(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) **1-0023919**

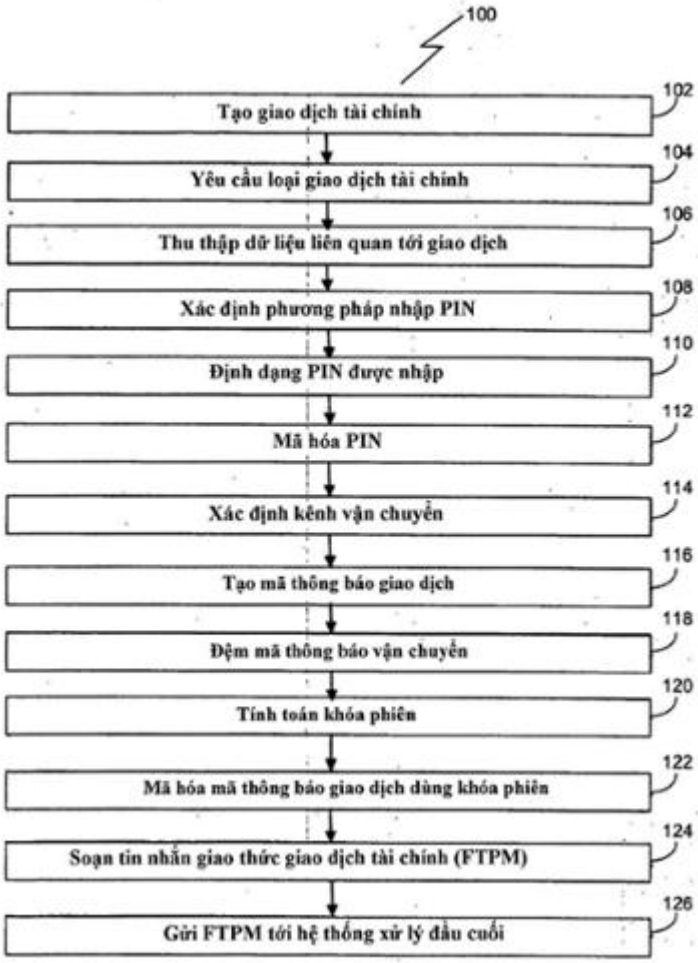
(51)[7] **H04L 9/32**; G06Q 40/00

(13) **B**

(21) 1-2013-01766
(22) 10/11/2010
(86) PCT/SG2010/000427 10/11/2010
(87) WO2012/064280 18/05/2012
(45) 25/06/2020 387
(43) 25/11/2013 308A
(73) EINNOVATIONS HOLDINGS PTE. LTD. (SG)
100 Beach Road, #25-06 Shaw Towers, Singapore 189702, Singapore
(72) IBASCO, Alex D. (PH); POSADAS, Patrick B. (PH); CO, Vincent C. (PH); YU, William Emmanuel S. (PH)
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP THỰC HIỆN GIAO DỊCH TÀI CHÍNH THÔNG QUA CƠ SỞ HẠ TẦNG LIÊN LẠC VIỄN THÔNG CÔNG CỘNG KHÔNG ĐƯỢC BẢO ĐẢM AN NINH VÀ THIẾT BỊ ĐỂ THỰC HIỆN PHƯƠNG PHÁP NÀY

(57) Sáng chế đề cập tới phương pháp thực hiện giao dịch tài chính thông qua cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh bao gồm: thu thập dữ liệu liên quan tới loại giao dịch tài chính được chỉ rõ; tạo mã thông báo giao dịch bao gồm dữ liệu được thu thập và/hoặc dữ liệu được lấy ra từ dữ liệu được thu thập; mã hóa mã thông báo giao dịch; tạo tin nhắn giao thức giao dịch tài chính tích hợp mã thông báo giao dịch đã được mã hóa là phụ thuộc vào kênh vận chuyển được chọn mà qua đó tin nhắn được vận chuyển; và vận chuyển tin nhắn giao thức giao dịch tài chính sử dụng kênh vận chuyển được chọn và bằng cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh tới đích, trong đó tin nhắn giao thức giao dịch tài chính còn được tiếp tục xử lý.


100
Tạo giao dịch tài chính
102
Yêu cầu loại giao dịch tài chính
104
Thu thập dữ liệu liên quan tới giao dịch
106
Xác định phương pháp nhập PIN
108
Định dạng PIN được nhập
110
Mã hóa PIN
112
Xác định kênh vận chuyển
114
Tạo mã thông báo giao dịch
116
Đệm mã thông báo vận chuyển
118
Tính toán khóa phiên
120
Mã hóa mã thông báo giao dịch dùng khóa phiên
122
Soạn tin nhắn giao thức giao dịch tài chính (FTPM)
124
Gửi FTPM tới hệ thống xử lý đầu cuối
126

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập tới phương pháp thực hiện giao dịch tài chính thông qua cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh và thiết bị tương tự. Sáng chế đặc biệt thích hợp cho việc vận hành điện thoại di động theo cách về cơ bản là giống với các thiết bị đầu cuối thanh toán điểm bán hàng (Point Of Sale - "POS") hiện có được sử dụng để xử lý các giao dịch thẻ ghi nợ và thẻ tín dụng.

Tình trạng kỹ thuật của sáng chế

Thảo luận dưới đây của tình trạng kỹ thuật cho sáng chế nhằm mục đích tạo thuận lợi cho việc hiểu sáng chế này. Tuy nhiên, cần hiểu rằng phần thảo luận này không phải là xác nhận hoặc thừa nhận rằng nội dung được đề cập tới được công bố, đã biết hoặc là một phần của hiểu biết chung tại thời điểm ưu tiên của sáng chế.

Các giao dịch mô đun ứng dụng an ninh thanh toán (Payment Security Application Module - "PSAM") hiện hoạt động với giả định rằng có kết nối an toàn giữa thiết bị đầu cuối và các hệ thống đầu cuối phía sau để đạt được thiết lập tài chính. Kết quả là, cơ chế an ninh duy nhất được sử dụng trong các giao dịch này là việc mã hóa của khối số nhận diện cá nhân (personal identification number - "PIN").

Trong khi giả định này có một vài giá trị cho các thiết bị đầu cuối có các đường dành riêng và các cấu trúc định tuyến để thu được thiết lập tài chính, vẫn có thể chặn việc truyền dẫn theo sau thông qua cấu trúc này.

Trái lại, người nộp đơn đã phát triển sáng chế này dựa trên giả định trái ngược rằng không có kết nối an toàn giữa thiết bị đầu cuối và hệ thống đầu cuối phía sau. Kết quả là, sáng chế của người nộp đơn cho phép sử dụng cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh để quản lý các giao dịch PSAM, như dịch vụ tin nhắn ngắn ("SMS"). Tuy nhiên, việc sử dụng của cơ sở hạ tầng SMS và các giao thức để quản lý các giao dịch tài chính còn có các vấn đề, trong lượng dữ liệu hạn chế có thể

được sử dụng để truyền thông các giao dịch này và cản trở vốn có của nó cho các phần đầu dữ liệu cao thông thường của việc mã hóa.

Tại cùng một thời điểm, các mô tả về phần cứng cho việc thực hiện các ứng dụng PSAM đã được xác định trong tài liệu "*Terminal Architecture for PSAM Application*" được công bố bởi tổ chức quốc tế Europay, thuộc hiệp hội dịch vụ quốc tế Visa và PBS A/S vào năm 2000. Tuy nhiên, như được mô tả bởi tài liệu này, PSAM là thiết bị đầu cuối được tiêu chuẩn hóa có cấu trúc phụ thuộc vào kiến trúc.

Kết quả đã được phát triển cho các thiết bị đầu cuối điểm bán hàng cụ thể với phần cứng dành riêng. Trong trường hợp các thiết bị đầu cuối điểm bán hàng di động, chip PSAM quản lý tất cả các chức năng PSAM, trong khi thẻ SIM tách biệt quản lý việc vận chuyển của dữ liệu được tạo ra bởi PSAM qua mạng không dây.

Kết quả của kiến trúc này:

- Yếu tố hình dạng của thiết bị đầu cuối điểm bán hàng di động phải có đủ kích thước để chứa hai chip tách biệt (chip PSAM và thẻ SIM); và
- Các thiết bị SIM của người sử dụng, như các điện thoại di động, không có khả năng để được sử dụng để quản lý các ứng dụng PSAM.

Hạn chế sau, được kết hợp với giá thành cao của phần cứng PSAM dành riêng, kiềm chế sự chấp nhận sử dụng PSAM của người bán hàng để quản lý các giao dịch tài chính.

Bản chất kỹ thuật của sáng chế

Trong suốt tài liệu này, trừ khi được chỉ rõ theo cách khác, các thuật ngữ "bao gồm", "tạo thành từ", và dạng tương tự, được coi là không làm hạn chế, hoặc theo nghĩa khác, nghĩa là "bao gồm, nhưng không giới hạn ở".

Theo khía cạnh thứ nhất, sáng chế đề xuất phương pháp thực hiện giao dịch tài chính thông qua cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh bao gồm các bước:

thu thập dữ liệu liên quan tới loại giao dịch tài chính được chỉ rõ;

tạo mã thông báo giao dịch bao gồm dữ liệu được thu thập và/hoặc dữ liệu được lấy ra từ dữ liệu được thu thập;

mã hóa mã thông báo giao dịch;

tạo tin nhắn giao thức giao dịch tài chính tích hợp mã thông báo giao dịch đã được mã hóa là phụ thuộc vào kênh vận chuyển được chọn mà qua đó tin nhắn được vận chuyển; và

vận chuyển tin nhắn giao thức giao dịch tài chính sử dụng kênh vận chuyển được chọn và theo cách của cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh tới đích, trong đó tin nhắn giao thức giao dịch tài chính còn được tiếp tục xử lý.

Bước thu thập dữ liệu liên quan tới loại giao dịch được chỉ rõ có thể còn bao gồm bước phụ thu thập dữ liệu xác thực mà sau đó được mã hóa, mã thông báo giao dịch được tạo ra sau đó bao gồm dữ liệu xác thực được mã hóa. Dữ liệu mã thông báo giao dịch cũng có thể được định dạng và/hoặc được mã hóa.

Bước thu thập dữ liệu liên quan tới loại giao dịch tài chính được chỉ rõ cũng có thể bao gồm thu dữ liệu bởi ít nhất một trong các cách sau: từ các tệp được lưu trên thiết bị được sử dụng để thu dữ liệu; từ bộ phận đọc dữ liệu được kết hợp với, hoặc được tích hợp vào, thiết bị được sử dụng để thu dữ liệu; từ khách hàng theo cách của giao diện người sử dụng của thiết bị được sử dụng để thu dữ liệu. Dữ liệu vì thế được thu có thể bao gồm bộ các quy tắc giao dịch có khả năng áp dụng cho loại giao dịch tài chính.

Mã thông báo giao dịch cũng có thể được đệm khi được yêu cầu cho kênh vận chuyển được chọn.

Phương pháp cũng có thể bao gồm bước tính toán khóa phiên, khóa phiên sau đó được sử dụng để mã hóa mã thông báo giao dịch trong suốt bước mã hóa mã thông báo giao dịch.

Kênh vận chuyển được chọn có thể là hệ thống radio gói chung (General Packet Radio System - "GPRS") hoặc SMS.

Trong đó, kênh vận chuyển được chọn là GPRS, bước tạo mã thông báo giao dịch có thể bao gồm các bước phụ:

gắn kèm giá trị dữ liệu ghi mã thông báo kết thúc vào mã thông báo giao dịch; và

đệm mã thông báo giao dịch với các giá trị trống cho tới khi mã thông báo giao dịch được thay đổi là nhiều lần của 8 bai.

Một cách tương tự, bước mã hóa mã thông báo giao dịch còn bao gồm các bước phụ tính toán khóa phiên mã xác thực tin nhắn và mã hóa mã thông báo giao dịch được thay đổi và được đệm bằng cách sử dụng khóa phiên mã xác thực tin nhắn.

Cũng vậy, khi kênh vận chuyển được chọn là GPRS, bước tạo tin nhắn giao thức giao dịch tài chính có thể bao gồm bước phụ tạo số chuỗi khóa và trong đó, tin nhắn giao thức giao dịch tài chính vì thế được tạo ra bao gồm số chuỗi khóa mã thông báo giao dịch và khóa phiên mã xác thực tin nhắn.

Trong trường hợp kênh vận chuyển được chọn là SMS, bước tạo mã thông báo giao dịch còn bao gồm các bước phụ xác định bộ đếm đệm và bộ đếm tin nhắn và gắn kèm bộ đếm đệm và bộ đếm tin nhắn cho tin nhắn. Bước mã hóa mã thông báo giao dịch cũng có thể bao gồm bước phụ mã hóa mã thông báo giao dịch bằng cách sử dụng khóa mã hóa dựa trên các đặc tả tiêu chuẩn 3GPP TS 03.48.

Khi kênh vận chuyển được chọn cũng là SMS, bước tạo tin nhắn giao thức giao dịch tài chính có thể chứa bước phụ đặt tiền tố mã thông báo giao dịch đã được mã hóa với phần đầu SMS.

Theo khía cạnh thứ hai, sáng chế đề xuất thiết bị truyền thông để tạo thuận lợi cho hiệu quả hoạt động giao dịch tài chính thông qua cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh, thiết bị truyền thông này có thể vận hành được để thực hiện phần mềm được lưu trên đó hoặc trên phương tiện có thể tháo rời được trong truyền thông dữ liệu và điều khiển với thiết bị để:

thu thập dữ liệu liên quan tới loại giao dịch tài chính được chỉ rõ;

tạo mã thông báo giao dịch bao gồm dữ liệu được thu thập và/hoặc dữ liệu được lấy ra từ dữ liệu được thu thập;

mã hóa mã thông báo giao dịch;

tạo tin nhắn giao thức giao dịch tài chính tích hợp mã thông báo giao dịch đã được mã hóa là phụ thuộc vào kênh vận chuyển được chọn mà qua đó tin nhắn được vận chuyển; và

vận chuyển tin nhắn giao thức giao dịch tài chính bằng cách sử dụng kênh vận chuyển được chọn và theo cách của cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh tới đích, trong đó tin nhắn giao thức giao dịch tài chính còn được tiếp tục xử lý.

Dữ liệu được thu thập có thể bao gồm dữ liệu xác thực. Mã thông báo giao dịch có thể bao gồm dữ liệu xác thực ở dạng được mã hóa.

Thiết bị truyền thông cũng có thể bao gồm bộ đọc để đọc thông tin được lưu trên các thiết bị ngoại vi.

Ưu tiên là, thiết bị truyền thông là có thể vận hành được để truyền thông theo cách của một hoặc nhiều kênh vận chuyển sau: GPRS; SMS.

Theo khía cạnh thứ ba, sáng chế đề xuất thẻ bao gồm ít nhất một mạch tích hợp, thẻ có kích thước và hình dạng tương tự như thẻ mô đun nhận diện thuê bao (Subscriber Identity Module - "SIM") truyền thống, trong đó khi thẻ được nhận trong thiết bị có giao diện thẻ SIM, phần mềm có thể thực hiện được được lưu trên các phương tiện nhớ của ít nhất một mạch tích hợp, khi được thực hiện, có khả năng truyền thông với phần mềm được lưu trên thiết bị để nhờ đó cho phép thiết bị cung cấp cả các chức năng SIM và PSAM cho người sử dụng thiết bị.

Thiết bị có thể chỉ có khả năng được vận hành như là SIM hoặc PSAM tại thời điểm bất kỳ và truyền thông giữa phần mềm được lưu trên các phương tiện nhớ và phần mềm được lưu trên thiết bị là theo cách của kênh truyền thông logic.

Mô tả vắn tắt các hình vẽ

Sáng chế sẽ được mô tả, theo cách chỉ làm ví dụ, có tham chiếu đến các hình vẽ kèm theo, trong đó:

Fig.1 là lưu đồ của phương án thực hiện thứ nhất của sáng chế này.

Fig.2 là mô tả chung của phần cứng được sử dụng trong phương án thực hiện thứ nhất của sáng chế này.

Fig.3 là thể hiện đồ họa của mã thông báo giao dịch như được sử dụng trong sáng chế này.

Fig.4 là lưu đồ thứ nhất của phương án thực hiện thứ hai của sáng chế này.

Fig.5 là lưu đồ thứ hai của phương án thực hiện thứ hai của sáng chế này.

Fig.6 là mô tả chung của thiết bị truyền thông tích hợp cả chức năng SIM và PSAM.

Mô tả chi tiết sáng chế

Theo phương án thực hiện thứ nhất, sáng chế đề xuất phương pháp thực hiện giao dịch tài chính thông qua cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh 100. Lưu đồ của phương pháp 100 được thể hiện trên Fig.1.

Các thực thể dưới đây hoạt động theo phương pháp bao gồm đơn vị đầu cuối 10 và hệ thống xử lý đầu cuối 12. Ứng dụng thanh toán 14 là chương trình thực hiện được trên đơn vị đầu cuối 10. Theo phương án thực hiện này, ứng dụng thanh toán 14 cũng được lưu trong bộ nhớ 16 của đơn vị đầu cuối 10.

Ngoài mã thực hiện được tạo thành cơ sở cho ứng dụng thanh toán 14, ứng dụng thanh toán 14 cũng bao gồm nhiều tệp dữ liệu 18. Các tệp dữ liệu 18 lưu dữ liệu được cần bởi ứng dụng thanh toán 14 trong suốt các phiên ứng dụng/giao dịch khác nhau. Các loại dữ liệu được lưu trong nhiều tệp dữ liệu 18 bao gồm:

- Dữ liệu an ninh;
- Dữ liệu kết nối; và
- Dữ liệu giao dịch.

Trong trường hợp của dữ liệu giao dịch, thông tin thông thường được lưu bao gồm nhận diện thiết bị di động toàn cầu (International Mobile Equipment Identity) của đơn vị đầu cuối 10; các quy tắc xử lý cho các giao dịch có thể khác nhau để được quản lý bởi

ứng dụng thanh toán 14; mã nhận diện duy nhất của hệ thống xử lý đầu cuối 12; và bản sao tạm thời của mã thông báo giao dịch cuối cùng.

Ứng dụng thanh toán 14 cũng duy trì nhật ký giao dịch 20. Nhật ký giao dịch 20 chứa các chi tiết được chọn của ít nhất ba giao dịch trước đó được quản lý bởi ứng dụng thanh toán 14 (bao gồm các chi tiết được chọn của trả lời bất kỳ được đưa ra bởi hệ thống xử lý đầu cuối 12). Thông tin được chọn lọc này cho phép ứng dụng thanh toán 14 xác nhận các giao dịch nào đã diễn ra cho các mục đích giải quyết tranh chấp và cũng là các phương tiện để tạo thuận tiện cho việc hủy giao dịch trong quá khứ.

Cũng cần chú ý rằng để loại bỏ việc trùng lặp, yêu cầu lặp lại giao dịch bất kỳ được tạo bởi ứng dụng thanh toán 14 không được lưu một cách tách biệt trong nhật ký giao dịch 20. Khi yêu cầu lặp lại giao dịch được tạo ra, bộ đếm lần thử lại được kết hợp với yêu cầu được tăng để ghi lại yêu cầu này.

Nhật ký giao dịch 20 là tệp dữ liệu chỉ đọc. Nhật ký giao dịch 20 duy trì dữ liệu liên quan tới các giao dịch trước đó trên cơ sở vào trước, ra trước.

Phương pháp theo phương án thực hiện thứ nhất hiện được mô tả như sau.

Người sử dụng duyệt giao diện người sử dụng của đơn vị đầu cuối theo cách để ra lệnh cho đơn vị đầu cuối rằng giao dịch tài chính mới được tạo ra (Bước 102).

Khi chỉ thị được tạo ra thể hiện rằng giao dịch tài chính mới được tạo ra, đơn vị đầu cuối yêu cầu người sử dụng loại giao dịch tài chính mới (Bước 104). Người sử dụng có lựa chọn để chỉ rõ một trong các loại giao dịch tài chính sau:

- Yêu cầu giao dịch;
- Yêu cầu lặp lại giao dịch; và
- Yêu cầu hủy giao dịch.

Một dạng của mỗi giao dịch trong các loại giao dịch tài chính này được thông báo bởi kênh vận chuyển được sử dụng, phương pháp theo phương án thực hiện này của sáng chế sẽ được mô tả đơn thuần trong ngữ cảnh của yêu cầu giao dịch.

Phần mô tả dưới đây chỉ ra rằng giao dịch tài chính mới là yêu cầu giao dịch, đơn vị đầu cuối vận hành để thu thập dữ liệu liên quan tới giao dịch (Bước 106). Thông tin này tới từ ba nguồn:

- Tự bản thân đơn vị đầu cuối, bao gồm các hệ thống tệp được lưu của nó;
- Thẻ tín dụng/thẻ ghi nợ của khách hàng; và/hoặc
- Tự bản thân khách hàng.

Một thành phần của thông tin được yêu cầu là PIN của người sử dụng.

Nhu cầu cho và phương pháp mà nhờ đó PIN được nhập vào được quản lý bởi các quy tắc xử lý được bao trong các hệ thống tệp được lưu của đơn vị đầu cuối (Bước 108). Trong các tình huống trong đó, PIN được yêu cầu nhập vào, có hai phương pháp để nhập PIN được thiết kế bởi phương án thực hiện của sáng chế này:

- Nhập theo cách của đơn vị đầu cuối; hoặc
- Nhập theo cách của phiên SIM Tool Kit ("STK").

Theo phương án thực hiện này, các quy tắc xử lý chỉ rõ rằng PIN nên được nhập vào theo cách của đơn vị đầu cuối.

Trong đó, mục PIN là theo cách của đơn vị đầu cuối, người sử dụng đơn giản là nhập pin sử dụng giao diện người sử dụng được tạo ra. PIN sau đó được định dạng như là khối ISO-0 PIN (Bước 110). Khối PIN sau đó được mã hóa sử dụng khóa PIN để truyền tới hệ thống xử lý đầu cuối. (Bước 112)

Khi đã thu được tất cả các thông tin cần thiết và liên quan, thông tin được phân loại và được sử dụng để tạo mã thông báo giao dịch (Bước 116). Tuy nhiên, trước khi mã thông báo giao dịch có thể được tạo ra một cách phù hợp, kênh vận chuyển của giao dịch tài chính cuối cùng phải được xác định (Bước 114). Kênh vận chuyển có thể theo cách của cơ sở hạ tầng liên lạc viễn thông công cộng bất kỳ không được đảm bảo an ninh có khả năng quản lý tin nhắn.

Khi kênh vận chuyển đã được xác định, mã thông báo giao dịch ban đầu được tạo ra. Mã thông báo giao dịch ban đầu bao gồm ba thành phần:

- Bộ phận nhận diện loại tin nhắn (Message Type Identifier). Bộ phận nhận diện loại tin nhắn chỉ thị loại tin nhắn được gửi (tức là yêu cầu giao dịch; yêu cầu lặp lại giao dịch; hoặc yêu cầu hủy giao dịch);
- Bản đồ bit (Bitmap). Bản đồ bit chỉ thị các thành phần dữ liệu nào được chứa trong tin nhắn.
- Các thành phần dữ liệu. Có các giá trị của các thành phần dữ liệu được đề cập tới trong bản đồ bit.

Cấu trúc này được thể hiện đồ họa trên Fig.3.

Người có hiểu biết trung bình trong lĩnh vực sẽ hiểu rằng cấu trúc được sử dụng để xác định bitmap được điều chỉnh về cơ bản là bởi ISO 8583:1987. Do đó, cấu trúc sẽ không được định nghĩa chi tiết hơn ở đây.

Mã thông báo giao dịch ban đầu sau đó được đệm khi thích hợp cho kênh vận chuyển được chọn (Bước 118). Điều này cũng có thể bao gồm việc bổ sung các thành phần dữ liệu khác nhau cho mã thông báo giao dịch. Các kết quả cuối cùng là mã thông báo giao dịch đã được thay đổi.

Khóa phiên sau đó sẽ được tính toán (Bước 120). Mã thông báo giao dịch đã được thay đổi sau đó được mã hóa sử dụng khóa phiên để tạo thành mã thông báo giao dịch đã được mã hóa (Bước 122).

Tin nhắn giao thức giao dịch tài chính sau đó được tạo thành bao gồm mã thông báo giao dịch đã được mã hóa và các yêu cầu truyền thông khác như được chỉ ra bởi kênh vận chuyển được chọn (Bước 124).

Cần chỉ ra ở đây rằng mã thông báo giao dịch ban đầu có thể bao gồm PIN của người sử dụng. Trong các tình huống này, PIN được mã hóa sử dụng khóa tách biệt cho nó để được sử dụng để mã hóa mã thông báo giao dịch.

Tin nhắn giao thức giao dịch tài chính sau đó gửi tới hệ thống xử lý đầu cuối thông qua kênh vận chuyển được chọn khi được xác định sớm hơn (Bước 126).

Theo các phương án thực hiện được ưu tiên thứ hai, trong đó, các số chỉ dẫn giống nhau đề cập tới các thành phần giống nhau, sáng chế đề xuất phương pháp thực hiện giao dịch tài chính 200.

Theo phương án thực hiện thứ hai này, đơn vị đầu cuối 14 là thiết bị truyền thông di động 202. Thiết bị truyền thông di động 202 tích hợp giao diện thẻ SIM 204 để nhận và giữ lại theo cách có thể loại bỏ được thẻ SIM 206.

Theo phương án thực hiện này, thẻ SIM 206 ở dạng của ít nhất một mạch tích hợp được tạo thành trên môi trường vật lý. Ít nhất một mạch tích hợp có các phương tiện nhớ có thể xóa được được lưu trên đó để lưu mã phần mềm có thể thực hiện được. Theo phương án thực hiện này, mã phầm mềm có thể thực hiện được được lưu trên ít nhất một mạch tích hợp được dẫn tới hai chức năng khác nhau, chức năng truyền thông và chức năng PSAM. Mã phầm mềm có thể thực hiện được được lưu trên ít nhất một mạch tích hợp vận hành để cung cấp chức năng lõi của mục đích tương ứng của nó (tức là chức năng truyền thông hoặc chức năng PSAM một cách thích hợp).

Môi trường vật lý có kích thước và hình dạng tương tự như của các thẻ SIM tiêu chuẩn (không được thể hiện) và có các tiếp xúc tương tự tại các vị trí tương tự. Các tiếp điểm ép vào và cho phép truyền thông giữa thẻ SIM 206 và giao diện thẻ SIM 204 khi thẻ SIM 206 được giữ theo cách có thể giải phóng được ở trong đó.

Theo cách này, tương tác của phần mềm được lưu trên thẻ SIM 206 được hướng tới chức năng truyền thông và phần mềm bổ sung được lưu trên thiết bị truyền thông di động 202 cho phép thiết bị truyền thông di động 202 truyền thông như là cho các thiết bị điện thoại di động thông thường (hoặc các tương đương của chúng). Điều này bao gồm việc cung cấp khả năng nhắn tin SMS. Ở đây, nó sẽ được đề cập tới như là ứng dụng SIM.

Một cách tương tự, tương tác của phần mềm được lưu trên thẻ SIM 206 được dẫn tới chức năng PSAM và phần mềm bổ sung được lưu trên thiết bị truyền thông di động 202 cho phép thiết bị truyền thông di động 202 hoạt động như là PSAM. Theo cách này,

khi chức năng PSAM được khởi tạo, giao diện của thiết bị truyền thông di động 202 hoạt động như là giao diện PSAM. Ở đây, nó sẽ được đề cập tới như là ứng dụng thanh toán.

Phương pháp theo phương án thực hiện thứ hai sẽ được mô tả dưới đây.

Người sử dụng vận hành thiết bị truyền thông di động 202 khi được yêu cầu để khởi tạo việc thực hiện của ứng dụng thanh toán (Bước 250). Khi được khởi tạo, ứng dụng thanh toán vận hành để tạo kênh truyền thông logic mới giữa phần mã được lưu trên thiết bị 202 và phần mã được lưu trên thẻ SIM 206 (Bước 252). Điều này là cần thiết để hạn chế việc gián đoạn của quy trình vận hành thông thường của ứng dụng SIM.

Kênh truyền thông logic vẫn mở cho tới khi ứng dụng thanh toán đóng nó.

Sau đó, người sử dụng duyệt giao diện người sử dụng của ứng dụng thanh toán theo cách để ra lệnh cho ứng dụng thanh toán rằng giao dịch tài chính mới được tạo (Bước 254).

Khi chỉ thị được tạo ra cho giao dịch tài chính mới được tạo ra, ứng dụng thanh toán yêu cầu người sử dụng về loại giao dịch tài chính mới (Bước 256). Người sử dung có lựa chọn để chỉ rõ một loại trong các loại giao dịch tài chính sau:

- Yêu cầu giao dịch;
- Yêu cầu lặp lại giao dịch; và
- Yêu cầu hủy giao dịch.

Khi loại của mỗi giao dịch trong các loại giao dịch tài chính này được chỉ ra bởi kênh vận chuyển được sử dụng, phương pháp theo phương án thực hiện này của sáng chế sẽ được thảo luận rõ ràng trong ngữ cảnh của yêu cầu giao dịch.

Mô tả sau chỉ ra giao dịch tài chính mới là yêu cầu giao dịch, ứng dụng thanh toán vận hành để thu thập dữ liệu liên quan tới giao dịch (Bước 258). Thông tin này tới từ bốn nguồn sau:

- Tự bản thân ứng dụng thanh toán;
- Hệ thống tệp của thẻ SIM 206;
- Thẻ tín dụng/thẻ ghi nợ của khách hàng; và/hoặc

- Trong đó, các quy tắc xử lý để chỉ định, phiên STK.

Với các mục đích của phương án thực hiện này, thông tin thẻ tín dụng/thẻ ghi nợ của người sử dụng được thu theo cách của bộ đọc thẻ được tích hợp trong, hoặc theo cách khác được gắn vào, thiết bị truyền thông di động 202.

Hơn nữa, các phương tiện để giải thích khía cạnh này của sáng chế, các quy tắc xử lý yêu cầu PIN phải được nhập theo cách của phiên STK (Bước 260).

Việc thu PIN thông qua phiên STK được quản lý bởi ứng dụng SIM như đã biết bởi người có hiểu biết trung bình trong lĩnh vực. Tuy nhiên, khi phiên STK được mở đầu, truyền thông giữa ứng dụng thanh toán và ứng dụng SIM sẽ nhận tin nhắn lỗi để chỉ thị rằng thẻ SIM là bận với phiên STK.

Sau khi PIN được truy hồi theo cách của phiên STK, PIN được định dạng như là khối ISO-0 PIN (Bước 262). Khối PIN được định dạng sau đó được mã hóa sử dụng khóa sử dụng độc quyền (Bước 264). Theo phương án thực hiện này, việc mã hóa là mã hóa DES bậc ba với chế độ CBC ngoài sử dụng ba phím khác nhau.

Khi tất cả thông tin được yêu cầu và thông tin liên quan đã được thu, thông tin được sắp xếp và được sử dụng để tạo ra mã thông báo giao dịch. Tuy nhiên, trước khi mã thông báo giao dịch có thể được tạo ra một cách thích hợp, kênh vận chuyển của giao dịch tài chính cuối cùng phải được xác định. Theo phương án thực hiện này, hai kênh vận chuyển thay thế là sẵn có:

- GPRS; hoặc
- SMS

GPRS là kênh vận chuyển được ưu tiên và, do đó kiểm tra đầu tiên được tạo ra bởi ứng dụng thanh toán để xác định xem liệu giao dịch tài chính có thể được truyền thông theo cách của GPRS (Bước 266) hay không. Nếu có, mã thông báo giao dịch ban đầu được tạo ra có cùng một cấu trúc như được mô tả trong phương án thực hiện thứ nhất của sáng chế (Bước 268).

Mã thông báo giao dịch ban đầu sau đó được đệm theo các yêu cầu ISO 7816-4/ISO 9797-1 phương pháp 2 (Bước 270). Giá trị dữ liệu ghi mã thông báo kết thúc sau đó được gắn vào thẻ bài được đệm trước khi đệm thẻ bài với số nhỏ nhất của các giá trị trống cho tới khi thẻ bài được thay đổi là nhiều lần của 8 bai (Bước 272).

Khóa phiên mã xác thực tin nhắn 128-bit sau đó được tính toán (Bước 274). Thẻ bài được thay đổi sau đó được mã hóa sử dụng khóa phiên mã xác thực tin nhắn để tạo thành mã thông báo giao dịch đã được mã hóa (bước 276). Theo phương án thực hiện này, các kỹ thuật mã hóa được sử dụng như là các thuật toán dựa trên DES.

Số chuỗi khóa sau đó cũng được tạo ra (Bước 278). Số chuỗi khóa là giá trị 80 bit.

Tin nhắn giao thức giao dịch tài chính sau đó được tạo thành với số chuỗi khóa tạo thành thành phần thứ nhất của tin nhắn giao thức, tiếp theo bởi mã thông báo giao dịch và cuối cùng khóa phiên mã xác thực tin nhắn (Bước 280).

Theo cách khác, nếu nó không thể truyền thông giao dịch tài chính theo cách của GPRS, tin nhắn giao thức giao dịch tài chính được tạo thành như sau.

Mã thông báo giao dịch ban đầu được tạo và được đệm theo cùng một cách như được mô tả cho truyền thông dựa trên GPRS (Các bước 268 và 270). Tuy nhiên, như là một phần của quy trình này bộ đếm đệm và bộ đếm tin nhắn được tạo thành (Bước 282). Bộ đếm đệm và bộ đếm tin nhắn sau đó được gắn kèm vào tin nhắn để tạo tin nhắn không được mã hóa (Bước 284). Tin nhắn không được mã hóa sau đó được mã hóa sử dụng khóa mã hóa dựa trên các đặc tả tiêu chuẩn 3GPP TS 03.48 (Bước 286).

Phần đầu SMS sau đó được thêm vào như là phần đệm cho tin nhắn được mã hóa để tạo thành tin nhắn giao thức giao dịch tài chính sẵn sàng để gửi (Bước 288).

Cần chỉ ra rằng mã thông báo giao dịch ban đầu có thể bao gồm PIN của người sử dụng. Trong các tình huống này, PIN được mã hóa sử dụng khóa tách biệt được sử dụng để mã hóa mã thông báo giao dịch.

Tin nhắn giao thức giao dịch tài chính sau đó được gửi tới hệ thống xử lý đầu cuối sử dụng kênh vận chuyển thích hợp khi được xác định sớm hơn (Bước 290). Trong

trường hợp của truyền thông theo cách của tin nhắn SMS, nó bao hàm việc chuyển tin nhắn tới ứng dụng SIM để truyền.

Khi nhận tin nhắn giao thức giao dịch tài chính theo cách của kênh vận chuyển GPRS, hệ thống xử lý đầu cuối đầu tiên sẽ xác nhận mã xác thực tin nhắn với tham chiếu tới khóa phiên mã xác thực tin nhắn (Bước 292). Nếu mã xác thực tin nhắn không thể được xác thực tin nhắn giao thức giao dịch tài chính bị bỏ qua và không có xử lý nào khác xuất hiện (Bước 294). Tuy nhiên, khi không có khả năng để xác thực tin nhắn giao thức giao dịch tài chính có thể là kết quả của các lỗi truyền hoặc dữ liệu bị hỏng, giao dịch sẽ bị dừng. Hệ thống xử lý đầu cuối chỉ đơn thuần là đợi tin nhắn quá hạn và đơn vị đầu cuối khởi tạo tin nhắn thử lại.

Khi đã được xác nhận, tin nhắn giao thức giao dịch tài chính được giải mã và chuyển tiếp tới mạng thu (Bước 296).

Trong trường hợp của tin nhắn giao thức các giao dịch tài chính được gửi theo cách của kênh vận chuyển SMS, giả định rằng SMSC mà tin nhắn được gửi tới đó giải mã tin nhắn giao thức giao dịch tài chính trước khi chuyển tiếp tới hệ thống xử lý đầu cuối (Bước 298). Hệ thống xử lý đầu cuối sau đó chuyển tiếp tin nhắn đã được mã hóa tới mạng thu (Bước 300).

Phương pháp và thiết bị được tạo ra theo phương án thực hiện sáng chế này có ưu điểm qua các phương án thực hiện khác. Cụ thể, người có hiểu biết trung bình trong lĩnh vực sẽ thấy rằng phương án thực hiện này giải quyết các vấn đề như:

- Tính dễ tổn thương của các SIM thông thường;
- Bộ nhớ hạn chế sẵn có cho SIM để sử dụng trong suốt quá trình xử lý.
- Bộ nhớ tiếp tục bị hạn chế của SIM sẵn có để sử dụng bởi các ứng dụng khác (như ứng dụng thanh toán); và
- Thông số dạng lớn được yêu cầu bởi các đơn vị hiện có tích hợp chức năng PSAM và SIM.

Người có hiểu biết trung bình trong lĩnh vực sẽ hiểu rằng sáng chế nêu trên không bị hạn chế vào các phương án thực hiện đã được mô tả. Cụ thể, các biến thể và các cải tiến sau có thể được tạo ra mà không tách khỏi phạm vi của sáng chế:

- Các dạng của cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh mà sáng chế được mô tả ở trên với nó có thể được áp dụng bao gồm: các hệ thống điện thoại có dây hiện có; internet. Do đó, cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh có thể là hệ thống liên lạc viễn thông có dây hoặc không dây.
- Cấu trúc và các mã được sử dụng trong việc tạo thành bitmap và các thành phần dữ liệu có thể thay đổi khi cần bởi hệ thống khi áp dụng. Do đó, tổ hợp bất kỳ của cấu trúc và mã có thể được sử dụng với sáng chế được mô tả ở trên.
- Dạng của việc mã hóa được sử dụng chỉ là đối tượng cho các hạn chế của môi trường vận chuyển và mức an ninh mong muốn được chấp nhận. Ví dụ, nếu ứng dụng được quan tâm yêu cầu xác thực tin nhắn thì kỹ thuật mã hóa được sử dụng cho mã xác thực tin nhắn có thể là ISO 9797-1 thuật toán 3, sử dụng thuật toán DES trong chế độ CBC.
- Ưu tiên là khối PIN được mã hóa sử dụng tiêu chuẩn mã hóa 3DES-CBC/CMAC hạ tầng liên lạc viễn thông
- Ưu tiên là việc mã hóa của mã thông báo giao dịch như là tổng thể là tiêu chuẩn mã hóa 3DES-CBC/CMAC, trong đó môi trường vận chuyển là GPRS và GSM 03.48, trong đó môi trường vận chuyển là SMS.
- Phong bì mã hóa thứ ba có thể được sử dụng để đảm bảo cho mã thông báo giao dịch đã được mã hóa.
- Các khóa công cộng hiện có có thể được sử dụng để mã hóa và xác thực thẻ bài như là tổng thể, nhưng PIN phải được mã hóa sử dụng khóa riêng sử dụng độc quyền, tách biệt.
- Giao diện người sử dụng của đơn vị đầu cuối 14 có thể là phần bất kỳ trong các phần sau: bàn phím vật lý dành riêng; bàn phín màn hình chạm; bút stylus số được kết hợp với phần mềm nhận diện ký tự hoặc nhận diện chữ viết tay.

- Trong đó, đơn vị đầu cuối 14 không được dành riêng về phía xử lý các giao dịch, ứng dụng xử lý có thể được yêu cầu để thiết lập các kênh truyền thông an ninh nằm trong đơn vị đầu cuối 14 tự bản thân nó để giải quyết các vấn đề liên quan tới tính an ninh.
- Kênh truyền thông logic an ninh bổ sung có thể được thiết lập giữa ứng dụng SIM và ứng dụng thanh toán trong đó, được coi là cần thiết.
- Các quy tắc xử lý cũng quản lý lượng nỗ lực được cho phép để nhập PIN hợp lệ.
- Số lần mà yêu cầu lặp lại giao dịch có thể được gửi liên quan tới yêu cầu giao dịch ban đầu cũng được quản lý bởi các quy tắc xử lý.
- Thông tin liên quan tới giao dịch có thể thu được tự động từ bộ đọc thẻ hoặc dạng tương tự, hoặc có thể được thu một cách gián tiếp bởi các chi tiết nhập vào của người sử dụng liên quan tới thẻ tín dụng/thẻ ghi nợ vào trong đơn vị đầu cuối 14.
- Thẻ tín dụng/thẻ ghi nợ của người sử dụng có thể là thẻ có băng từ, thẻ thông minh như thẻ RFID, bộ phận đọc dữ liệu truyền thông tầm gần hoặc dạng tương tự. Sáng chế chỉ đơn thuần là yêu cầu bộ đọc thích hợp, hoặc thiết bị đầu vào thích hợp để nhập thông tin liên quan tới thẻ tín dụng/thẻ ghi nợ, được tích hợp ở đây như là một phần của đơn vị đầu cuối 14.
- Trong khi sáng chế được mô tả trong ngữ cảnh của các giao dịch tiền tệ, sáng chế nên được coi là không bị hạn chế ở các giao dịch này. Sáng chế chỉ có thể dễ dàng được sử dụng để giải quyết các giao dịch bao gồm các cơ chế tín dụng, các cơ chế giá trị, các cơ chế điểm hoặc các cơ chế khác được sử dụng bởi các thương gia để thực hiện giao dịch (bao gồm các mẫu trung thành và mẫu thưởng).
- Các ứng dụng ghi nợ, ứng dụng tín dụng và các ứng dụng ngân hàng khác có thể vận hành được để thực hiện trên thẻ SIM 206 có thể vận hành cùng với chức năng PSAM của thẻ SIM 206 để hoàn thành các giao dịch tài chính khác nhau không được mô tả trong sáng chế này.
- Trong khi sáng chế được thiết kế khi được sử dụng rộng rãi với các thiết bị mà các chức năng của chúng tập trung quanh giao diện thẻ SIM 204 tạo sẵn, sáng chế

cũng có thể được sử dụng với thiết bị bất kỳ theo cách khác kết nối với bộ chuyển đổi tích hợp như giao diện thẻ SIM 204.

Người có hiểu biết trung bình trong lĩnh vực sẽ hiểu rằng một hoặc nhiều phương án trong các phương án hoặc các cải tiến nêu trên không bị loại trừ có thể còn được kết hợp để tạo thành các phương án thực hiện khác của sáng chế này.

Ví dụ thực hiện sáng chế

1. Phương pháp thực hiện giao dịch tài chính thông qua cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh bao gồm các bước:

thu thập dữ liệu liên quan tới loại giao dịch tài chính được chỉ rõ;

tạo mã thông báo giao dịch bao gồm dữ liệu được thu thập và/hoặc dữ liệu được lấy ra từ dữ liệu được thu thập;

mã hóa mã thông báo giao dịch;

tạo tin nhắn giao thức giao dịch tài chính tích hợp mã thông báo giao dịch được mã hóa là phụ thuộc vào kênh vận chuyển được chọn mà qua đó tin nhắn được vận chuyển; và

vận chuyển tin nhắn giao thức giao dịch tài chính sử dụng kênh vận chuyển được chọn và theo cách của cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh tới đích, trong đó tin nhắn giao thức giao dịch tài chính còn được tiếp tục xử lý.

2. Phương pháp theo ví dụ 1, trong đó bước thu thập dữ liệu liên quan tới loại giao dịch được chỉ rõ bao gồm bước phụ thu thập dữ liệu xác thực sau đó được mã hóa và mã thông báo giao dịch được tạo ra sau đó bao gồm dữ liệu xác thực được mã hóa.

3. Phương pháp theo ví dụ 2, bao gồm bước định dạng dữ liệu xác thực.

4. Phương pháp theo ví dụ 2 hoặc ví dụ 3, bao gồm bước mã hóa dữ liệu xác thực.

5. Phương pháp theo ví dụ 1, trong đó, bước thu thập dữ liệu liên quan tới loại giao dịch tài chính được chỉ rõ bao gồm thu dữ liệu bởi ít nhất một trong các cách sau: từ các tệp được lưu trên thiết bị được sử dụng để thu dữ liệu; từ bộ phận đọc dữ liệu được kết hợp với, hoặc được tích hợp vào, thiết bị được sử dụng để thu dữ liệu; từ khách hàng theo cách của giao diện người sử dụng của thiết bị được sử dụng để thu dữ liệu.

6. Phương pháp theo ví dụ 1, trong đó, bước thu thập dữ liệu liên quan tới loại giao dịch tài chính được chỉ rõ bao gồm thu bộ các quy tắc giao dịch có khả năng áp dụng cho loại giao dịch tài chính.

7. Phương pháp theo ví dụ 1, còn bao gồm bước đệm mã thông báo giao dịch khi được yêu cầu cho kênh vận chuyển được chọn.

8. Phương pháp theo ví dụ 1, còn bao gồm bước tính toán khóa phiên, khóa phiên sau đó được sử dụng để mã hóa mã thông báo giao dịch trong suốt bước mã hóa mã thông báo giao dịch.

9. Phương pháp theo ví dụ 1, trong đó, kênh vận chuyển được chọn là GPRS.

10. Phương pháp theo ví dụ 9, trong đó, bước tạo mã thông báo giao dịch bao gồm các bước phụ:

gắn kèm giá trị dữ liệu ghi mã thông báo kết thúc vào mã thông báo giao dịch; và

đệm mã thông báo giao dịch với các giá trị trống cho tới khi mã thông báo giao dịch được thay đổi là nhiều lần của 8 bai.

11. Phương pháp theo ví dụ 10, trong đó, bước mã hóa mã thông báo giao dịch còn bao gồm các bước phụ tính toán khóa phiên mã xác thực tin nhắn và mã hóa mã thông báo giao dịch được đệm và được thay đổi sử dụng khóa phiên mã xác thực tin nhắn.

12. Phương pháp theo ví dụ 11, trong đó, bước tạo tin nhắn giao thức giao dịch tài chính bao gồm bước phụ tạo số chuỗi khóa và trong đó, tin nhắn giao thức giao dịch tài chính để được tạo bao gồm số chuỗi khóa mã thông báo giao dịch và khóa phiên mã xác thực tin nhắn.

13. Phương pháp theo ví dụ 1, trong đó, kênh vận chuyển được chọn là SMS.

14. Phương pháp theo ví dụ 13, trong đó, bước tạo mã thông báo giao dịch còn bao gồm các bước phụ xác định bộ đếm đệm và bộ đếm tin nhắn và gắn kèm bộ đếm đệm và bộ đếm tin nhắn cho tin nhắn.

15. Phương pháp theo ví dụ 14, trong đó, bước mã hóa mã thông báo giao dịch bao gồm bước phụ mã hóa mã thông báo giao dịch sử dụng khóa mã hóa dựa trên các đặc tả tiêu chuẩn 3GPP TS 03.48.

16. Phương pháp theo ví dụ 14 hoặc ví dụ 15, trong đó, bước tạo tin nhắn giao thức giao dịch tài chính bao gồm bước phụ đặt tiền tố mã thông báo giao dịch đã được mã hóa với phần đầu SMS.

17. Thiết bị truyền thông để tận dụng hiệu quả hoạt động giao dịch tài chính thông qua cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh, thiết bị truyền thông có thể vận hành được để thực hiện phần mềm được lưu trên đó hoặc trên vật ghi loại bỏ được trong dữ liệu và truyền thông điều khiển với thiết bị để:

thu thập dữ liệu liên quan tới loại giao dịch tài chính được chỉ rõ;

tạo dựng mã thông báo giao dịch bao gồm dữ liệu được thu thập và/hoặc dữ liệu được lấy ra từ dữ liệu được thu thập;

mã hóa mã thông báo giao dịch;

tạo tin nhắn giao thức giao dịch tài chính tích hợp mã thông báo giao dịch đã được mã hóa là phụ thuộc vào kênh vận chuyển được chọn mà qua đó tin nhắn được vận chuyển; và

vận chuyển tin nhắn giao thức giao dịch tài chính sử dụng kênh vận chuyển được chọn và theo cách của cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh tới đích, trong đó tin nhắn giao thức giao dịch tài chính còn được tiếp tục xử lý.

18. Thiết bị truyền thông theo ví dụ 17, trong đó dữ liệu được thu thập bao gồm dữ liệu xác thực và trong đó mã thông báo giao dịch bao gồm dữ liệu xác thực ở dạng được mã hóa.

19. Thiết bị truyền thông theo ví dụ 16, còn bao gồm bộ đọc để đọc thông tin được lưu trên các thiết bị ngoại vi.

20. Thiết bị truyền thông theo ví dụ 16, thiết bị truyền thông có thể vận hành để truyền thông theo cách của một hoặc nhiều kênh vận chuyển sau: GPRS; SMS.

21. Thẻ bao gồm ít nhất một mạch tích hợp, thẻ có kích thước và hình dạng tương tự như thẻ SIM truyền thống, trong đó khi thẻ được nhận trong thiết bị có giao diện thẻ SIM, phần mềm có thể thực hiện được được lưu trên các phương tiện nhớ của ít nhất một mạch tích hợp, mà khi được thực hiện, sẽ có khả năng liên kết với phần mềm được lưu trên thiết bị để nhờ đó cho phép thiết bị tạo ra cả các chức năng SIM và PSAM cho người sử dụng thiết bị.

22. Thẻ theo ví dụ 21, trong đó, thiết bị chỉ có thể được vận hành như là SIM hoặc PSAM tại thời điểm bất kỳ và truyền thông giữa phần mềm được lưu trên các phương tiện nhớ và phần mềm được lưu trên thiết bị là theo cách của kênh truyền thông logic.

YÊU CẦU BẢO HỘ

1. Phương pháp hoạt động của thiết bị để thực hiện giao dịch tài chính thông qua cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh bao gồm các bước:

(a) thu thập dữ liệu liên quan tới loại giao dịch tài chính được chỉ rõ bởi người sử dụng, trong đó dữ liệu được thu thập này bao gồm loại giao dịch tài chính được chỉ rõ bởi người sử dụng và số nhận diện cá nhân (PIN) của người sử dụng, và trong đó loại giao dịch tài chính được chỉ rõ bởi người sử dụng này chỉ rõ một loại trong các loại yêu cầu giao dịch; yêu cầu lặp lại giao dịch; và yêu cầu hủy giao dịch;

(b) mã hóa PIN sử dụng khóa riêng sử dụng độc quyền;

(c) xác định kênh vận chuyển được chọn để truyền thông giao dịch tài chính;

(d) tạo mã thông báo giao dịch bao gồm loại giao dịch tài chính và PIN được mã hóa, trong đó mã thông báo giao dịch này được đệm khi thích hợp cho kênh vận chuyển được chọn;

(e) mã hóa mã thông báo giao dịch được đệm sử dụng khóa thứ hai được kết hợp với kênh vận chuyển được chọn, trong đó khóa thứ hai này tách biệt với khóa riêng sử dụng độc quyền;

(f) tạo tin nhắn giao thức giao dịch tài chính tích hợp mã thông báo giao dịch được mã hóa và yêu cầu truyền thông được chỉ ra bởi kênh vận chuyển được chọn, là phụ thuộc vào kênh vận chuyển được chọn mà qua đó tin nhắn được vận chuyển; và

(g) vận chuyển tin nhắn giao thức giao dịch tài chính sử dụng kênh vận chuyển được chọn và theo cách của cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh tới đích, trong đó tin nhắn giao thức giao dịch tài chính còn được tiếp tục xử lý.

2. Phương pháp theo điểm 1, bao gồm bước định dạng PIN.

3. Phương pháp theo điểm 1, trong đó bước thu thập dữ liệu liên quan tới loại giao dịch tài chính được chỉ rõ bởi người sử dụng bao gồm việc thu dữ liệu bởi ít nhất một trong các cách sau: từ các tệp được lưu trên thiết bị được sử dụng để thu dữ liệu; từ bộ phận đọc dữ liệu được kết hợp với, hoặc được tích hợp vào, thiết bị được sử dụng để thu

dữ liệu; từ khách hàng theo cách của giao diện người sử dụng của thiết bị được sử dụng để thu dữ liệu.

4. Phương pháp theo điểm 1, trong đó bước thu thập dữ liệu liên quan tới loại giao dịch tài chính được chỉ rõ bởi người sử dụng bao gồm việc thu bộ các quy tắc giao dịch có khả năng áp dụng cho loại giao dịch tài chính.

5. Phương pháp theo điểm 1, trong đó kênh vận chuyển được chọn là GPRS.

6. Phương pháp theo điểm 5, trong đó bước mã hóa mã thông báo giao dịch còn bao gồm các bước phụ tính toán khóa phiên mã xác thực tin nhắn và mã hóa mã thông báo giao dịch được đệm sử dụng khóa phiên mã xác thực tin nhắn.

7. Phương pháp theo điểm 6, trong đó bước tạo tin nhắn giao thức giao dịch tài chính bao gồm bước phụ tạo số chuỗi khóa và trong đó, tin nhắn giao thức giao dịch tài chính cũng được tạo bao gồm số chuỗi khóa mã thông báo giao dịch và khóa phiên mã xác thực tin nhắn.

8. Phương pháp theo điểm 1, trong đó kênh vận chuyển được chọn là SMS.

9. Phương pháp theo điểm 8, trong đó bước tạo mã thông báo giao dịch còn bao gồm các bước phụ xác định bộ đếm đệm và bộ đếm tin nhắn và gắn kèm bộ đếm đệm và bộ đếm tin nhắn cho tin nhắn.

10. Phương pháp theo điểm 9, trong đó bước mã hóa mã thông báo giao dịch bao gồm bước phụ mã hóa mã thông báo giao dịch sử dụng khóa mã hóa dựa trên các đặc tả tiêu chuẩn 3GPP TS 03.48.

11. Phương pháp theo điểm 8 hoặc theo điểm 9, trong đó bước tạo tin nhắn giao thức giao dịch tài chính bao gồm bước phụ đặt tiền tố mã thông báo giao dịch đã được mã hóa với phần đầu SMS.

12. Thiết bị truyền thông để tận dụng hiệu quả hoạt động giao dịch tài chính thông qua cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh, thiết bị truyền thông có thể vận hành được để thực hiện phần mềm được lưu trên đó, phần mềm, khi được thực hiện, khiến thiết bị truyền thông thực hiện các bước:

(a) thu thập dữ liệu liên quan tới loại giao dịch tài chính được chỉ rõ bởi người sử dụng, trong đó dữ liệu được thu thập này bao gồm loại giao dịch tài chính được chỉ rõ bởi người sử dụng và PIN của người sử dụng, và trong đó loại giao dịch tài chính được chỉ rõ

bởi người sử dụng này chỉ rõ một loại trong các loại yêu cầu giao dịch; yêu cầu lặp lại giao dịch; và yêu cầu hủy giao dịch;

(b) mã hóa PIN sử dụng khóa riêng sử dụng độc quyền;

(c) xác định kênh vận chuyển được chọn để truyền thông giao dịch tài chính;

(d) tạo mã thông báo giao dịch bao gồm loại giao dịch tài chính và PIN được mã hóa, trong đó mã thông báo giao dịch này được đệm thích hợp cho kênh vận chuyển được chọn;

(e) mã hóa mã thông báo giao dịch được đệm sử dụng khóa thứ hai được kết hợp với kênh vận chuyển được chọn, trong đó khóa thứ hai này tách biệt với khóa riêng sử dụng độc quyền;

(f) tạo tin nhắn giao thức giao dịch tài chính tích hợp mã thông báo giao dịch đã được mã hóa và yêu cầu truyền thông được chỉ ra bởi kênh vận chuyển được chọn là phụ thuộc vào kênh vận chuyển được chọn mà qua đó tin nhắn được vận chuyển; và

(g) vận chuyển tin nhắn giao thức giao dịch tài chính sử dụng kênh vận chuyển được chọn và theo cách của cơ sở hạ tầng liên lạc viễn thông công cộng không được đảm bảo an ninh tới đích, trong đó tin nhắn giao thức giao dịch tài chính còn được tiếp tục xử lý.

13. Thiết bị truyền thông theo điểm 12, thiết bị này còn bao gồm bộ đọc để đọc thông tin được lưu trên các thiết bị ngoại vi.

14. Thiết bị truyền thông theo điểm 12, thiết bị truyền thông này có thể vận hành để truyền thông theo cách của một hoặc nhiều các kênh vận chuyển sau: GPRS; SMS.

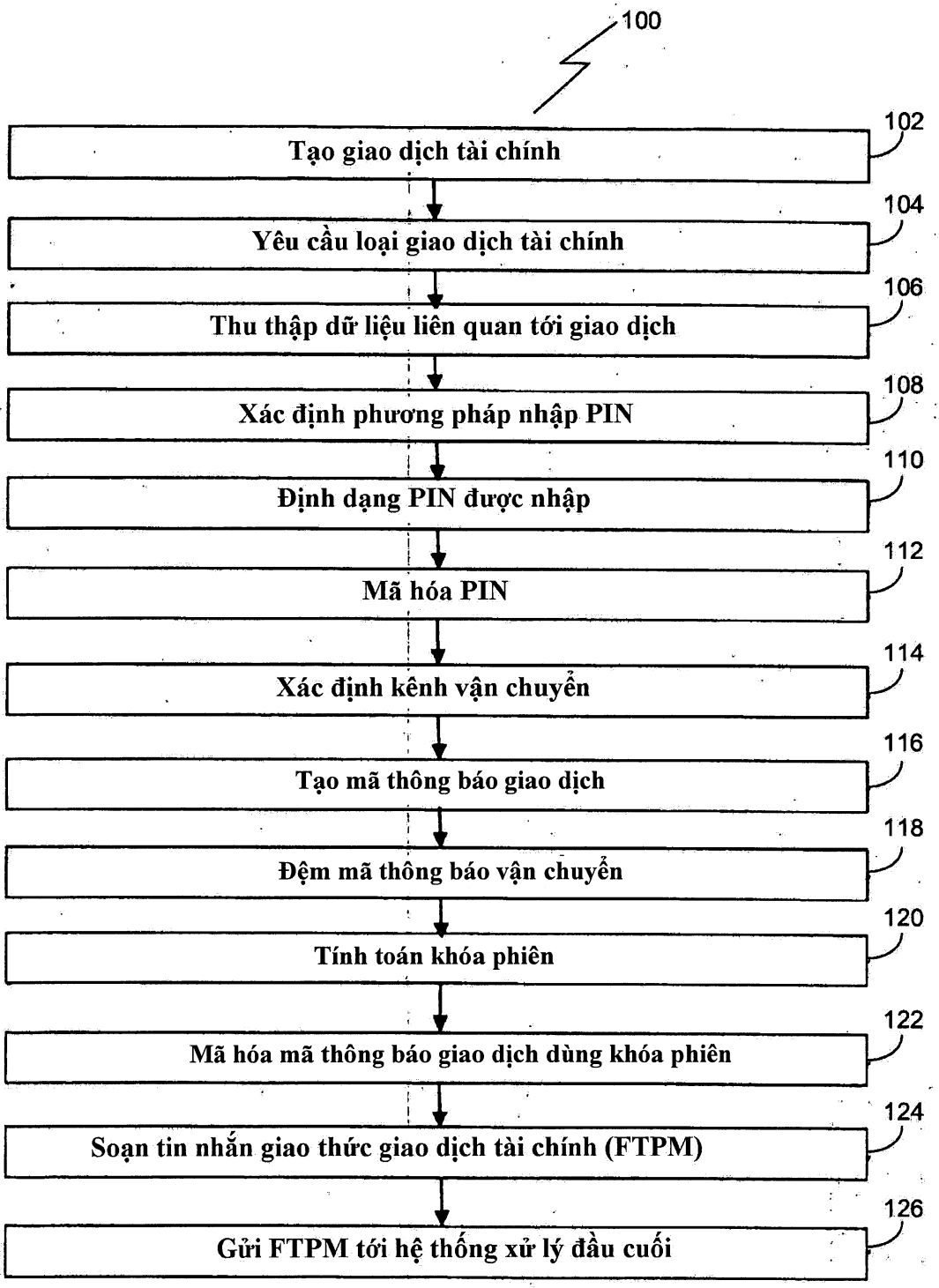

100
Tạo giao dịch tài chính
102
Yêu cầu loại giao dịch tài chính
104
Thu thập dữ liệu liên quan tới giao dịch
106
Xác định phương pháp nhập PIN
108
Định dạng PIN được nhập
110
Mã hóa PIN
112
Xác định kênh vận chuyển
114
Tạo mã thông báo giao dịch
116
Đệm mã thông báo vận chuyển
118
Tính toán khóa phiên
120
Mã hóa mã thông báo giao dịch dùng khóa phiên
122
Soạn tin nhắn giao thức giao dịch tài chính (FTPM)
124
Gửi FTPM tới hệ thống xử lý đầu cuối
126

Fig 1

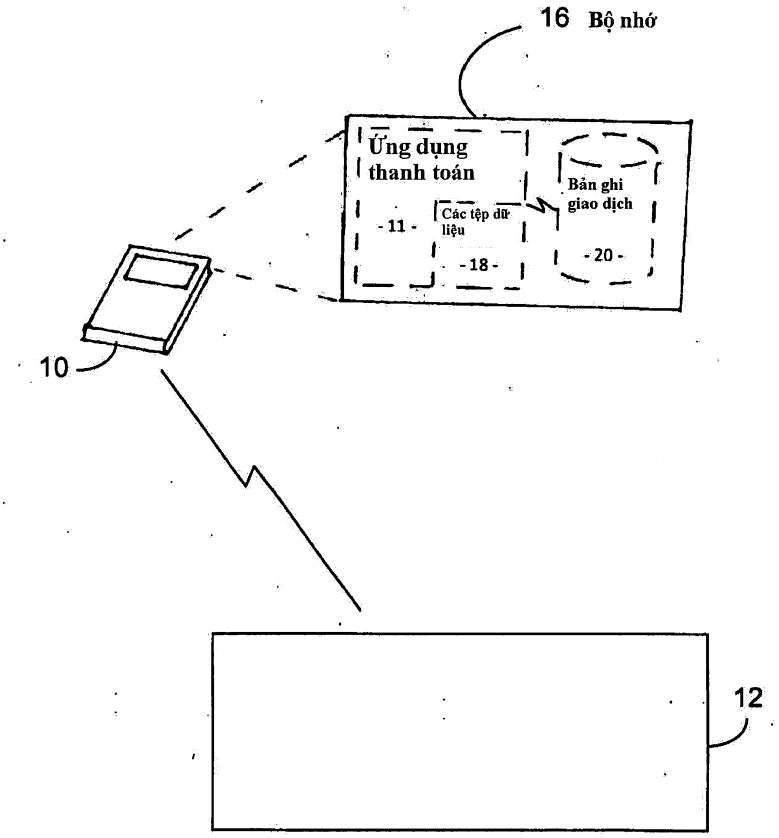

16 Bộ nhớ
Ứng dụng thanh toán
- 11 -
Các tệp dữ liệu
- 18 -
Bản ghi giao dịch
- 20 -
10
12

Fig 2

Tin nhắn **Loại** **ID**	**Bản đồ bit**	**Các thành phần dữ liệu**

Fig 3

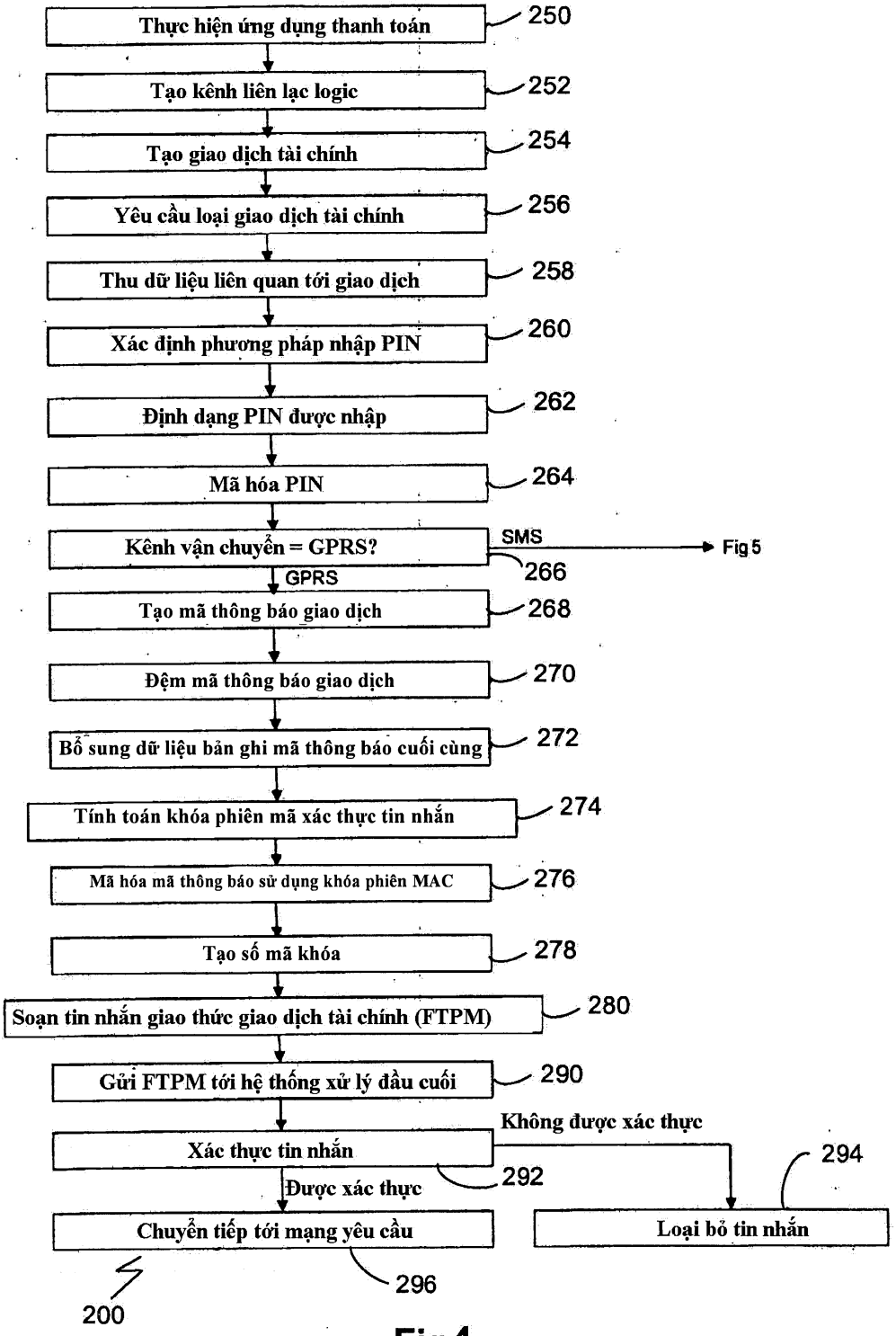

Thực hiện ứng dụng thanh toán
250
Tạo kênh liên lạc logic
252
Tạo giao dịch tài chính
254
Yêu cầu loại giao dịch tài chính
256
Thu dữ liệu liên quan tới giao dịch
258
Xác định phương pháp nhập PIN
260
Định dạng PIN được nhập
262
Mã hóa PIN
264
Kênh vận chuyển = GPRS?
SMS
Fig 5
266
GPRS
Tạo mã thông báo giao dịch
268
Đệm mã thông báo giao dịch
270
Bổ sung dữ liệu bản ghi mã thông báo cuối cùng
272
Tính toán khóa phiên mã xác thực tin nhắn
274
Mã hóa mã thông báo sử dụng khóa phiên MAC
276
Tạo số mã khóa
278
Soạn tin nhắn giao thức giao dịch tài chính (FTPM)
280
Gửi FTPM tới hệ thống xử lý đầu cuối
290
Không được xác thực
Xác thực tin nhắn
294
292
Được xác thực
Chuyển tiếp tới mạng yêu cầu
Loại bỏ tin nhắn
296
200

Fig 4

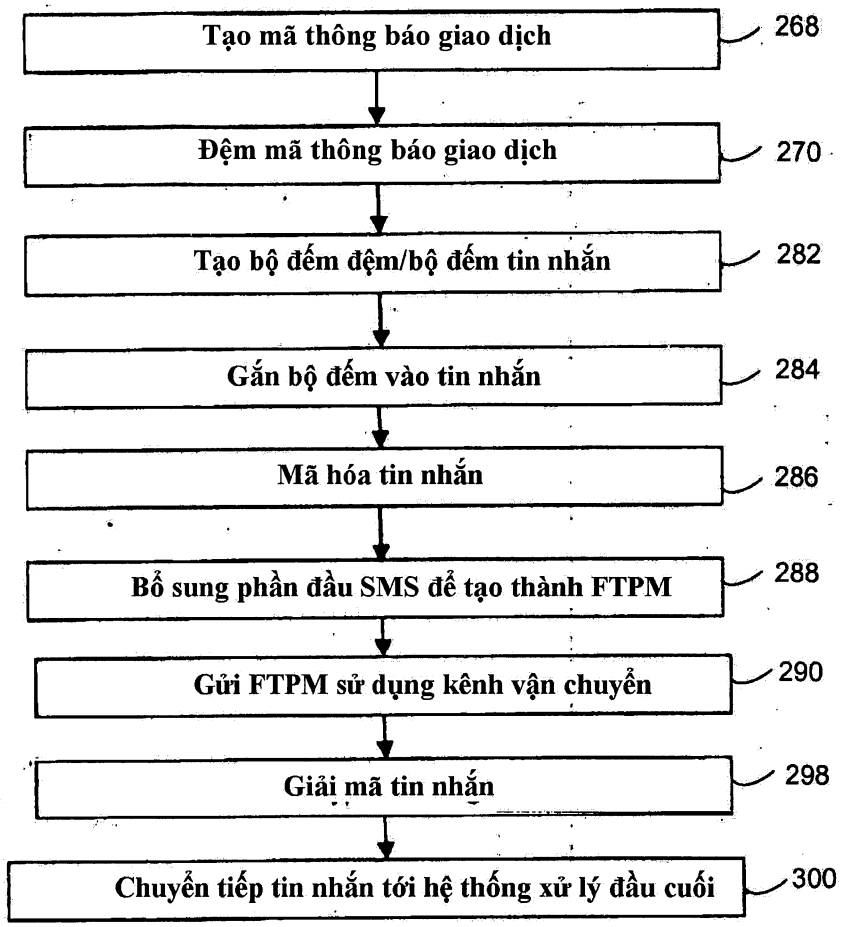

Tạo mã thông báo giao dịch
268
Đệm mã thông báo giao dịch
270
Tạo bộ đếm đệm/bộ đếm tin nhắn
282
Gắn bộ đếm vào tin nhắn
284
Mã hóa tin nhắn
286
Bổ sung phần đầu SMS để tạo thành FTPM
288
Gửi FTPM sử dụng kênh vận chuyển
290
Giải mã tin nhắn
298
Chuyển tiếp tin nhắn tới hệ thống xử lý đầu cuối
300

Fig 5

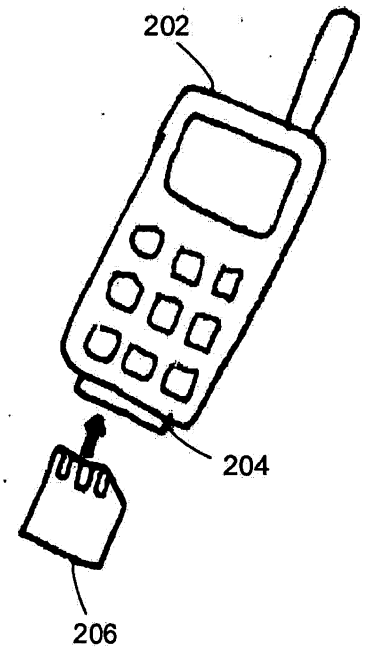


Fig 6