một điện thoại di động được cài đặt phần mềm máy khách, và đi xe buýt từ nhà đến công ty lúc 8:00 sáng. Người dùng có thể di chuyển thuận tiện với mã vạch hai chiều của chứng thư điện tử xe buýt trong phần mềm máy khách. Sau khi đến, người dùng có thể vào công ty với chứng thư điện tử kiểm soát truy cập, và có thể ghi dấu vào bằng cách sử dụng chứng thư điện tử. Vào lúc 11:00 sáng, người dùng A cần đến ngân hàng để xử lý dịch vụ ngân hàng, và thẻ căn cước điện tử và thẻ ngân hàng điện tử có thể được sử dụng để xử lý dịch vụ. Lúc 17:00, người dùng A cần đi đến ga xe lửa để đi công tác. Khi người dùng A đi qua cửa quay, việc xác minh tên thật có thể được thực hiện bằng cách sử dụng thẻ căn cước điện tử và vé tàu điện tử. Sau khi xác minh thành công, người dùng có thể đi tàu. Phương pháp bảo mật trước để xử lý mã vạch hai chiều được sử dụng sau khi chứng thư điện tử được xác minh. Ví dụ đã nêu nhằm minh họa sự tiện lợi và an toàn mà chứng thư điện tử mang lại cho cuộc sống và công việc, và không nhằm mục đích giới hạn một trường hợp áp dụng cụ thể của chứng thư điện tử.

Trong các phương án đã nêu, các quy trình mà máy chủ, phần mềm máy khách, và thiết bị đầu cuối xác minh chứng thư xử lý mã vạch hai chiều được mô tả chi tiết riêng biệt. Tuy nhiên, trên thực tế, máy chủ, phần mềm máy khách, và thiết bị đầu cuối xác minh chứng thư là không thể thiếu trong việc xác minh mã vạch hai chiều. Trong các phương án sau đây, máy chủ, phần mềm máy khách, và thiết bị đầu cuối xác minh chứng thư được tóm tắt và mô tả. Như được thể hiện trên Fig.7, phương pháp bao gồm các bước sau:

501. Thiết bị đầu cuối xác minh chứng thư tạo chứng thư điện tử dựa trên mã nhận dạng người dùng, và đồng bộ hóa chứng thư điện tử tương ứng với máy chủ dựa

trên mã nhận dạng người dùng, để máy chủ gửi chứng thư điện tử đến phần mềm máy khách.

502. Phần mềm máy khách gửi yêu cầu tiếp nhận chứng thư điện tử đến máy chủ, trong đó yêu cầu tiếp nhận chứng thư điện tử bao gồm mã nhận dạng người dùng và thời gian hiệu lực của dịch vụ.

503. Máy chủ nhận yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, phân tích cú pháp yêu cầu tiếp nhận chứng thư điện tử, và có được thời gian hiệu lực của dịch vụ có trong yêu cầu tiếp nhận chứng thư điện tử.

504. Máy chủ xác minh xem thời gian hiệu lực của dịch vụ có tuân thủ thông số kỹ thuật của dịch vụ hay không.

Nếu thời gian hiệu lực của dịch vụ tuân thủ thông số kỹ thuật của dịch vụ, bước 505 được thực hiện. Nếu thời gian hiệu lực của dịch vụ không tuân thủ tiêu chuẩn dịch vụ, yêu cầu tiếp nhận chứng thư điện tử sẽ bị bỏ qua.

505. Lấy chứng thư điện tử tương ứng với mã nhận dạng người dùng và mã hóa chứng thư điện tử.

Thông tin yêu cầu để nhận được chứng thư điện tử có thể được gửi thêm đến thiết bị đầu cuối xác minh chứng thư dựa trên mã nhận dạng người dùng để thu được chứng thư điện tử.

506. Máy chủ ký mã khóa công khai của người dùng từ phần mềm máy khách và chứng thư điện tử bằng cách sử dụng mã khóa riêng của máy chủ để có được thông tin chữ ký của máy chủ, và gửi thông tin chữ ký của máy chủ và chứng thư điện tử đến phần mềm máy khách.

507. Máy chủ phát đi một mã khóa công khai tương ứng với mã khóa riêng của máy chủ, để phần mềm máy khách và thiết bị đầu cuối xác minh chứng thư thực hiện xác minh thông tin chữ ký dựa trên mã khóa công khai của máy chủ.

508. Phần mềm máy khách nhận và lưu trữ mã khóa công khai được phát đi bởi máy chủ.

509. Phần mềm máy khách nhận thông tin chữ ký của máy chủ và chứng thư điện tử được gửi bởi máy chủ.

510. Phần mềm máy khách xác minh thông tin chữ ký của máy chủ dựa trên mã khóa công khai được phát bởi máy chủ, để thu được chứng thư điện tử.

Nếu xác minh thông tin chữ ký của máy chủ thành công, bước 511 được thực hiện. Nếu xác minh thông tin chữ ký của máy chủ không thành công, có thể không thu được được chứng thư điện tử do máy chủ cung cấp.

511. Phần mềm máy khách ký chứng thư điện tử bằng cách sử dụng mã khóa công khai của người dùng để lấy thông tin chữ ký của phần mềm máy khách và tạo mã vạch hai chiều dựa trên thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng.

512. Thiết bị đầu cuối xác minh chứng thư có được mã vạch hai chiều trong phần mềm máy khách, xác minh khoảng thời gian hiệu lực của thông tin bảo mật định trước, và xác minh thông tin chữ ký của phần mềm máy khách và thông tin chữ ký của máy chủ.

513. Nếu việc xác minh mỗi thông tin trong số thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, và thông tin chữ ký của máy chủ thành công, có được thời gian hiệu lực của dịch vụ có trong chứng thư điện tử để xác minh; và nếu việc xác minh thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử thành công, xác định rằng việc xác minh chứng thư điện tử thành công.

Cần lưu ý là đối với các phần mô tả chi tiết của bước từ 501 đến bước 513, có thể tham chiếu đến các phần mô tả liên quan trước đó. Các chi tiết được bỏ qua để đơn giản theo phương án này của sáng chế.

Hơn nữa, về phương án thực hiện phương pháp được thể hiện trên Fig.1, một phương án khác của sáng chế còn đề xuất máy chủ. Phương án về thiết bị này tương ứng với phương án của phương pháp đã nêu. Để dễ đọc, các chi tiết theo phương án của phương pháp đã nêu được bỏ qua theo phương án về thiết bị này. Tuy nhiên, cần phải rõ ràng rằng thiết bị theo phương án này có thể thực hiện tương ứng tất cả nội dung trong phương án thực hiện phương pháp đã nêu.

Hơn nữa, phương án của sáng chế đề xuất máy chủ. Như được thể hiện trên Fig.8, thiết bị gồm các phần sau: đơn vị nhận 61, được tạo cấu hình để nhận yêu cầu

tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, trong đó yêu cầu tiếp nhận chứng thư điện tử bao gồm mã nhận dạng người dùng; đơn vị tiếp nhận thứ nhất 62, được tạo cấu hình để thu được chứng thư điện tử tương ứng với mã nhận dạng người dùng nhận được bởi đơn vị nhận; đơn vị ký 63, được tạo cấu hình để ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng của máy chủ để có thông tin chữ ký của máy chủ; và đơn vị gửi 64, được tạo cấu hình để gửi thông tin chữ ký của máy chủ có được bởi đơn vị ký 63 và chứng thư điện tử có được bởi đơn vị tiếp nhận thứ nhất tới phần mềm máy khách, để phần mềm máy khách xác minh thông tin chữ ký của máy chủ trong thời gian có hiệu lực của mã khóa công khai của người dùng, và tạo mã vạch hai chiều dựa trên chứng thư điện tử, để thiết bị đầu cuối xác minh chứng thư thực hiện xác minh chứng thư điện tử có trong mã vạch hai chiều, trong đó thiết bị đầu cuối xác minh chứng thư được tạo cấu hình để tạo chứng thư điện tử dựa trên mã nhận dạng người dùng.

Hơn nữa, như được thể hiện trên Fig.9, đơn vị ký 63 bao gồm các phần sau: môđun gán 631, được tạo cấu hình để gán mã khóa chữ ký người dùng cho chứng thư điện tử; môđun ký thứ nhất 632, được tạo cấu hình để ký, bằng cách sử dụng mã khóa riêng của máy chủ, chứng thư điện tử và mã khóa công khai thứ nhất của người dùng được gán bởi môđun gán, trong đó mã khóa chữ ký người dùng được gán bao gồm mã khóa công khai thứ nhất của người dùng; môđun tiếp nhận 633, được tạo cấu hình để thu được mã khóa công khai thứ hai của người dùng được gửi bởi phần mềm máy khách; và môđun ký thứ hai 634, được tạo cấu hình để ký, bằng cách sử dụng mã khóa riêng của máy chủ, chứng thư điện tử và mã khóa công khai thứ hai của người dùng có được từ môđun tiếp nhận.

Ngoài ra, nếu mã khóa công khai thứ nhất của người dùng được ký bằng cách sử dụng mã khóa riêng của máy chủ, đơn vị gửi 64 còn được tạo cấu hình để gửi mã khóa chữ ký người dùng đã gán, thông tin chữ ký của máy chủ và chứng thư điện tử tới phần mềm máy khách.

Hơn nữa, như được thể hiện trên Fig.9, máy chủ còn bao gồm các phần sau: đơn vị phân tích 65, được tạo cấu hình để: trước khi đơn vị tiếp nhận thứ nhất 62 nhận được chứng thư điện tử tương ứng với mã nhận dạng người dùng, phân tích cú pháp yêu cầu tiếp nhận chứng thư điện tử; đơn vị tiếp nhận thứ hai 66, được tạo cấu hình để: sau khi đơn vị phân tích 65 phân tích cú pháp yêu cầu tiếp nhận chứng thư điện tử, có

được thời gian hiệu lực của dịch vụ có trong yêu cầu tiếp nhận chứng thư điện tử; và đơn vị xác minh 67, được tạo cấu hình để xác minh xem thời gian hiệu lực của dịch vụ có được bởi đơn vị tiếp nhận thứ hai 66 có tuân thủ với tiêu chuẩn dịch vụ hay không, trong đó đơn vị tiếp nhận thứ nhất 62 còn được tạo cấu hình để: khi đơn vị xác minh 67 xác minh rằng thời gian hiệu lực của dịch vụ tuân thủ với tiêu chuẩn dịch vụ, có được chứng thư điện tử tương ứng với mã nhận dạng người dùng.

Hơn nữa, như được thể hiện trên Fig.9, đơn vị tiếp nhận thứ nhất 62 bao gồm: môđun nhận 621, được tạo cấu hình để: sau khi thiết bị đầu cuối xác minh chứng thư xác tạo chứng thư điện tử dựa trên mã nhận dạng người dùng, nhận chứng thư điện tử được đồng bộ hóa bởi thiết bị đầu cuối xác minh chứng thư; và môđun xử lý 622, được tạo cấu hình để gửi thông tin yêu cầu để thu được chứng thư điện tử đến thiết bị đầu cuối xác minh chứng thư dựa trên mã nhận dạng người dùng, để thu được chứng thư điện tử.

Hơn nữa, mã khóa chữ ký người dùng là khóa mã bất đối xứng.

Hơn nữa, như được thể hiện trên Fig.9, máy chủ còn bao gồm phần sau: đơn vị phát 68, được tạo cấu hình để phát mã khóa công khai tương ứng với mã khóa riêng của máy chủ, để phần mềm máy khách và đơn vị xác minh chứng thư thực hiện xác minh thông tin chữ ký dựa trên mã khóa công khai của máy chủ.

Một phương án của sáng chế còn đề xuất phần mềm máy khách. Như được thể hiện trên Fig.10, phần mềm máy khách bao gồm các phần sau: đơn vị nhận thứ nhất 71, được tạo cấu hình để nhận thông tin chữ ký của máy chủ và chứng thư điện tử được gửi bởi máy chủ, ở đây thông tin chữ ký của máy chủ có được bởi máy chủ bằng cách ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng của máy chủ; đơn vị xác minh chữ ký 72, được tạo cấu hình để xác minh thông tin chữ ký của máy chủ để thu được chứng thư điện tử; đơn vị tiếp nhận 73, được tạo cấu hình để thu được mã khóa của người dùng tương ứng với mã khóa công khai của người dùng; đơn vị ký 74, được tạo cấu hình để ký chứng thư điện tử bằng cách sử dụng mã khóa công khai của người dùng có được bởi đơn vị tiếp nhận 73 để có được thông tin chữ ký của phần mềm máy khách; và đơn vị kiến tạo 75, được tạo cấu hình để tạo mã vạch hai chiều dựa trên thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ,

chứng thư điện tử, và mã khóa công khai của người dùng, để thiết bị đầu cuối xác minh chứng thư thực hiện xác minh chứng thư điện tử bao gồm trong mã vạch hai chiều dựa trên thông tin bảo mật định trước và mã khóa công khai của người dùng, ở đây thông tin bảo mật định trước có thời hạn hiệu lực, và thiết bị đầu cuối xác minh chứng thư được tạo cấu hình để tạo chứng thư điện tử dựa vào mã nhận dạng người dùng.

Hơn nữa, như được thể hiện trên Fig.11, phần mềm máy khách còn bao gồm các phần sau: đơn vị nhận thứ hai 76, được tạo cấu hình để: trước khi thu được mã khóa của người dùng tương ứng với mã khóa công khai của người dùng, nhận mã khóa chữ ký người dùng được gán cho chứng thư điện tử và được gửi bởi máy chủ.

Đơn vị tiếp nhận 73 còn được tạo cấu hình để nhận được mã khóa thứ nhất của người dùng bao gồm trong mã khóa chữ ký người dùng mà được máy chủ gán cho chứng thư điện tử và được nhận bởi đơn vị nhận thứ hai.

Đơn vị tiếp nhận 73 còn được tạo cấu hình để lấy mã khóa thứ hai của người dùng được tạo bởi phần mềm máy khách và tương ứng với mã khóa công khai của người dùng.

Hơn nữa, như được thể hiện trên Fig.11, đơn vị ký 74 bao gồm các phần sau: môđun ký thứ nhất 741, được tạo cấu hình để ký chứng thư điện tử bằng cách sử dụng mã khóa công khai thứ nhất của người dùng; và môđun ký thứ hai 742, được tạo cấu hình để ký chứng thư điện tử bằng cách sử dụng mã khóa công khai thứ hai của người dùng.

Hơn nữa, như được thể hiện trên Fig.11, đơn vị xác minh chữ ký 72 bao gồm các phần sau: môđun nhận 721, được tạo cấu hình để nhận mã khóa công khai của máy chủ được phát quảng bá bởi máy chủ; môđun lưu trữ 722, được tạo cấu hình để lưu trữ mã khóa công khai của máy chủ nhận được bởi môđun nhận; và môđun xác minh chữ ký thứ nhất 723, được tạo cấu hình để xác minh thông tin chữ ký của máy chủ dựa trên mã khóa công khai của máy chủ được lưu trữ bởi môđun lưu trữ, mã khóa công khai của phần mềm máy khách, và chứng thư điện tử.

Hơn nữa, mã khóa công khai của người dùng và mã khóa của người dùng là các khóa mã bất đối xứng.

Hơn nữa, như được thể hiện trên Fig.11, đơn vị kiến tạo 75 bao gồm các phần sau: môđun thiết đặt 751, được tạo cấu hình để đặt khoảng thời gian hiệu lực của thông tin bảo mật định trước; và môđun kiến tạo 752, được tạo cấu hình để tạo mã vạch hai chiều dựa trên thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, mã khóa công khai của người dùng, khoảng thời gian hiệu lực của thông tin bảo mật định trước, và mã nhận dạng người dùng.

Phương án của sáng chế còn đề xuất thiết bị đầu cuối xác minh chứng thư. Như được thể hiện trên Fig.12, thiết bị đầu cuối xác minh chứng thư bao gồm: đơn vị tiếp nhận thứ nhất 81, được tạo cấu hình để lấy mã vạch hai chiều trong phần mềm máy khách, ở đây mã vạch hai chiều được tạo bởi phần mềm máy khách dựa trên thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử và mã khóa công khai của người dùng, thông tin chữ ký của phần mềm máy khách có được bởi phần mềm máy khách bằng cách ký chứng thư điện tử, và thông tin chữ ký của máy chủ có được bởi máy chủ bằng cách ký chứng thư điện tử và mã khóa công khai của người dùng; đơn vị xác minh thứ nhất 82, được tạo cấu hình để xác minh khoảng thời gian hiệu lực của thông tin bảo mật định trước có được bởi đơn vị tiếp nhận thứ nhất; đơn vị xác minh thứ hai 83, được tạo cấu hình để xác minh thông tin chữ ký của phần mềm máy khách và thông tin chữ ký của máy chủ; đơn vị xác minh thứ ba 84, được tạo cấu hình để có thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử để xác minh khi việc xác minh của đơn vị xác minh thứ nhất trên thông tin bảo mật định trước thành công, việc xác minh của đơn vị xác minh thứ hai trên mỗi trong số thông tin chữ ký phần mềm máy khách và thông tin chữ ký của máy chủ thành công; và đơn vị xác định 85, được tạo cấu hình để xác định rằng việc xác minh chứng thư điện tử thành công khi việc xác minh của đơn vị xác minh thứ ba về thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử thành công.

Hơn nữa, như được thể hiện trên Fig.13, thiết bị đầu cuối xác minh chứng thư bao gồm các thành phần sau: đơn vị kiến tạo 86, được tạo cấu hình để tạo chứng thư điện tử dựa trên mã nhận dạng người dùng trước khi đơn vị tiếp nhận thứ nhất 81 có được mã vạch hai chiều trong phần mềm máy khách; đơn vị đồng bộ hóa 87, được tạo cấu hình để đồng bộ hóa chứng thư điện tử tương ứng với máy chủ dựa trên mã nhận dạng người dùng, để máy chủ gửi chứng thư điện tử đến phần mềm máy khách; đơn vị

nhận 88, được tạo cấu hình để nhận thông tin yêu cầu lấy chứng thư điện tử được gửi bởi máy chủ; và đơn vị gửi 89, được tạo cấu hình để gửi chứng thư điện tử đến máy chủ, trong đó thông tin yêu cầu thu được chứng thư điện tử bao gồm mã nhận dạng người dùng.

Hơn nữa, như được thể hiện trên Fig.13, đơn vị xác minh thứ hai 83 bao gồm: môđun tiếp nhận 831, được tạo cấu hình để lấy mã khóa công khai của người dùng bao gồm trong mã vạch hai chiều; môđun xác minh chữ ký thứ nhất 832, được tạo cấu hình để xác minh thông tin chữ ký của phần mềm máy khách dựa trên mã khóa công khai của người dùng có được bởi môđun tiếp nhận và chứng thư điện tử; môđun nhận 833, được tạo cấu hình để nhận mã khóa công khai của máy chủ tương ứng với mã khóa riêng của máy chủ và được phát bởi máy chủ; một môđun lưu trữ 834, được tạo cấu hình để lưu trữ mã khóa công khai của máy chủ nhận được bởi môđun nhận; và môđun xác minh thứ hai 835, được tạo cấu hình để xác minh thông tin chữ ký của máy chủ dựa trên mã khóa công khai của máy chủ được lưu trữ bởi môđun lưu trữ, mã khóa công khai của phần mềm máy khách, và chứng thư điện tử.

Hơn nữa, như được thể hiện trên Fig.13, thiết bị đầu cuối xác minh chứng thư bao gồm các thành phần sau: đơn vị tiếp nhận thứ hai 810, được tạo cấu hình để: trước khi đơn vị xác định 85 xác định rằng việc xác minh trên chứng thư điện tử thành công, lấy được mã nhận dạng người dùng có trong mã vạch hai chiều; và đơn vị xác minh thứ tư 811, được tạo cấu hình để xác minh mã nhận dạng người dùng có được bởi đơn vị tiếp nhận thứ hai 810.

Đơn vị xác định 85 còn được tạo cấu hình để: khi đơn vị xác minh thứ tư 811 xác định rằng việc xác minh mã nhận dạng người dùng thành công, xác định rằng việc xác minh chứng thư điện tử thành công.

Hơn nữa, như được thể hiện trên Fig.14, phương án của sáng chế còn đề xuất hệ thống xử lý mã vạch hai chiều, và hệ thống này bao gồm các phần sau: phần mềm máy khách 91, được tạo cấu hình để gửi yêu cầu tiếp nhận chứng thư điện tử đến máy chủ 92, ở đây yêu cầu tiếp nhận chứng thư điện tử gồm mã nhận dạng người dùng; máy chủ 92, được tạo cấu hình để nhận yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách 91, và thu được chứng thư điện tử từ thiết bị đầu cuối xác minh chứng thư 93 dựa trên mã nhận dạng người dùng; và thiết bị đầu cuối xác minh chứng

thư 93, được tạo cấu hình để nhận và trả lời thông tin yêu cầu thu được chứng thư điện tử được gửi bởi máy chủ 92, và gửi chứng thư điện tử đến máy chủ 92.

Máy chủ 92 còn được tạo cấu hình để nhận chứng thư điện tử được gửi bởi thiết bị đầu cuối xác minh chứng thư 93, ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách 91 để lấy thông tin chữ ký của máy chủ 92 và gửi thông tin chữ ký của máy chủ 92 và chứng thư điện tử tới phần mềm máy khách 91.

Phần mềm máy khách 91 được tạo cấu hình để nhận thông tin chữ ký của máy chủ 92 và chứng thư điện tử được gửi bởi máy chủ 92, xác minh thông tin chữ ký của máy chủ 92 để nhận được chứng thư điện tử, thu được mã khóa của người dùng tương ứng với mã khóa công khai của người dùng, ký chứng thư điện tử bằng cách sử dụng mã khóa của người dùng để có được thông tin chữ ký của phần mềm máy khách 91 và tạo mã vạch hai chiều dựa trên thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách 91, thông tin chữ ký của máy chủ 92, chứng thư điện tử, và mã khóa công khai của người dùng.

Thiết bị đầu cuối xác minh chứng thư 93 được tạo cấu hình để nhận được mã vạch hai chiều trong phần mềm máy khách 91, xác minh khoảng thời gian hiệu lực của thông tin bảo mật định trước, và xác minh thông tin chữ ký của phần mềm máy khách 91 và thông tin chữ ký của máy chủ 92; và nếu việc xác minh một trong số thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách 91, và thông tin chữ ký của máy chủ 92 thành công, có được thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử để xác minh, và nếu việc xác minh thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử thành công, xác định rằng việc xác minh chứng thư điện tử thành công.

Theo máy chủ, phần mềm máy khách, thiết bị đầu cuối xác minh chứng thư, hệ thống xử lý mã vạch hai chiều được đề xuất theo sáng chế, sau khi nhận được yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, máy chủ ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng của máy chủ để có được thông tin chữ ký của máy chủ, và gửi thông tin chữ ký của máy chủ và chứng thư điện tử đến phần mềm máy khách. Phần mềm máy khách nhận thông tin chữ ký của máy chủ và chứng thư điện tử được gửi bởi máy chủ, xác minh thông tin chữ ký của máy chủ, sau khi xác minh thông tin chữ ký

thành công, ký chứng thư điện tử và tạo mã vạch hai chiều dựa trên thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử và mã khóa công khai của người dùng. Sau khi có được mã vạch hai chiều, thiết bị đầu cuối xác minh chứng thư có thể xác minh thông tin chữ ký của máy chủ, thông tin chữ ký của phần mềm máy khách, và thông tin bảo mật định trước trong mã vạch hai chiều để xác định xem chứng thư điện tử có bị giả mạo trong quá trình truyền hay không, để đảm bảo tính bảo mật của chứng thư điện tử trong quá trình sử dụng.

Trong các phương án đã nêu, phần mô tả của mỗi phương án có trọng tâm tương ứng. Đối với phần không được mô tả chi tiết theo phương án này, có thể tham khảo đến các phần mô tả liên quan trong các phương án khác.

Có thể hiểu rằng các dấu hiệu liên quan theo phương pháp và thiết bị đã nêu có thể được tham chiếu lẫn nhau. Ngoài ra, "thứ nhất", "thứ hai", v.v. theo phương án đã nêu được sử dụng để phân biệt giữa các phương án, và không thể hiện ưu điểm và nhược điểm của mỗi phương án.

Người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng có thể hiểu rõ rằng để mô tả thuận tiện và ngắn gọn, đối với quy trình làm việc cụ thể của hệ thống, thiết bị, và thiết bị được mô tả ở trên, có thể tham chiếu đến quy trình tương ứng trong các phương án thực hiện phương pháp đã nêu, và các chi tiết được bỏ qua để đơn giản hóa theo phương án của sáng chế.

Thuật toán và hiển thị được đưa ra ở đây vốn không liên quan đến bất kỳ máy tính, hệ thống ảo, hoặc thiết bị cụ thể nào khác. Các hệ thống đa năng khác nhau cũng có thể được sử dụng cùng với chỉ dẫn trong bản mô tả này. Dựa vào mô tả ở trên, cấu trúc cần thiết để xây dựng một hệ thống như vậy là rõ ràng. Hơn nữa, sáng chế không áp dụng cho bất kỳ ngôn ngữ lập trình cụ thể nào. Cần hiểu rằng nội dung của sáng chế được mô tả ở đây có thể được thực hiện bằng cách sử dụng các ngôn ngữ lập trình khác nhau, và mô tả đã nêu của ngôn ngữ chi tiết được sử dụng để bộc lộ phương án tối ưu của sáng chế.

Một số lượng lớn các nội dung chi tiết được đưa ra trong bản mô tả này. Tuy nhiên, có thể hiểu rằng các phương án của sáng chế có thể được thực hiện mà không cần các nội dung chi tiết này. Trong một số trường hợp đặc biệt, các phương pháp, cấu

trúc, và công nghệ phổ biến không được thể hiện chi tiết, để không làm cho bản mô tả bị khó hiểu.

Tương tự, cần hiểu rằng, để đơn giản hóa phần bộc lộ này và giúp hiểu một hoặc nhiều khía cạnh sáng tạo khác nhau, các dấu hiệu của sáng chế đôi khi được nhóm lại thành một phương án, hình vẽ hoặc mô tả của sáng chế. Tuy nhiên, không nên hiểu phương pháp được bộc lộ dưới dạng phản ánh ý định sau: tức là, phần bộc lộ yêu cầu bảo hộ cần nhiều dấu hiệu hơn các dấu hiệu được chỉ ra trong mỗi điểm yêu cầu bảo hộ. Chính xác hơn là, như được phản ánh trong các điểm yêu cầu bảo hộ dưới đây, các khía cạnh sáng tạo ít hơn tất cả các dấu hiệu của một phương án đã được bộc lộ. Do đó, các điểm yêu cầu bảo hộ theo một phương án chi tiết theo cách xác định bao gồm phương án chi tiết. Mỗi điểm yêu cầu bảo hộ đóng vai trò là một phương án riêng của sáng chế.

Người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng có thể hiểu rằng các môđun ở các thiết bị trong các phương án có thể được thay đổi và sắp xếp một cách thích hợp trong một hoặc nhiều thiết bị khác với các phương án này. Các môđun hoặc đơn vị hoặc thành phần trong các phương án có thể được kết hợp thành một môđun hoặc đơn vị hoặc thành phần, và ngoài ra có thể được chia thành một số lượng lớn các môđun phụ hoặc đơn vị phụ hoặc thành phần phụ. Ngoại trừ thực tế là ít nhất một số dấu hiệu và/hoặc quy trình hoặc đơn vị này là riêng biệt với nhau, tất cả các dấu hiệu được bộc lộ và tất cả các quy trình hoặc đơn vị của phương pháp bất kỳ hoặc thiết bị bất kỳ được bộc lộ theo phương pháp trong bản mô tả này (bao gồm các điểm yêu cầu bảo hộ kèm theo, bản tóm tắt, và các hình vẽ kèm theo) có thể được kết hợp theo hình thức kết hợp bất kỳ. Trừ khi được trình chỉ rõ theo cách khác, mỗi dấu hiệu được bộc lộ trong bản mô tả này (bao gồm các điểm yêu cầu bảo hộ kèm theo, bản tóm tắt, và các hình vẽ kèm theo) có thể được thay thế bằng một dấu hiệu khác, nhằm đạt được mục đích giống, tương đương, hoặc tương tự.

Ngoài ra, người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng có thể hiểu rằng, mặc dù một số phương án được mô tả ở đây bao gồm một số dấu hiệu gồm trong một phương án khác thay vì bao gồm một dấu hiệu khác, sự kết hợp các dấu hiệu của các phương án khác nhau có nghĩa là nằm trong phạm vi của sáng chế và hình thành các phương án khác nhau. Ví dụ, trong các điểm yêu cầu bảo hộ sau đây, bất kỳ

một trong những phương án được dự tính có thể được sử dụng theo hình thức kết hợp bất kỳ.

Các phương án về các phần khác nhau trong sáng chế có thể được thực hiện bằng phần cứng, hoặc các môđun phần mềm chạy trên một hoặc nhiều bộ xử lý, hoặc kết hợp của chúng. Người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng nên hiểu rằng bộ vi xử lý hoặc bộ xử lý tín hiệu số (DSP) có thể được sử dụng trong thực tế để thực hiện một số hoặc tất cả các chức năng của một số hoặc tất cả các thành phần có tên bộc lộ (ví dụ, thiết bị để xử lý mã vạch hai chiều) dựa trên phương án của sáng chế. Sáng chế cũng có thể được thực hiện dưới dạng một thiết bị hoặc chương trình máy móc (ví dụ, chương trình máy tính và sản phẩm chương trình máy tính) để thực hiện một phần hoặc tất cả các phương pháp được mô tả ở đây. Một chương trình như vậy để thực hiện sáng chế có thể được lưu trữ trong một phương tiện đọc được bằng máy tính hoặc có thể có hình thức một hoặc nhiều tín hiệu. Một tín hiệu như vậy có thể được tải xuống từ một trang web Internet, hoặc được cung cấp trên tín hiệu sóng mang, hoặc được cung cấp theo bất kỳ hình thức nào khác.

Cần lưu ý là các phương án đã nêu nhằm mục đích mô tả sáng chế, thay vì giới hạn sáng chế, và người có hiểu biết trung bình về lĩnh vực kỹ thuật này có thể thiết kế một phương án thay thế mà không nằm ngoài phạm vi của các điểm yêu cầu bảo hộ kèm theo. Trong các điểm yêu cầu bảo hộ, ký hiệu tham chiếu bất kỳ giữa các dấu ngoặc không nên được hiểu dưới dạng giới hạn về các yêu cầu bảo hộ. Từ "bao gồm" không loại trừ sự tồn tại của các phần tử hoặc các bước không được liệt kê trong các điểm yêu cầu bảo hộ. Từ “một” hoặc “chỉ một/ duy chỉ một” trước phần tử không loại trừ sự hiện diện của nhiều phần tử như vậy. Sáng chế có thể được thực hiện bằng phần cứng bao gồm các phần tử khác nhau và máy tính được lập trình phù hợp. Trong các điểm yêu cầu bảo hộ thiết bị liệt kê một số thiết bị, một số thiết bị này có thể được thể hiện bằng cách sử dụng cùng một mục phần cứng. Việc sử dụng các từ "thứ nhất", "thứ hai", và "thứ ba" không biểu thị bất kỳ trình tự nào. Những từ này có thể được hiểu dưới dạng các tên gọi.

Yêu cầu bảo hộ

1. Phương pháp xử lý các mã vạch hai chiều bao gồm các bước:

nhận, bởi máy chủ, yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, trong đó yêu cầu tiếp nhận chứng thư điện tử bao gồm mã nhận dạng người dùng;

thu được chứng thư điện tử tương ứng với mã nhận dạng người dùng, và ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng tư của máy chủ để thu được thông tin chữ ký của máy chủ; và

gửi thông tin chữ ký của máy chủ và chứng thư điện tử đến phần mềm máy khách, để cho phần mềm máy khách thực hiện xác minh thông tin chữ ký của máy chủ, và tạo ra mã vạch hai chiều trên cơ sở chứng thư điện tử này để cho thiết bị đầu cuối xác minh chứng thư thực hiện xác minh chứng thư điện tử bao gồm trong mã vạch hai chiều, trong đó thiết bị đầu cuối xác minh chứng thư được tạo cấu hình để tạo ra chứng thư điện tử trên cơ sở mã nhận dạng người dùng.

2. Phương pháp theo điểm 1, trong đó bước ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng tư của máy chủ bao gồm việc:

gán mã khóa chữ ký người dùng cho chứng thư điện tử, và ký chứng thư điện tử và mã khóa công khai thứ nhất của người dùng bằng cách sử dụng mã khóa riêng tư của máy chủ, trong đó mã khóa chữ ký người dùng bao gồm mã khóa công khai thứ nhất của người dùng; hoặc

thu được mã khóa công khai thứ hai của người dùng được gửi bởi phần mềm máy khách, và ký chứng thư điện tử và mã khóa công khai thứ hai của người dùng bằng cách sử dụng mã khóa riêng tư của máy chủ.

3. Phương pháp theo điểm 2, trong đó nếu mã khóa công khai thứ nhất của người dùng được ký bằng cách sử dụng mã khóa riêng tư của máy chủ, thì bước gửi thông tin chữ ký của máy chủ và chứng thư điện tử đến phần mềm máy khách bao gồm việc:

gửi mã khóa chữ ký người dùng, thông tin chữ ký của máy chủ, và chứng thư

điện tử đến phần mềm máy khách.

4. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó trước bước thu được chứng thư điện tử tương ứng với mã nhận dạng người dùng, phương pháp này còn bao gồm bước:

phân tích cú pháp yêu cầu tiếp nhận chứng thư điện tử, và thu được thời gian hiệu lực của dịch vụ bao gồm trong yêu cầu tiếp nhận chứng thư điện tử; và

xác minh xem liệu thời gian hiệu lực của dịch vụ có tuân theo tiêu chuẩn dịch vụ hay không; và

thu được chứng thư điện tử tương ứng với mã nhận dạng người dùng bao gồm:

nếu thời gian hiệu lực của dịch vụ tuân theo tiêu chuẩn dịch vụ, thì thu được chứng thư điện tử tương ứng với mã nhận dạng người dùng.

5. Phương pháp theo điểm 4, trong đó bước thu được chứng thư điện tử tương ứng với mã nhận dạng người dùng bao gồm việc:

sau khi thiết bị đầu cuối xác minh chứng thư tạo ra chứng thư điện tử trên cơ sở mã nhận dạng người dùng, nhận chứng thư điện tử được đồng bộ bởi thiết bị đầu cuối xác minh chứng thư; hoặc

gửi thông tin yêu cầu thu được chứng thư điện tử đến thiết bị đầu cuối xác minh chứng thư trên cơ sở mã nhận dạng người dùng để thu được chứng thư điện tử.

6. Phương pháp theo điểm 2, trong đó mã khóa chữ ký người dùng là mã khóa bất đối xứng.

7. Phương pháp theo điểm 4, trong đó phương pháp này còn bao gồm bước:

phát quảng bá mã khóa công khai tương ứng với mã khóa riêng tư của máy chủ, để cho phần mềm máy khách và thiết bị đầu cuối xác minh chứng thư thực hiện xác minh thông tin chữ ký trên cơ sở mã khóa công khai của máy chủ.

8. Phương pháp xử lý các mã vạch hai chiều bao gồm các bước:

nhận, bởi phần mềm máy khách, thông tin chữ ký của máy chủ và chứng thư điện tử được gửi bởi máy chủ, trong đó thông tin chữ ký của máy chủ thu được bởi máy chủ bằng cách ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng tư của máy chủ;

xác minh thông tin chữ ký của máy chủ để thu được chứng thư điện tử;

thu được mã khóa của người dùng tương ứng với mã khóa công khai của người dùng, và ký chứng thư điện tử bằng cách sử dụng mã khóa của người dùng để thu được thông tin chữ ký của phần mềm máy khách; và

tạo ra mã vạch hai chiều trên cơ sở thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng, để cho thiết bị đầu cuối xác minh chứng thư thực hiện xác minh chứng thư điện tử bao gồm trong mã vạch hai chiều trên cơ sở thông tin bảo mật định trước và mã khóa công khai của người dùng, trong đó thông tin bảo mật định trước có khoảng thời gian hiệu lực, và thiết bị đầu cuối xác minh chứng thư được tạo cấu hình để tạo ra chứng thư điện tử trên cơ sở mã nhận dạng người dùng.

9. Phương pháp theo điểm 8, trong đó trước khi thu được mã khóa của người dùng tương ứng với mã khóa công khai của người dùng, phương pháp này còn bao gồm bước:

nhận mã khóa chữ ký người dùng được gán cho chứng thư điện tử và được gửi bởi máy chủ; và

thu được mã khóa của người dùng tương ứng với mã khóa công khai của người dùng bao gồm:

thu được mã khóa thứ nhất của người dùng bao gồm trong mã khóa chữ ký người dùng được gán bởi máy chủ cho chứng thư điện tử; hoặc

thu được mã khóa thứ hai của người dùng được tạo ra bởi phần mềm máy khách và tương ứng với mã khóa công khai của người dùng.

10. Phương pháp theo điểm 9, trong đó bước ký chứng thư điện tử bằng cách sử dụng mã khóa của người dùng bao gồm việc:

ký chứng thư điện tử bằng cách sử dụng mã khóa thứ nhất của người dùng; hoặc

ký chứng thư điện tử bằng cách sử dụng mã khóa thứ hai của người dùng.

11. Phương pháp theo điểm 8, trong đó bước xác minh thông tin chữ ký của máy chủ bao gồm việc:

nhận và lưu mã khóa công khai của máy chủ được phát quảng bá bởi máy chủ; và

xác minh thông tin chữ ký của máy chủ trên cơ sở mã khóa công khai của máy chủ, mã khóa công khai của phần mềm máy khách, và chứng thư điện tử.

12. Phương pháp theo điểm bất kỳ trong số các điểm từ 8 đến 11, trong đó mã khóa công khai của người dùng và mã khóa của người dùng là các mã khóa bất đối xứng.

13. Phương pháp theo điểm 12, trong đó bước tạo ra mã vạch hai chiều trên cơ sở thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng bao gồm việc:

thiết đặt khoảng thời gian hiệu lực của thông tin bảo mật định trước; và

tạo ra mã vạch hai chiều trên cơ sở thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, mã khóa công khai của người dùng, khoảng thời gian hiệu lực của thông tin bảo mật định trước, và mã nhận dạng người dùng.

14. Phương pháp xử lý các mã vạch hai chiều bao gồm các bước:

thu được, bởi thiết bị đầu cuối xác minh chứng thư, mã vạch hai chiều trong phần mềm máy khách, trong đó mã vạch hai chiều được tạo ra bởi phần mềm máy khách trên cơ sở thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng, thông tin chữ ký của phần mềm máy khách thu được bởi phần mềm máy khách bằng cách ký chứng thư điện tử, và thông tin chữ ký của máy chủ thu được bởi máy chủ bằng cách ký chứng thư điện tử và mã khóa công khai của người dùng;

xác minh khoảng thời gian hiệu lực của thông tin bảo mật định trước, và xác minh thông tin chữ ký của phần mềm máy khách và thông tin chữ ký của máy chủ;

nếu việc xác minh từng thông tin trong số thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, và thông tin chữ ký của máy chủ thành công, thu được thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử dùng cho xác minh; và

nếu việc xác minh thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử thành công, xác định rằng việc xác minh chứng thư điện tử thành công.

15. Phương pháp theo điểm 14, trong đó trước khi thu được mã vạch hai chiều trong

phần mềm máy khách, phương pháp này còn bao gồm các bước:

tạo chứng thư điện tử trên cơ sở mã nhận dạng người dùng; và

đồng bộ chứng thư điện tử với máy chủ trên cơ sở mã nhận dạng người dùng, để cho máy chủ gửi chứng thư điện tử đến phần mềm máy khách; hoặc

nhận thông tin yêu cầu thu được chứng thư điện tử được gửi bởi máy chủ, và gửi chứng thư điện tử đến máy chủ, trong đó thông tin yêu cầu thu được chứng thư điện tử bao gồm mã nhận dạng người dùng.

16. Phương pháp theo điểm 15, trong đó bước xác minh thông tin chữ ký của phần mềm máy khách và thông tin chữ ký của máy chủ bao gồm việc:

thu được mã khóa công khai của người dùng bao gồm trong mã vạch hai chiều, và xác minh thông tin chữ ký của phần mềm máy khách trên cơ sở mã khóa công khai của người dùng và chứng thư điện tử;

nhận và lưu mã khóa công khai của máy chủ tương ứng với mã khóa riêng tư của máy chủ và phát quảng bá bởi máy chủ; và

xác minh thông tin chữ ký của máy chủ trên cơ sở mã khóa công khai của máy chủ, mã khóa công khai của phần mềm máy khách, và chứng thư điện tử.

17. Phương pháp theo điểm 16, trong đó trước bước xác định rằng việc xác minh chứng thư điện tử thành công, phương pháp này còn bao gồm bước:

thu được mã nhận dạng người dùng bao gồm trong mã vạch hai chiều, và xác minh mã nhận dạng người dùng; và

bước xác định rằng việc xác minh chứng thư điện tử thành công bao gồm việc:

nếu xác định được rằng việc xác minh mã nhận dạng người dùng thành công, xác định rằng việc xác minh chứng thư điện tử thành công.

18. Máy chủ bao gồm:

đơn vị nhận, được tạo cấu hình để nhận yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, trong đó yêu cầu tiếp nhận chứng thư điện tử bao gồm mã nhận dạng người dùng;

đơn vị tiếp nhận thứ nhất, được tạo cấu hình để thu được chứng thư điện tử tương ứng với mã nhận dạng người dùng nhận được bởi đơn vị nhận;

đơn vị ký, được tạo cấu hình để ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng tư của máy chủ để thu được thông tin chữ ký của máy chủ; và

đơn vị gửi, được tạo cấu hình để gửi thông tin chữ ký của máy chủ thu được bởi đơn vị ký và chứng thư điện tử thu được bởi đơn vị tiếp nhận thứ nhất đến phần mềm máy khách, để cho phần mềm máy khách thực hiện xác minh thông tin chữ ký của máy chủ trong thời gian hiệu lực của mã khóa của người dùng, và tạo ra mã vạch hai chiều trên cơ sở chứng thư điện tử này để cho thiết bị đầu cuối xác minh chứng thư thực hiện xác minh chứng thư điện tử bao gồm trong mã vạch hai chiều, trong đó thiết bị đầu cuối xác minh chứng thư được tạo cấu hình để tạo ra chứng thư điện tử trên cơ sở mã nhận dạng người dùng.

19. Máy chủ theo điểm 18, trong đó đơn vị ký bao gồm:

môđun gán, được tạo cấu hình để gán mã khóa chữ ký người dùng cho chứng thư điện tử;

môđun ký thứ nhất, được tạo cấu hình để ký, bằng cách sử dụng mã khóa riêng tư của máy chủ, chứng thư điện tử và mã khóa công khai thứ nhất của người dùng được gán bởi môđun gán, trong đó mã khóa chữ ký người dùng bao gồm mã khóa công khai thứ nhất của người dùng;

môđun tiếp nhận, được tạo cấu hình để nhận được mã khóa công khai thứ hai của người dùng được gửi bởi phần mềm máy khách; và

môđun ký thứ hai, được tạo cấu hình để ký, bằng cách sử dụng mã khóa riêng tư của máy chủ, chứng thư điện tử và mã khóa công khai thứ hai của người dùng thu được bởi môđun tiếp nhận.

20. Máy chủ theo điểm 19, trong đó nếu mã khóa công khai thứ nhất của người dùng được ký bằng cách sử dụng mã khóa riêng tư của máy chủ, đơn vị gửi còn được tạo cấu hình để gửi mã khóa chữ ký người dùng, thông tin chữ ký của máy chủ, và chứng thư điện tử đến phần mềm máy khách.

21. Máy chủ theo điểm bất kỳ trong số các điểm từ 18 đến 20, trong đó máy chủ này còn bao gồm:

đơn vị phân tích cú pháp, được tạo cấu hình để: trước khi đơn vị tiếp nhận thứ

nhất thu được chứng thư điện tử tương ứng với mã nhận dạng người dùng, phân tích cú pháp yêu cầu tiếp nhận chứng thư điện tử;

đơn vị tiếp nhận thứ hai, được tạo cấu hình để: sau khi đơn vị phân tích cú pháp thực hiện phân tích cú pháp yêu cầu tiếp nhận chứng thư điện tử, thu được thời gian hiệu lực của dịch vụ bao gồm trong yêu cầu tiếp nhận chứng thư điện tử; và

đơn vị xác minh, được tạo cấu hình để xác minh xem liệu thời gian hiệu lực của dịch vụ thu được bởi đơn vị tiếp nhận thứ hai có tuân theo tiêu chuẩn dịch vụ hay không, trong đó:

đơn vị tiếp nhận thứ nhất còn được tạo cấu hình để: khi đơn vị xác minh thực hiện xác minh rằng thời gian hiệu lực của dịch vụ tuân theo tiêu chuẩn dịch vụ, thu được chứng thư điện tử tương ứng với mã nhận dạng người dùng.

22. Máy chủ theo điểm 21, trong đó đơn vị tiếp nhận thứ nhất bao gồm:

môđun nhận, được tạo cấu hình để: sau khi thiết bị đầu cuối xác minh chứng thư tạo ra chứng thư điện tử trên cơ sở mã nhận dạng người dùng, nhận chứng thư điện tử được đồng bộ bởi thiết bị đầu cuối xác minh chứng thư; và

môđun xử lý, được tạo cấu hình để gửi thông tin yêu cầu thu được chứng thư điện tử đến thiết bị đầu cuối xác minh chứng thư trên cơ sở mã nhận dạng người dùng để thu được chứng thư điện tử.

23. Máy chủ theo điểm 19, trong đó mã khóa chữ ký người dùng là mã khóa bất đối xứng.

24. Máy chủ theo điểm 21, trong đó máy chủ này còn bao gồm:

đơn vị phát quảng bá, được tạo cấu hình để phát quảng bá mã khóa công khai tương ứng với mã khóa riêng tư của máy chủ, để cho phần mềm máy khách và thiết bị đầu cuối xác minh chứng thư thực hiện xác minh thông tin chữ ký trên cơ sở mã khóa công khai của máy chủ.

25. Phần mềm máy khách bao gồm:

đơn vị nhận thứ nhất, được tạo cấu hình để nhận thông tin chữ ký của máy chủ và chứng thư điện tử được gửi bởi máy chủ, trong đó thông tin chữ ký của máy chủ thu được bởi máy chủ bằng cách ký chứng thư điện tử và mã khóa công khai của người

dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng tư của máy chủ;

đơn vị xác minh chữ ký, được tạo cấu hình để xác minh thông tin chữ ký của máy chủ để thu được chứng thư điện tử;

đơn vị tiếp nhận, được tạo cấu hình để nhận được mã khóa của người dùng tương ứng với mã khóa công khai của người dùng;

đơn vị ký, được tạo cấu hình để ký chứng thư điện tử bằng cách sử dụng mã khóa của người dùng thu được bởi đơn vị tiếp nhận để thu được thông tin chữ ký của phần mềm máy khách; và

đơn vị kiến tạo, được tạo cấu hình để tạo mã vạch hai chiều trên cơ sở thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng, để cho thiết bị đầu cuối xác minh chứng thư thực hiện xác minh chứng thư điện tử bao gồm trong mã vạch hai chiều trên cơ sở thông tin bảo mật định trước và mã khóa công khai của người dùng, trong đó thông tin bảo mật định trước có khoảng thời gian hiệu lực, và thiết bị đầu cuối xác minh chứng thư được tạo cấu hình để tạo ra chứng thư điện tử trên cơ sở mã nhận dạng người dùng.

26. Phần mềm máy khách theo điểm 25, trong đó phần mềm máy khách còn bao gồm:

đơn vị nhận thứ hai, được tạo cấu hình để: trước khi thu được mã khóa của người dùng tương ứng với mã khóa công khai của người dùng, nhân mã khóa chữ ký người dùng được gán cho chứng thư điện tử và được gửi bởi máy chủ; và

đơn vị tiếp nhận này còn được tạo cấu hình để nhận được mã khóa thứ nhất của người dùng bao gồm trong mã khóa chữ ký người dùng mà được gán bởi máy chủ cho chứng thư điện tử và nhận được bởi đơn vị nhận thứ hai; và

đơn vị tiếp nhận này còn được tạo cấu hình để nhận được mã khóa thứ hai của người dùng được tạo ra bởi phần mềm máy khách và tương ứng với mã khóa công khai của người dùng.

27. Phần mềm máy khách theo điểm 26, trong đó đơn vị ký bao gồm:

môđun ký thứ nhất, được tạo cấu hình để ký chứng thư điện tử bằng cách sử dụng mã khóa thứ nhất của người dùng; và

môđun ký thứ hai, được tạo cấu hình để ký chứng thư điện tử bằng cách sử dụng mã khóa thứ hai của người dùng.

28. Phần mềm máy khách theo điểm 25, trong đó đơn vị xác minh chữ ký bao gồm:

môđun nhận, được tạo cấu hình để nhận mã khóa công khai của máy chủ được phát quảng bá bởi máy chủ;

môđun lưu trữ, được tạo cấu hình để lưu mã khóa công khai của máy chủ nhận được bởi môđun nhận; và

môđun xác minh chữ ký, được tạo cấu hình để xác minh thông tin chữ ký của máy chủ trên cơ sở mã khóa công khai của máy chủ được lưu bởi môđun lưu trữ, mã khóa công khai của phần mềm máy khách, và chứng thư điện tử.

29. Phần mềm máy khách theo điểm bất kỳ trong số các điểm từ 25 đến 28, trong đó mã khóa công khai của người dùng và mã khóa của người dùng là các mã khóa bất đối xứng.

30. Phần mềm máy khách theo điểm 29, trong đó đơn vị kiến tạo bao gồm:

môđun thiết đặt, được tạo cấu hình để thiết đặt khoảng thời gian hiệu lực của thông tin bảo mật định trước; và

môđun kiến tạo, được tạo cấu hình để tạo mã vạch hai chiều trên cơ sở thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, mã khóa công khai của người dùng, khoảng thời gian hiệu lực của thông tin bảo mật định trước, và mã nhận dạng người dùng.

31. Thiết bị đầu cuối xác minh chứng thư bao gồm:

đơn vị tiếp nhận thứ nhất, được tạo cấu hình để nhận được mã vạch hai chiều trong phần mềm máy khách, trong đó mã vạch hai chiều được tạo ra bởi phần mềm máy khách trên cơ sở thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng, thông tin chữ ký của phần mềm máy khách thu được bởi phần mềm máy khách bằng cách ký chứng thư điện tử, và thông tin chữ ký của máy chủ thu được bởi máy chủ bằng cách ký chứng thư điện tử và mã khóa công khai của người dùng;

đơn vị xác minh thứ nhất, được tạo cấu hình để xác minh khoảng thời gian hiệu

lực của thông tin bảo mật định trước thu được bởi đơn vị tiếp nhận thứ nhất;

đơn vị xác minh thứ hai, được tạo cấu hình để xác minh thông tin chữ ký của phần mềm máy khách và thông tin chữ ký của máy chủ;

đơn vị xác minh thứ ba, được tạo cấu hình để: khi việc xác minh của đơn vị xác minh thứ nhất về thông tin bảo mật định trước thành công, việc xác minh của đơn vị xác minh thứ hai về từng thông tin trong số thông tin chữ ký của phần mềm máy khách và thông tin chữ ký của máy chủ thành công, thu được thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử dùng cho xác minh; và

đơn vị xác định, được tạo cấu hình để: khi việc xác minh của đơn vị xác minh thứ ba về thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử thành công, xác định rằng việc xác minh chứng thư điện tử thành công.

32. Thiết bị đầu cuối xác minh chứng thư theo điểm 31, trong đó thiết bị đầu cuối xác minh chứng thư còn bao gồm:

đơn vị kiến tạo, được tạo cấu hình để tạo chứng thư điện tử trên cơ sở mã nhận dạng người dùng trước khi đơn vị tiếp nhận thứ nhất thu được mã vạch hai chiều trong phần mềm máy khách;

đơn vị đồng bộ, được tạo cấu hình để đồng bộ chứng thư điện tử theo máy chủ trên cơ sở mã nhận dạng người dùng, để cho máy chủ gửi chứng thư điện tử đến phần mềm máy khách;

đơn vị nhận, được tạo cấu hình để nhận thông tin yêu cầu thu được chứng thư điện tử được gửi bởi máy chủ; và

đơn vị gửi, được tạo cấu hình để gửi chứng thư điện tử đến máy chủ, trong đó thông tin yêu cầu thu được chứng thư điện tử bao gồm mã nhận dạng người dùng.

33. Thiết bị đầu cuối xác minh chứng thư theo điểm 32, trong đó đơn vị xác minh thứ hai bao gồm:

môđun tiếp nhận, được tạo cấu hình để nhận được mã khóa công khai của người dùng bao gồm trong mã vạch hai chiều;

môđun xác minh chữ ký thứ nhất, được tạo cấu hình để xác minh thông tin chữ ký của phần mềm máy khách trên cơ sở mã khóa công khai của người dùng thu được bởi

môđun tiếp nhận và chứng thư điện tử;

môđun nhận, được tạo cấu hình để nhận mã khóa công khai của máy chủ tương ứng với mã khóa riêng tư của máy chủ và phát quảng bá bởi máy chủ;

môđun lưu trữ, được tạo cấu hình để lưu mã khóa công khai của máy chủ nhận được bởi môđun nhận; và

môđun xác minh thứ hai, được tạo cấu hình để xác minh thông tin chữ ký của máy chủ trên cơ sở mã khóa công khai của máy chủ được lưu bởi môđun lưu trữ, mã khóa công khai của phần mềm máy khách, và chứng thư điện tử.

34. Thiết bị đầu cuối xác minh chứng thư theo điểm 33, trong đó thiết bị đầu cuối xác minh chứng thư còn bao gồm:

đơn vị tiếp nhận thứ hai, được tạo cấu hình để: trước khi đơn vị xác định thực hiện xác định rằng việc xác minh chứng thư điện tử thành công, thu được mã nhận dạng người dùng bao gồm trong mã vạch hai chiều; và

đơn vị xác minh thứ tư, được tạo cấu hình để xác minh mã nhận dạng người dùng thu được bởi đơn vị tiếp nhận thứ hai, trong đó:

đơn vị xác định còn được tạo cấu hình để: khi đơn vị xác minh thứ tư xác định rằng việc xác minh mã nhận dạng người dùng thành công, xác định rằng việc xác minh chứng thư điện tử thành công.

35. Hệ thống xử lý các mã vạch hai chiều, trong đó hệ thống này bao gồm:

phần mềm máy khách, được tạo cấu hình để gửi yêu cầu tiếp nhận chứng thư điện tử đến máy chủ, trong đó yêu cầu tiếp nhận chứng thư điện tử bao gồm mã nhận dạng người dùng;

máy chủ, được tạo cấu hình để nhận yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, và thu được chứng thư điện tử từ thiết bị đầu cuối xác minh chứng thư trên cơ sở mã nhận dạng người dùng; và

thiết bị đầu cuối xác minh chứng thư, được tạo cấu hình để nhận và đáp lại thông tin yêu cầu thu được chứng thư điện tử được gửi bởi máy chủ, và gửi chứng thư điện tử đến máy chủ, trong đó:

máy chủ còn được tạo cấu hình để nhận chứng thư điện tử được gửi bởi thiết bị

đầu cuối xác minh chứng thư, ký chứng thư điện tử và mã khóa công khai của người dùng từ phần mềm máy khách để thu được thông tin chữ ký của máy chủ, và gửi thông tin chữ ký của máy chủ và chứng thư điện tử đến phần mềm máy khách;

phần mềm máy khách được tạo cấu hình để nhận thông tin chữ ký của máy chủ và chứng thư điện tử mà được gửi bởi máy chủ, xác minh thông tin chữ ký của máy chủ để thu được chứng thư điện tử, thu được mã khóa của người dùng tương ứng với mã khóa công khai của người dùng, ký chứng thư điện tử bằng cách sử dụng mã khóa của người dùng để thu được thông tin chữ ký của phần mềm máy khách, và tạo mã vạch hai chiều trên cơ sở thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng; và

thiết bị đầu cuối xác minh chứng thư được tạo cấu hình để nhận được mã vạch hai chiều trong phần mềm máy khách, xác minh khoảng thời gian hiệu lực của thông tin bảo mật định trước, và xác minh thông tin chữ ký của phần mềm máy khách và thông tin chữ ký của máy chủ; và nếu việc xác minh từng thông tin trong số thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, và thông tin chữ ký của máy chủ thành công, thu được thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử dùng cho xác minh, và nếu việc xác minh thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử thành công, xác định rằng việc xác minh chứng thư điện tử thành công.

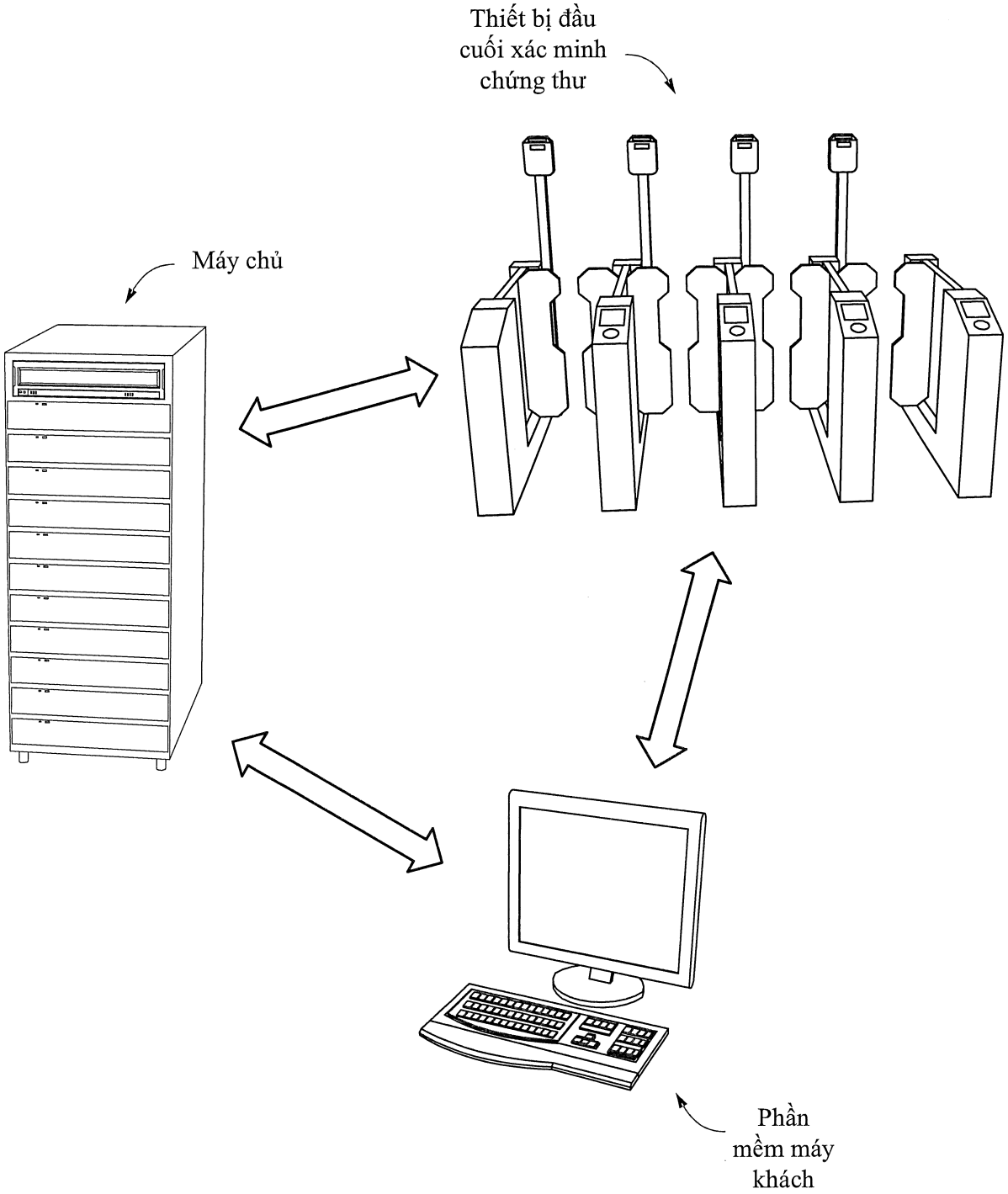

Thiết bị đầu cuối xác minh chứng thư
Máy chủ
Phần mềm máy khách

FIG. 1

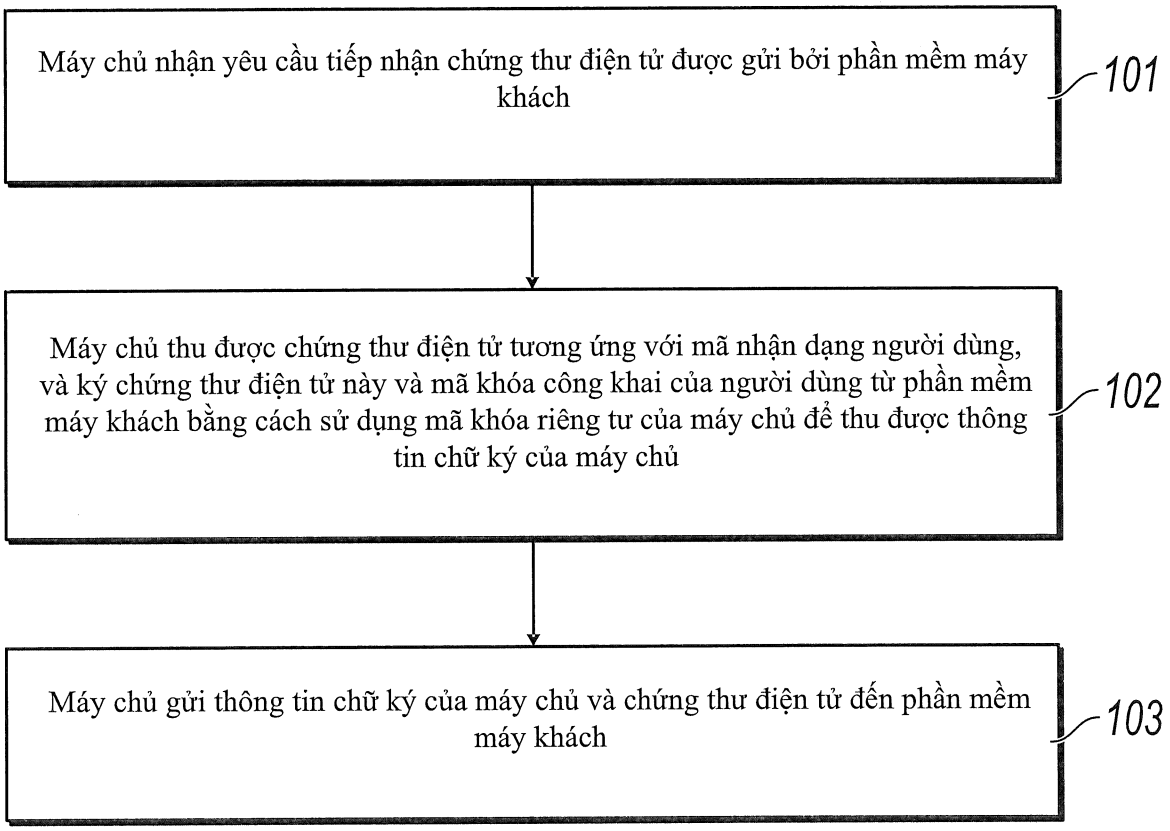

Máy chủ nhận yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách
101
Máy chủ thu được chứng thư điện tử tương ứng với mã nhận dạng người dùng, và ký chứng thư điện tử này và mã khóa công khai của người dùng từ phần mềm máy khách bằng cách sử dụng mã khóa riêng tư của máy chủ để thu được thông tin chữ ký của máy chủ
102
Máy chủ gửi thông tin chữ ký của máy chủ và chứng thư điện tử đến phần mềm máy khách
103

FIG. 2

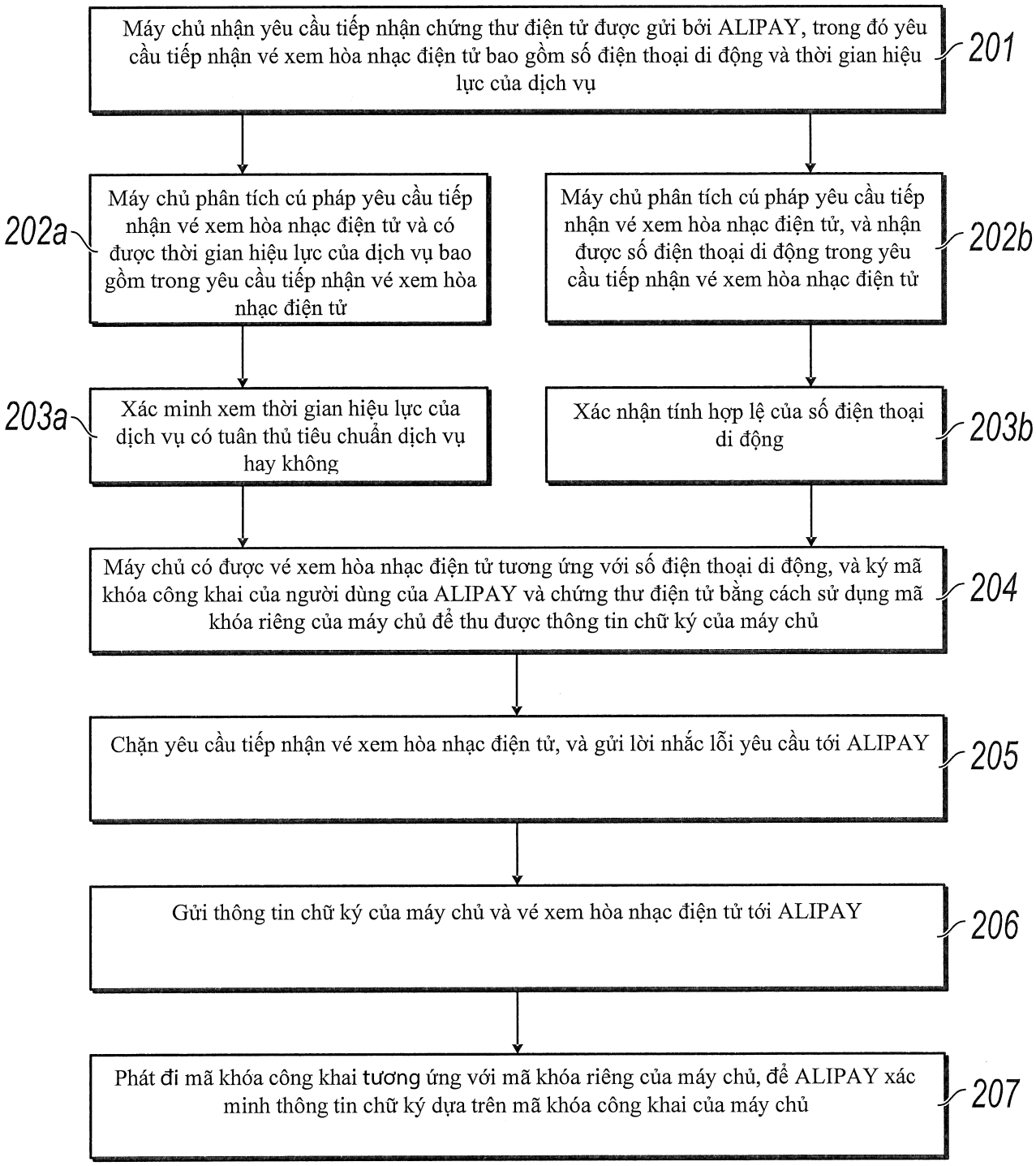

Máy chủ nhận yêu cầu tiếp nhận chứng thư điện tử được gửi bởi ALIPAY, trong đó yêu cầu tiếp nhận vé xem hòa nhạc điện tử bao gồm số điện thoại di động và thời gian hiệu lực của dịch vụ
201
Máy chủ phân tích cú pháp yêu cầu tiếp nhận vé xem hòa nhạc điện tử và có được thời gian hiệu lực của dịch vụ bao gồm trong yêu cầu tiếp nhận vé xem hòa nhạc điện tử
202a
Máy chủ phân tích cú pháp yêu cầu tiếp nhận vé xem hòa nhạc điện tử, và nhận được số điện thoại di động trong yêu cầu tiếp nhận vé xem hòa nhạc điện tử
202b
Xác minh xem thời gian hiệu lực của dịch vụ có tuân thủ tiêu chuẩn dịch vụ hay không
203a
Xác nhận tính hợp lệ của số điện thoại di động
203b
Máy chủ có được vé xem hòa nhạc điện tử tương ứng với số điện thoại di động, và ký mã khóa công khai của người dùng của ALIPAY và chứng thư điện tử bằng cách sử dụng mã khóa riêng của máy chủ để thu được thông tin chữ ký của máy chủ
204
Chặn yêu cầu tiếp nhận vé xem hòa nhạc điện tử, và gửi lời nhắc lỗi yêu cầu tới ALIPAY
205
Gửi thông tin chữ ký của máy chủ và vé xem hòa nhạc điện tử tới ALIPAY
206
Phát đi mã khóa công khai tương ứng với mã khóa riêng của máy chủ, để ALIPAY xác minh thông tin chữ ký dựa trên mã khóa công khai của máy chủ
207

FIG. 3

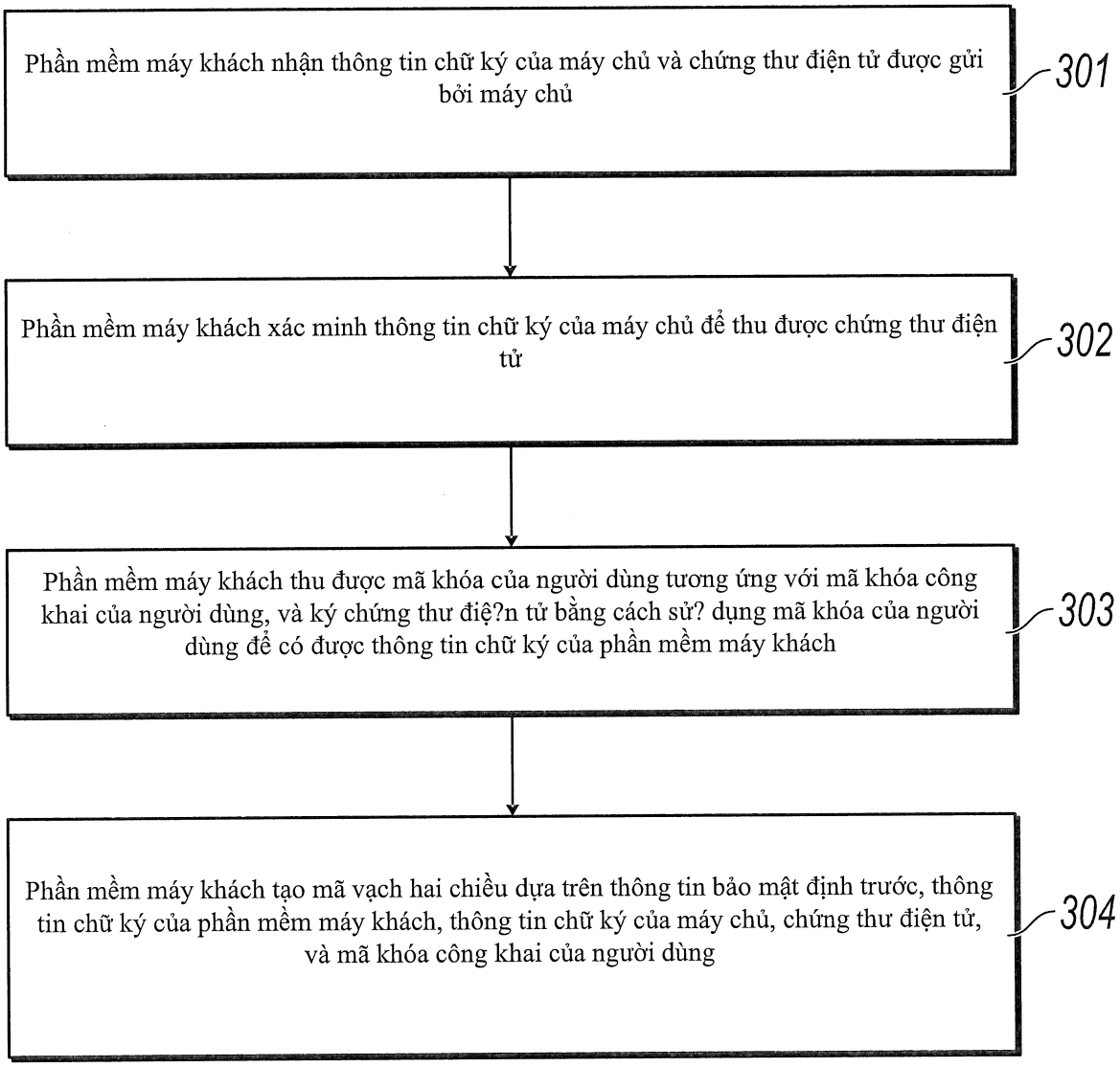

Phần mềm máy khách nhận thông tin chữ ký của máy chủ và chứng thư điện tử được gửi bởi máy chủ
301
Phần mềm máy khách xác minh thông tin chữ ký của máy chủ để thu được chứng thư điện tử
302
Phần mềm máy khách thu được mã khóa của người dùng tương ứng với mã khóa công khai của người dùng, và ký chứng thư điệ?n tử bằng cách sử? dụng mã khóa của người dùng để có được thông tin chữ ký của phần mềm máy khách
303
Phần mềm máy khách tạo mã vạch hai chiều dựa trên thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng
304

FIG. 4

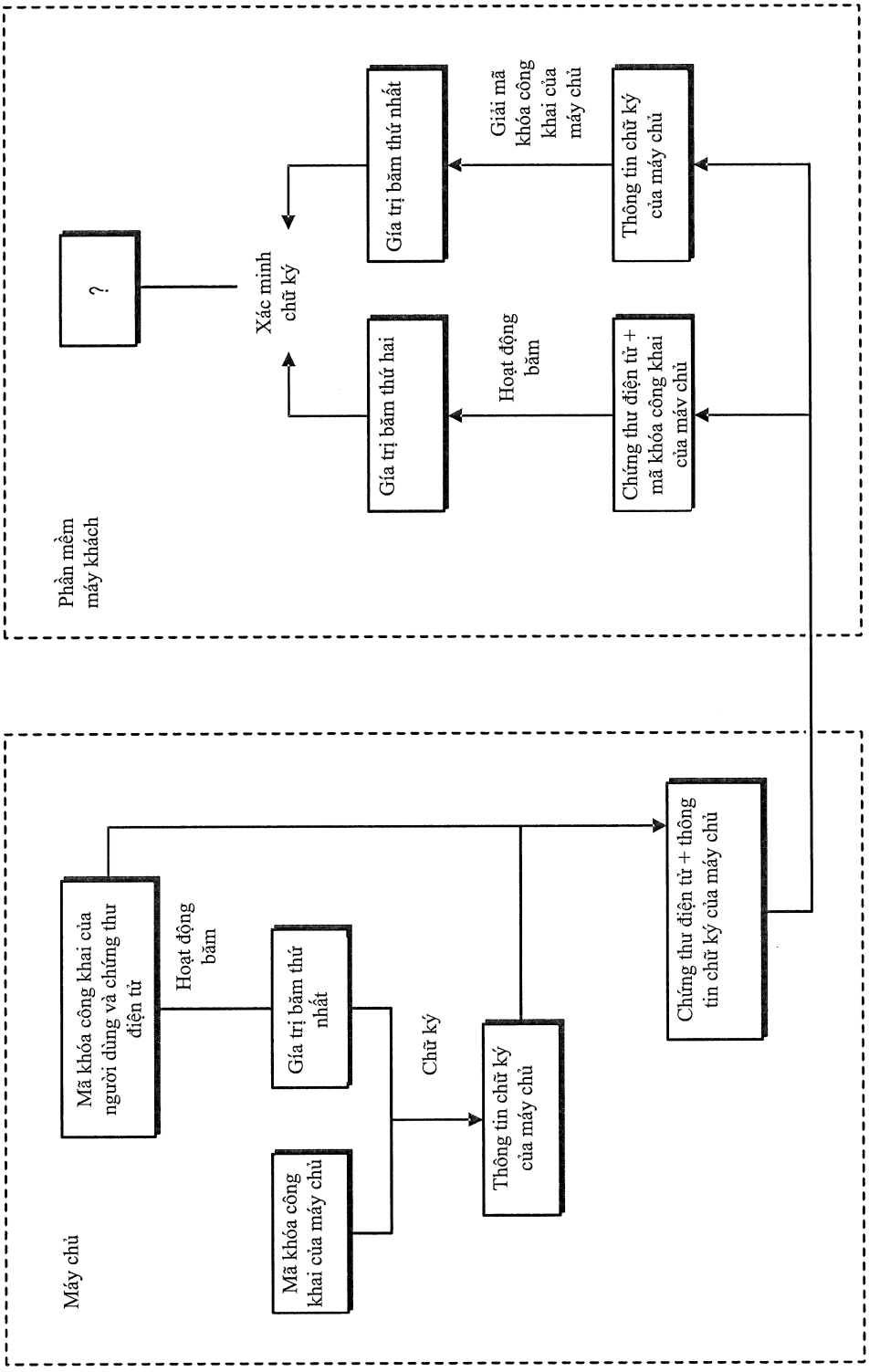

Máy chủ
Mã khóa công khai của người dùng và chứng thư điện tử
Hoạt động băm
Giá trị băm thứ nhất
Mã khóa công khai của máy chủ
Chữ ký
Thông tin chữ ký của máy chủ
Chứng thư điện tử + thông tin chữ ký của máy chủ
Phần mềm máy khách
?
Xác minh chữ ký
Giá trị băm thứ nhất
Giải mã khóa công khai của máy chủ
Thông tin chữ ký của máy chủ
Giá trị băm thứ hai
Hoạt động băm
Chứng thư điện tử + mã khóa công khai của máy chủ

FIG. 5

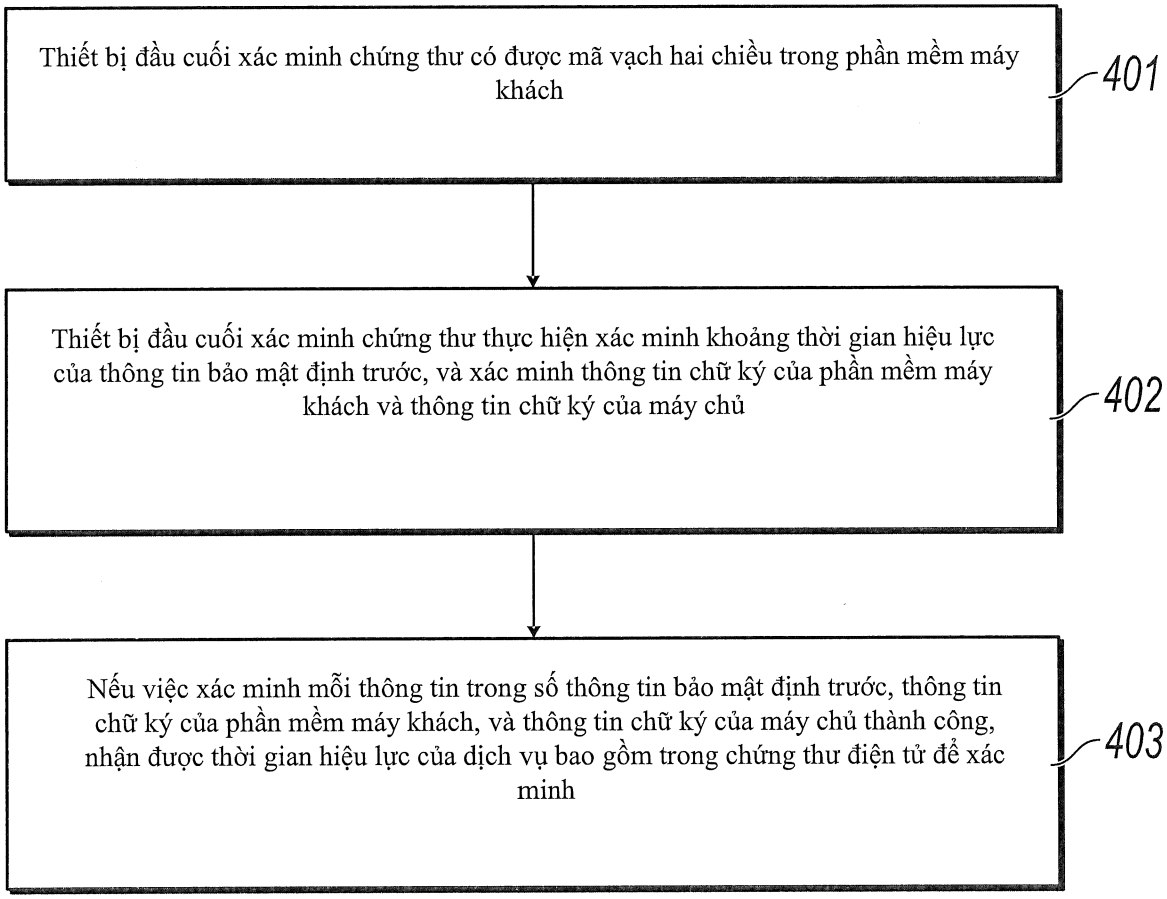

Thiết bị đầu cuối xác minh chứng thư có được mã vạch hai chiều trong phần mềm máy khách
401
Thiết bị đầu cuối xác minh chứng thư thực hiện xác minh khoảng thời gian hiệu lực của thông tin bảo mật định trước, và xác minh thông tin chữ ký của phần mềm máy khách và thông tin chữ ký của máy chủ
402
Nếu việc xác minh mỗi thông tin trong số thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, và thông tin chữ ký của máy chủ thành công, nhận được thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử để xác minh
403

FIG. 6

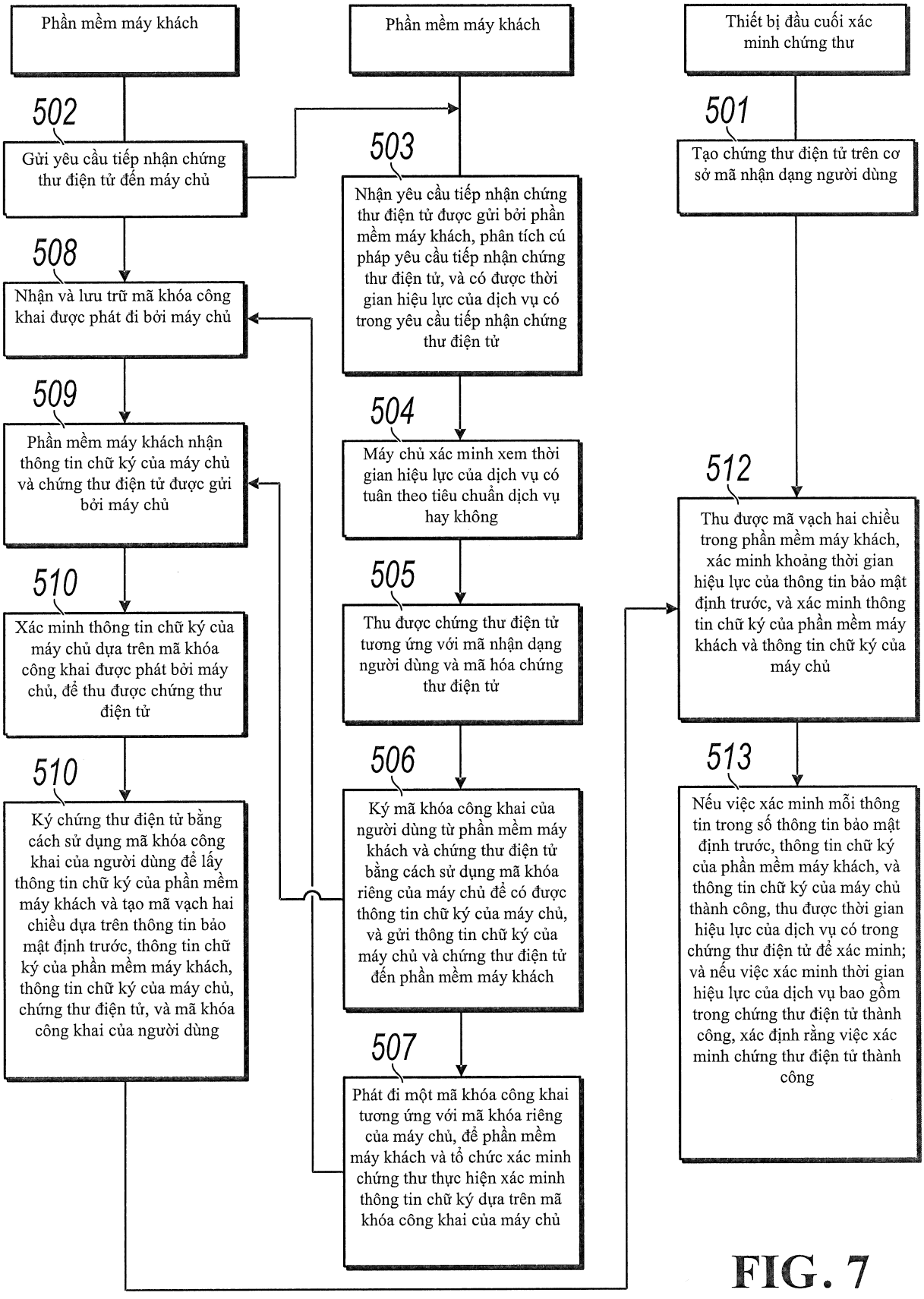

Phần mềm máy khách
Phần mềm máy khách
Thiết bị đầu cuối xác minh chứng thư
502
Gửi yêu cầu tiếp nhận chứng thư điện tử đến máy chủ
503
Nhận yêu cầu tiếp nhận chứng thư điện tử được gửi bởi phần mềm máy khách, phân tích cú pháp yêu cầu tiếp nhận chứng thư điện tử, và có được thời gian hiệu lực của dịch vụ có trong yêu cầu tiếp nhận chứng thư điện tử
501
Tạo chứng thư điện tử trên cơ sở mã nhận dạng người dùng
508
Nhận và lưu trữ mã khóa công khai được phát đi bởi máy chủ
509
Phần mềm máy khách nhận thông tin chữ ký của máy chủ và chứng thư điện tử được gửi bởi máy chủ
504
Máy chủ xác minh xem thời gian hiệu lực của dịch vụ có tuân theo tiêu chuẩn dịch vụ hay không
512
Thu được mã vạch hai chiều trong phần mềm máy khách, xác minh khoảng thời gian hiệu lực của thông tin bảo mật định trước, và xác minh thông tin chữ ký của phần mềm máy khách và thông tin chữ ký của máy chủ
510
Xác minh thông tin chữ ký của máy chủ dựa trên mã khóa công khai được phát bởi máy chủ, để thu được chứng thư điện tử
505
Thu được chứng thư điện tử tương ứng với mã nhận dạng người dùng và mã hóa chứng thư điện tử
513
Nếu việc xác minh mỗi thông tin trong số thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, và thông tin chữ ký của máy chủ thành công, thu được thời gian hiệu lực của dịch vụ có trong chứng thư điện tử để xác minh; và nếu việc xác minh thời gian hiệu lực của dịch vụ bao gồm trong chứng thư điện tử thành công, xác định rằng việc xác minh chứng thư điện tử thành công
510
Ký chứng thư điện tử bằng cách sử dụng mã khóa công khai của người dùng để lấy thông tin chữ ký của phần mềm máy khách và tạo mã vạch hai chiều dựa trên thông tin bảo mật định trước, thông tin chữ ký của phần mềm máy khách, thông tin chữ ký của máy chủ, chứng thư điện tử, và mã khóa công khai của người dùng
506
Ký mã khóa công khai của người dùng từ phần mềm máy khách và chứng thư điện tử bằng cách sử dụng mã khóa riêng của máy chủ để có được thông tin chữ ký của máy chủ, và gửi thông tin chữ ký của máy chủ và chứng thư điện tử đến phần mềm máy khách
507
Phát đi một mã khóa công khai tương ứng với mã khóa riêng của máy chủ, để phần mềm máy khách và tổ chức xác minh chứng thư thực hiện xác minh thông tin chữ ký dựa trên mã khóa công khai của máy chủ

FIG. 7

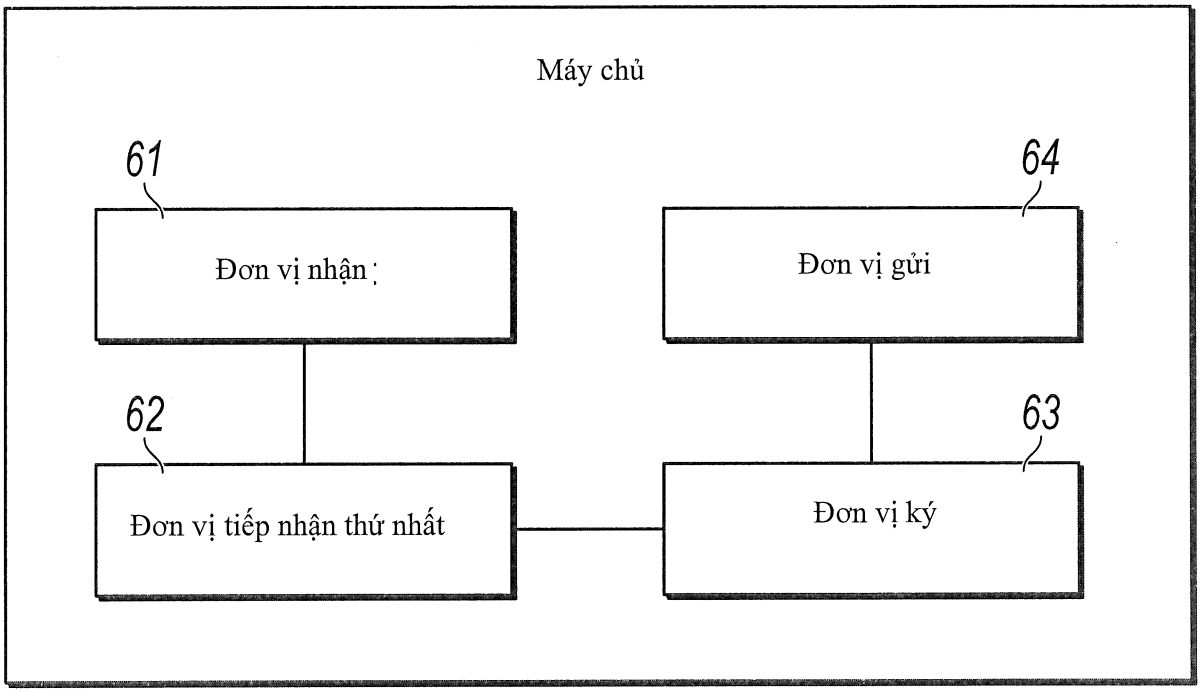

Máy chủ
61
Đơn vị nhận
64
Đơn vị gửi
62
Đơn vị tiếp nhận thứ nhất
63
Đơn vị ký

FIG. 8

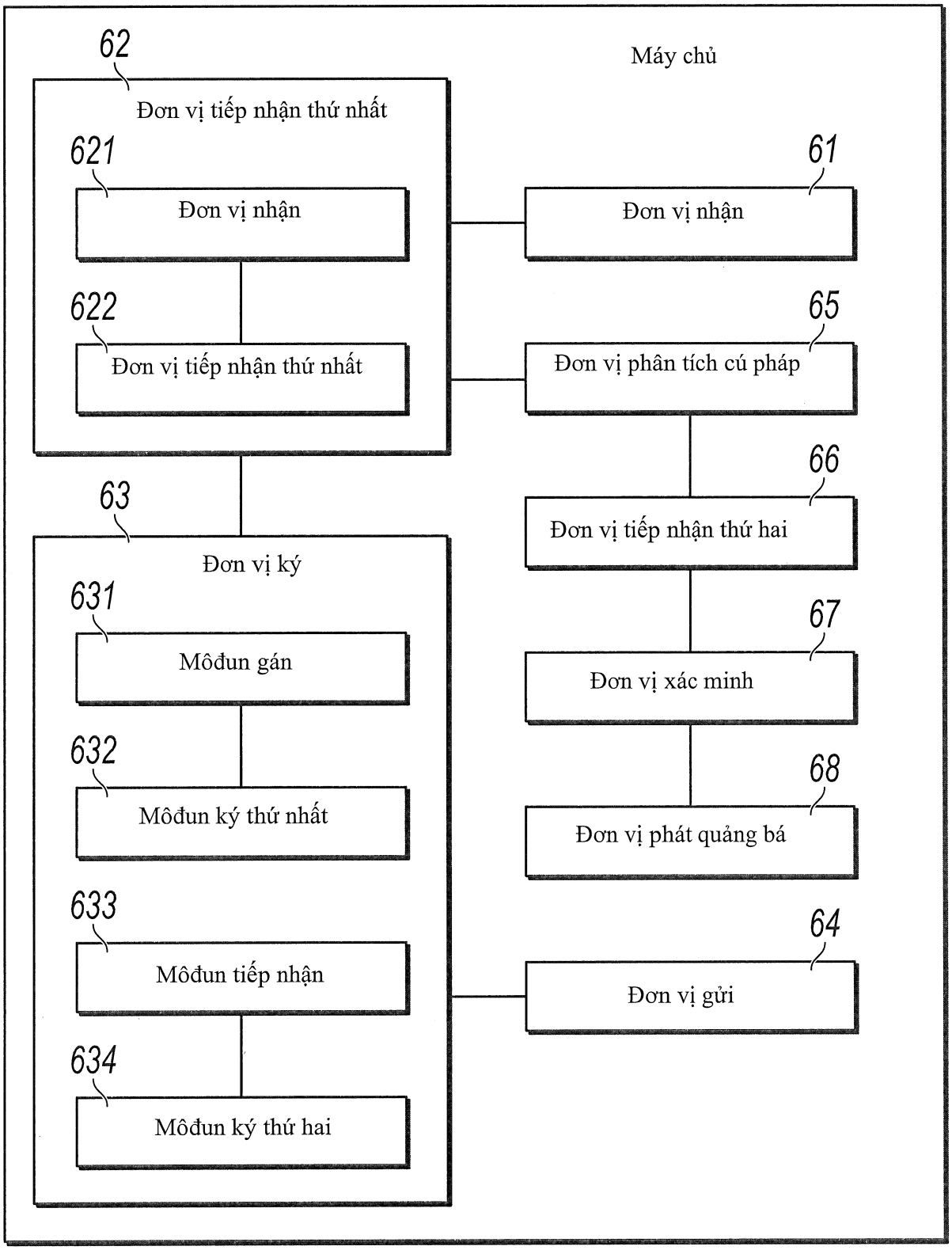

Máy chủ
62
Đơn vị tiếp nhận thứ nhất
621
Đơn vị nhận
622
Đơn vị tiếp nhận thứ nhất
63
Đơn vị ký
631
Môđun gán
632
Môđun ký thứ nhất
633
Môđun tiếp nhận
634
Môđun ký thứ hai
61
Đơn vị nhận
65
Đơn vị phân tích cú pháp
66
Đơn vị tiếp nhận thứ hai
67
Đơn vị xác minh
68
Đơn vị phát quảng bá
64
Đơn vị gửi

FIG. 9

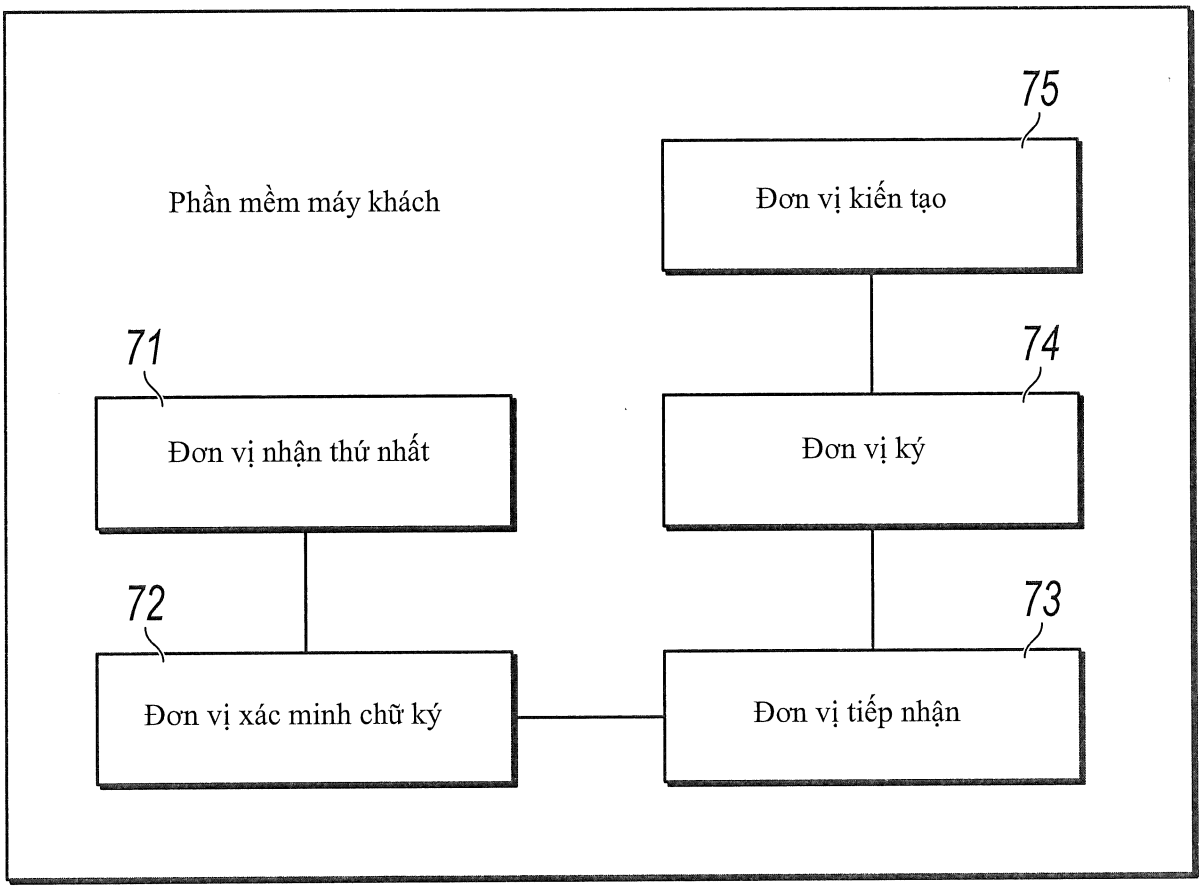

Phần mềm máy khách
75
Đơn vị kiến tạo
71
Đơn vị nhận thứ nhất
74
Đơn vị ký
72
Đơn vị xác minh chữ ký
73
Đơn vị tiếp nhận

FIG. 10

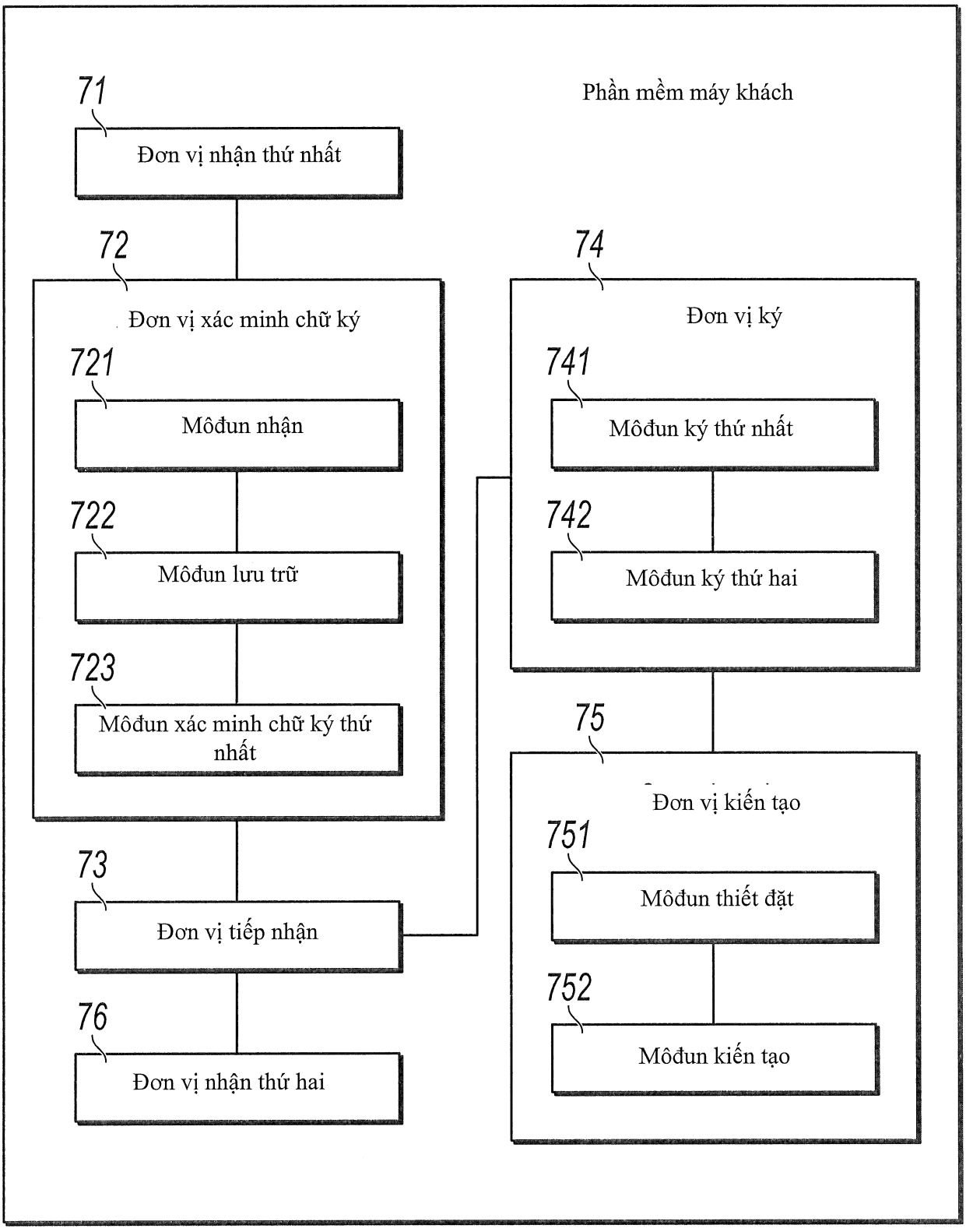

Phần mềm máy khách
71
Đơn vị nhận thứ nhất
72
Đơn vị xác minh chữ ký
721
Môđun nhận
722
Môđun lưu trữ
723
Môđun xác minh chữ ký thứ nhất
73
Đơn vị tiếp nhận
76
Đơn vị nhận thứ hai
74
Đơn vị ký
741
Môđun ký thứ nhất
742
Môđun ký thứ hai
75
Đơn vị kiến tạo
751
Môđun thiết đặt
752
Môđun kiến tạo

FIG. 11

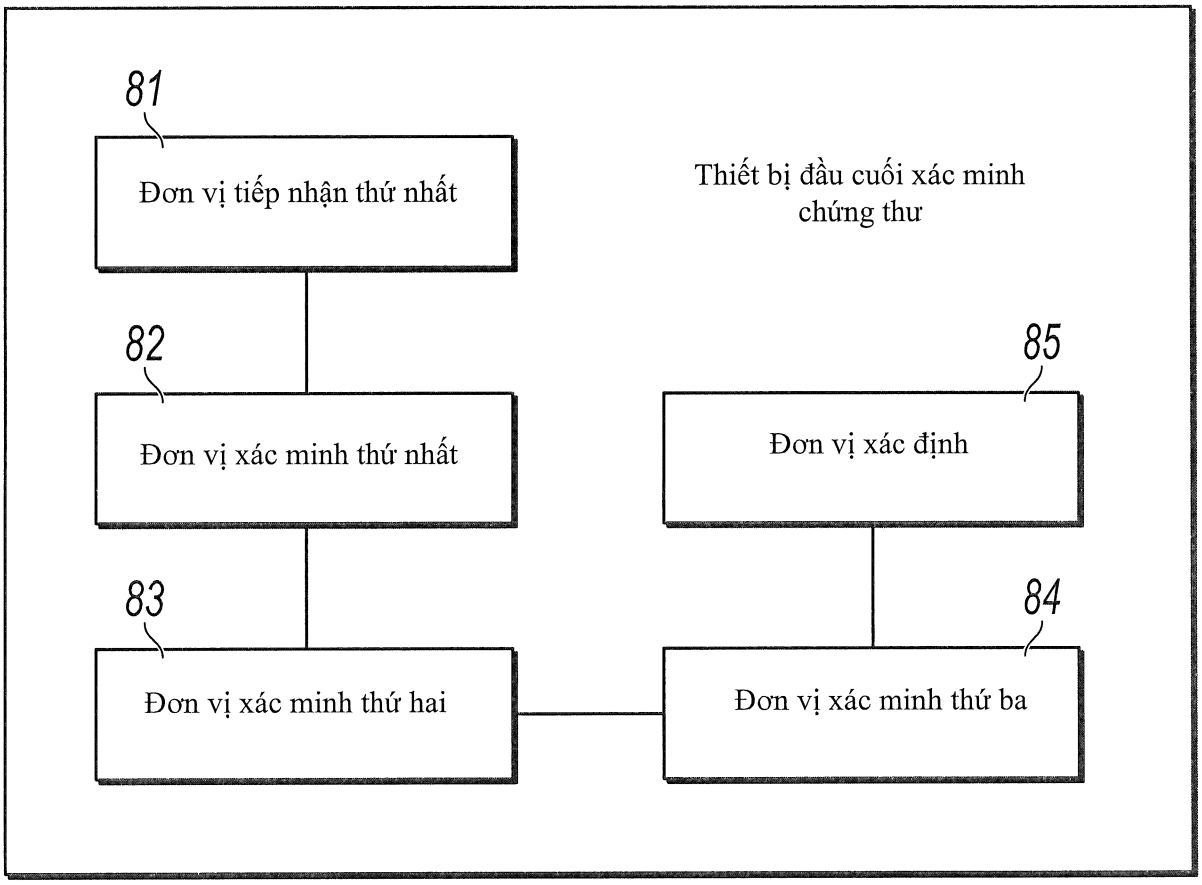

81
Đơn vị tiếp nhận thứ nhất
Thiết bị đầu cuối xác minh chứng thư
82
Đơn vị xác minh thứ nhất
85
Đơn vị xác định
83
Đơn vị xác minh thứ hai
84
Đơn vị xác minh thứ ba

FIG. 12

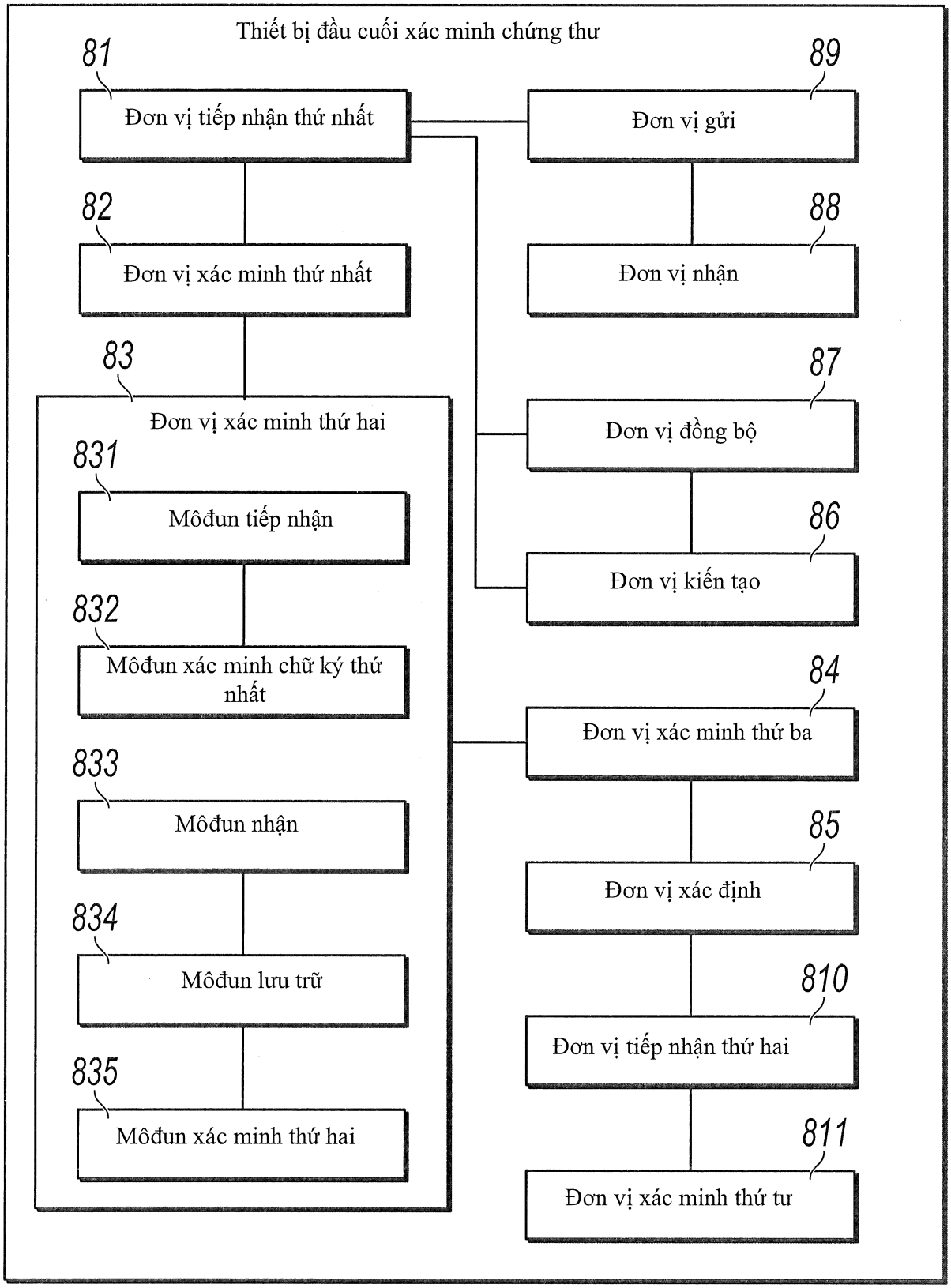

Thiết bị đầu cuối xác minh chứng thư
81
Đơn vị tiếp nhận thứ nhất
82
Đơn vị xác minh thứ nhất
83
Đơn vị xác minh thứ hai
831
Môđun tiếp nhận
832
Môđun xác minh chữ ký thứ nhất
833
Môđun nhận
834
Môđun lưu trữ
835
Môđun xác minh thứ hai
89
Đơn vị gửi
88
Đơn vị nhận
87
Đơn vị đồng bộ
86
Đơn vị kiến tạo
84
Đơn vị xác minh thứ ba
85
Đơn vị xác định
810
Đơn vị tiếp nhận thứ hai
811
Đơn vị xác minh thứ tư

FIG. 13

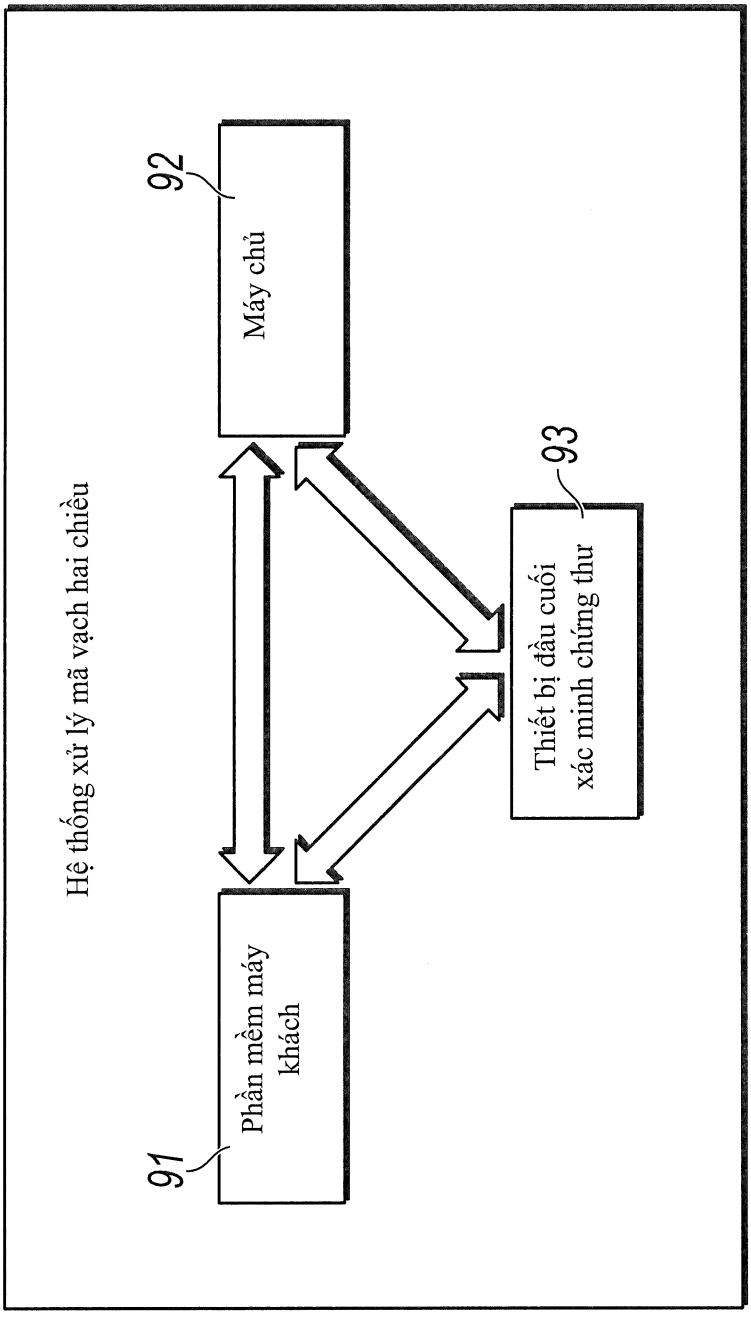

Hệ thống xử lý mã vạch hai chiều
92
Máy chủ
93
Thiết bị đầu cuối xác minh chứng thư
91
Phần mềm máy khách

FIG. 14