República Federativa do Brasil
Ministério do Desenvolvimento, Indústria e do Comércio Exterior
Instituto Nacional da Propriedade Industrial

(21) **PI 1003963-5 A2**

BRPI1003963A2

(22) Data de Depósito: 08/10/2010
(43) Data da Publicação: 13/02/2013
(RPI 2197)

(51) Int.Cl.:
H04W 12/06

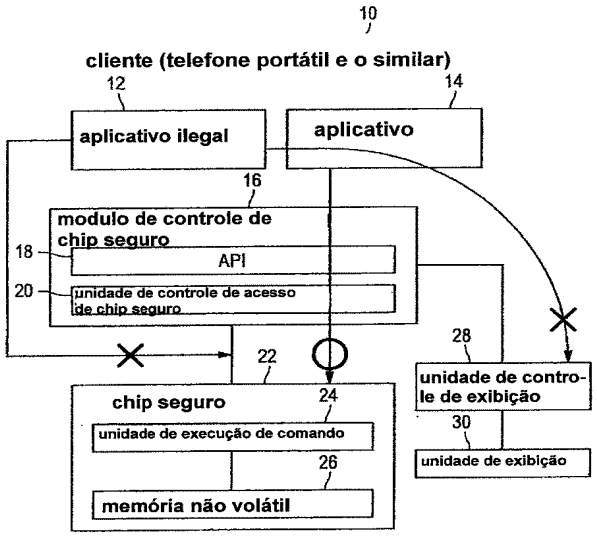
(54) Título: CHIP DE CIRCUITO INTEGRADO, APARELHO DE PROCESSAMENTO DE INFORMAÇÃO, SISTEMA DE PROCESSAMENTO DE INFORMAÇÃO, MÉTODO, E, MEIO DE ARMAZENAMENTO

(30) Prioridade Unionista: 16/10/2009 JP p2009-239257

(73) Titular(es): Felica Networks, Inc.

(72) Inventor(es): Itsuki Kamino, Naofumi Hanaki, Shinichi Kato, Shuichi Sekiya

(57) Resumo: CHIP DE CIRCUITO INTEGRADO, APARELHO DE PROCESSAMENTO DE INfORMAÇÃO, SISTEMA DE PROCESSAMENTO DE INFORMAÇÃO, MÉTODO, E, MEIO DE ARMAZENAMENTO. Um chip de IC, um aparelho de processamento de informação, sistema, método, e programa são fornecidos. Um chip de IC inclui uma unidade de controle de autenticação configurado para autenticar uma solicitação usando informação de autenticação, A solicitação e/ou a informação de autenticação é recebida a partir de fora do chip de IC.



"CHIP DE CIRCUITO INTEGRADO, APARELHO DE PROCESSAMENTO DE INFORMAÇÃO, SISTEMA DE PROCESSAMENTO DE INFORMAÇÃO, MÉTODO, E, MEIO DE ARMAZENAMENTO"

REFERÊNCIAS CRUZADAS PARA PEDIDOS RELACIONADOS

O presente pedido reivindica prioridade para Pedido de Patente de Prioridade Japonesa JP 2009 – 239257 depositado no Escritório de Patente do Japão em 16 de outubro de 2009, o conteúdo inteiro do qual estão aqui incorporados para referência.

FUNDAMENTOS

O presente pedido se relaciona a um chip de IC, um aparelho de processamento de informação, sistema, método e programa.

Nos anos recentes, aparelhos de processamento de informação tais como um telefone portátil incluindo um chip de IC tendo propriedades invioláveis (daqui em diante referido como "chip seguro") entraram em uso generalizado. Um usuário pode comunicar dados simplesmente passando tal aparelho de processamento de informação sobre um leitor / impressora, por exemplo. Conseqüentemente, o aparelho de processamento de informação é extremamente conveniente. Por exemplo, quando este aparelho de processamento de informação é aplicado a um sistema de dinheiro eletrônico, o usuário pode imediatamente fazer pagamento em uma loja e o similar simplesmente passado o aparelho de processamento de informação sobre o leitor / impressora.

Informação armazenada em uma memória não volátil de um chip seguro é protegida por meio de criptografia. Por conseguinte, é difícil violar a informação. Contudo, se qualquer aplicativo é permitido livremente usar o chip seguro no aparelho de processamento de informação, há possibilidade que o aplicativo possa usar o chip de segurança sem o usuário estar ciente disso e o aplicativo pode executar um comando para

temporariamente parar o uso do chip de segurança por conta própria, que causa questões em termos de segurança.

De modo a superar esta questão, um aparelho de processamento de informação tendo um chip seguro simples usualmente tem um mecanismo para prevenir um aplicativo de diretamente operar o chip seguro quando o aplicativo usa o chip seguro. Mais especificamente, quando o aplicativo opera o chip seguro, o mecanismo força o aplicativo operar o chip seguro por meio de um predeterminado módulo de controle do chip seguro em todos os momentos. O módulo de controle do chip seguro restringe comandos do chip seguro que podem ser executados pelo aplicativo, assim prevenindo abusos.

SUMÁRIO

Contudo, no método de prevenção de abuso descrito acima, a plataforma do aparelho de processamento de informação tem de ser implementado com o mecanismo para prevenir o aplicativo de diretamente operar o chip seguro. Por outro lado, quando o mecanismo é violado há uma possibilidade que o chip seguro seja usado ilegalmente desenvolvendo um método para trabalhar em torno do módulo de controle do chip seguro para diretamente operar o chip seguro.

À luz do descrito anteriormente, é desejável fornece um novo e melhorado chip de IC, aparelho de processamento de informação, sistema, método, e programa que pode de modo confiável prevenir um aplicativo de fazer um acesso ilegal a um chip de IC.

Em uma modalidade exemplo, um chip de circuito integrado inclui uma unidade de controle de autenticação configurada para autenticar uma solicitação usando informação de autenticação, onde pelo menos uma da solicitação e da informação de autenticação é recebida de fora do chip de circuito integrado.

Em uma modalidade exemplo, a solicitação inclui pelo menos

um de, um comando executável, uma região de acesso e um código de identificação de emissor.

Em uma modalidade exemplo, a informação de autenticação inclui um valor de erros de dados.

Em uma modalidade exemplo, um dispositivo de emissão do chip de circuito integrado gera pelo menos uma da solicitação e da informação de autenticação.

Em uma modalidade exemplo, o dispositivo de emissão emite a pelo menos uma da solicitação e da informação de autenticação para um gerador de aplicativo.

Em uma modalidade exemplo, o dispositivo de emissão registra informação relacionada a uma região de acesso da solicitação com um servidor de emissão de região de acesso.

Em uma modalidade exemplo, o dispositivo de emissão registra um valor de PIN relacionado a uma região de acesso da solicitação com um servidor de emissão de região de acesso.

Em uma modalidade exemplo, o chip de circuito integrado executa um comando com base na informação sobre comandos que um aplicativo é permitido executar; e informação sobre regiões de memória do chip de circuito integrado que o aplicativo é permitido acessar.

Em uma modalidade exemplo, um módulo de controle do chip recebe a solicitação proveniente de um aplicativo, liga o chip de circuito integrado, emite um comando de autenticação para o chip de circuito integrado, e transmite a solicitação para o chip de circuito integrado.

Em uma modalidade exemplo, a solicitação é recebida no chip de circuito integrado, e em resposta à solicitação, o circuito integrado conduz um acesso para uma localização de memória.

Em uma modalidade exemplo, a solicitação é autenticada para determinar se a solicitação é legal, a solicitação é determinada para ser legal,

a solicitação é aceita, o chip de circuito integrado notifica o módulo de controle do chip que a solicitação foi aceita, e o módulo de controle do chip notifica o aplicativo que a solicitação foi autenticada.

Em uma modalidade exemplo, o aplicativo chama uma operação do chip para usar o chip de circuito integrado, o módulo de controle do chip emite um comando executável para o chip de circuito integrado, a unidade de controle de autenticação verifica se o comando executável é permitido ser executado e se a região de acesso do comando executável é permitido ser acessado.

Em uma modalidade exemplo, o chip de circuito integrado executa o comando executável, o chip de circuito integrado notifica o módulo de controle do chip do resultado da execução do comando executável, o módulo de controle do chip notifica a amplificador operacional do resultado da execução do comando executável, o aplicativo solicita o módulo de controle do chip para terminar o uso do chip de circuito integrado, e o módulo de controle do chip desliga o chip de circuito integrado.

Em uma modalidade exemplo, a solicitação e a informação de autenticação são apagadas.

Em uma modalidade exemplo, seguindo a autenticação da solicitação, informação que é legalmente acessada pela solicitação é exibida em uma unidade de exibição.

Em uma modalidade exemplo, um aparelho de processamento de informação inclui um chip de circuito integrado incluindo uma unidade de controle de autenticação configurada para autenticar uma solicitação usando informação de autenticação, onde pelo menos uma da solicitação e da informação de autenticação é recebida de fora do chip de circuito integrado.

Em uma modalidade exemplo, o aparelho de processamento de informação é um telefone portátil.

Em uma modalidade exemplo, um sistema de processamento

de informação inclui um aparelho de processamento de informação incluindo um chip de circuito integrado incluindo uma unidade de controle de autenticação configurado para autenticar uma solicitação usando informação de autenticação, onde pelo menos uma da solicitação e da informação de autenticação é recebida de fora do chip de circuito integrado.

Em uma modalidade exemplo, um método inclui autenticar, através de um chip de circuito integrado incluindo uma unidade de controle de autenticação, uma solicitação usando informação de autenticação, onde pelo menos uma da solicitação e da informação de autenticação é recebida de fora da chip de circuito integrado.

Em uma modalidade exemplo, um meio de armazenamento armazena um programa que, quando executado, força um chip de circuito integrado incluindo uma unidade de controle de autenticação a autenticar uma solicitação usando informação de autenticação, onde pelo menos uma da solicitação e da informação de autenticação é recebida de fora do chip de circuito integrado.

De acordo com as modalidades exemplo descritas acima, o aplicativo pode ser de modo confiável prevenida de fazer acesso ilegal ao chip de IC.

Características e vantagens adicionais são aqui descritas, e serão aparentes a partir da seguinte Descrição Detalhada e das figuras.

BREVE DESCRIÇÃO DAS FIGURAS

FIG. 1 é um diagrama explicativo para ilustrar um exemplo de controle de acesso de um aplicativo para um chip seguro em um aparelho de processamento de informação relacionado

FIG. 2 é um diagrama explicativo para ilustrar um exemplo de configuração esquemática de uma sistema de processamento de informação de acordo com uma modalidade exemplo.

FIG. 3 é um diagrama explicativo para ilustrar uma

configuração esquemática de exemplo de um cliente 100 servindo como o aparelho de processamento de informação da FIG. 2.

FIG. 4 é um diagrama explicativo para ilustrar um exemplo de configuração esquemática de um tíquete de acesso do chip de exemplo

FIG. 5 é um exemplo de diagrama seqüencial de um primeiro processamento de preparação para controle de acesso do cliente 100 que é executada por um sistema de processamento de informação 1000 da FIG. 2.

FIG. 6 é um exemplo de diagrama seqüencial de um segundo processamento de preparação para controle de acesso do cliente 100 que é executada por um servidor de emissão de região de acesso de exemplo 500 e no cliente de exemplo 100 no sistema de processamento de informação 1000 da FIG. 2.

FIG. 7 é um exemplo de diagrama seqüencial ilustrando um processamento de controle de acesso executado pelo cliente 100 da FIG. 3.

FIG. 8 é um fluxograma ilustrando um exemplo de processamento de autenticação de tíquete de acesso do chip executado no passo S308 da FIG. 7.

FIG. 9 é um fluxograma ilustrando os detalhes do processamento de controle de acesso da FIG. 7.

FIG. 10 é um exemplo de diagrama seqüencial ilustrando um processamento de mudança do valor de PIN executado pelo servidor de emissão de região de acesso 500 e pelo cliente 100 no sistema de processamento de informação 1000 da FIG. 2.

FIG. 11 é um fluxograma ilustrando um exemplo de modificação do processamento de autenticação do tíquete de acesso do chip executado no passo S308 da FIG. 7.

FIG. 12 é um fluxograma ilustrando um exemplo de processamento de efetuado de acordo com códigos de erro que são executados pelo cliente 100 da FIG. 3.

DESCRIÇÃO DETALHADA

Daqui em diante, exemplos de modalidades serão descritas em detalhes com referência aos desenho anexos. Note que, nesta especificação e nos desenhos anexos, elementos estruturais que têm substancialmente a mesma função e estrutura são denotados com os mesmos numerais de referência, e explicações repetidas desses elementos estruturais são omitidos.

A explicação será feita por meio de exemplos na seguinte ordem.

1. Controle de acesso do aparelho de processamento de informação relacionado

2. Configuração do sistema de processamento de informação

3. Configuração do aparelho de processamento de informação

4. Configuração do tíquete de acesso do chip

5. Primeiro processamento de preparação para controle de acesso

6. Segundo processamento de preparação para controle de acesso

7. Processamento de controle de acesso

8. Processamento de autenticação do tíquete de acesso do chip

9. Detalhes do processamento de controle de acesso

10. Processamento de mudança do valor de PIN

11. Modificação do processamento de autenticação de tíquete de acesso do chip

12. Processamento efetuado de acordo com códigos de erros

[1. Controle de acesso do aparelho de processamento de informação relacionado]

Antes de explicar o sistema de processamento de informação e o aparelho de processamento de informação de acordo com um exemplo de modalidade, um controle de acesso de um aplicativo para um chip seguro em

um aparelho de processamento de informação relacionado será primeiro descrito. FIG. 1 é um diagrama explicativo de um exemplo de controle de acesso do aplicativo para o chip seguro no aparelho de processamento de informação relacionado.

Na FIG. 1, um cliente 10 tal como um telefone portátil servindo como aparelho de processamento de informação relacionado inclui um módulo de controle do chip seguro 16, um chip seguro 22, uma unidade de controle de exibição 28, e uma unidade de exibição 30 tal com LED. Um aplicativo ilegal 12 e um aplicativo 14 são instalados no cliente 10.

O módulo de controle do chip seguro 16 inclui uma API (Interface de Programa de Aplicativo) 18 e uma unidade de controle de acesso do chip seguro 20. O chip seguro 22 inclui uma unidade de execução de comando 24 e uma memória não volátil 26.

Por exemplo, o cliente 10 permite o aplicativo 14 usar informação armazenada em uma região da memória não volátil 26 do chip seguro 22, assim fornecendo vários serviços como serviço de dinheiro eletrônico para o usuário.

Quando, no cliente 10, o aplicativo 14 solicita ao módulo de controle do chip seguro 16, por meio da API 18, para permitir o aplicativo 14 acessar o chip seguro 22, a unidade de controle de acesso do chip seguro 20 controla o acesso feito pelo aplicativo 14 ao chip seguro 22. Já que o aplicativo 14 é um aplicativo legal, a unidade de controle de acesso do chip seguro 20 permite o aplicativo 14 acessar o chip seguro 22 conforme mostrado por um círculo na FIG. 1. A unidade de controle de acesso do chip seguro 20 também pode restringir o comando que pode ser executado pelo aplicativo 14.

Quando, no cliente 10, o aplicativo ilegal 12 solicita ao módulo de controle do chip seguro 16, por meio da API 18, para permitir o aplicativo ilegal 12 acessar o chip seguro 22, a unidade de controle de acesso

do chip seguro 20 não permite o aplicativo ilegal 12 acessar o chip seguro 22. O aplicativo legal 14 e o aplicativo ilegal 12 são distinguidos forçando a unidade de controle de acesso do chip seguro 20 para verificar a assinatura de aplicativo anexa ao aplicativo. Por conseguinte, o aplicativo ilegal 12 pode ser prevenido de acessar de forma ilegal o chip seguro 22. Quando o módulo de controle do chip seguro 16 aceita uma solicitação de acesso proveniente do aplicativo ilegal 12 ao chip seguro 22, o módulo de controle do chip seguro 16 controla a unidade de controle de exibição 28 e usa a unidade de exibição 30 para notificar ao usuário da situação de acesso.

Contudo, no exemplo de controle de acesso descrito acima, a plataforma do cliente 10 tem de ter um mecanismo para prevenir o aplicativo de diretamente operar o chip seguro 22. Quando o mecanismo é violado, os seguintes métodos podem ser desenvolvidos: como mostrado por X no lado esquerdo da FIG. 1, o módulo de controle do chip seguro 16 pode ser contornado, e o chip seguro 22 pode ser diretamente operado; e como mostrado por X no lado direito da FIG. 1, a unidade de controle de exibição 28 pode ser operada de forma ilegal, e a função da unidade de controle de exibição 28 é desativada.

Quando somente os comandos são restritos, o aplicativo pode varrer a memória não volátil 26 para coletar informação privada, e.g., que tipo de serviços são usados pelo usuário, e há uma questão em que é difícil prevenir o aplicativo de fazer tal acesso ilegal ao chip seguro 22.

De modo a resolver as questões acima, o próprio chip seguro 22 pode ter um mecanismo para restringir o uso. Contudo, as técnicas divulgadas no Pedido de Patente Japonês Aberto ao público de No. 2001-56848 e Pedido de Patente Japonês Aberto ao Público de No. 2005-56292 têm uma questão na qual é difícil aplica controle de acesso flexível a vários aplicativos executados em após a outra no cliente.

Nas técnicas divulgadas no Pedido de Patente Japonês Aberto

ao Público de No. 2005-56292, permissão de acesso pode ser estabelecida para cada comando executado no cartão de IC. Contudo, uma permissão de comando tem de ser estabelecida entrando uma senha para re-escrever a permissão de acesso de um comando a partir de fora, e conseqüentemente o lado da plataforma tem de ter a função de configuração. Com um resultado, é difícil para o próprio chip seguro estabelecer diferentes permissões de acesso para cada um dos aplicativos usados, e a permissão de aceso do comando é mantida permanentemente no chip seguro. Por esta razão, em um ambiente onde diferentes aplicativos são executados uma após outra em um terminal, há uma questão em que uma permissão de um aplicativo anteriormente executado pode permanecer sem ser eliminada, quando, e.g., o terminal é acidentalmente desligado enquanto o aplicativo ainda está sendo executado.

Na técnica divulgada no Pedido de Patente Japonês Aberto ao Público de No. 2005-56292, uma pluralidade de meios de autenticação são arrumados, e o usuário pode ser notificado que o aplicativo no terminal está tentando usar o chip seguro. Embora o usuário possa controlar se fornece permissão de acesso para cada aplicativo, o usuário somente pode estabelece se permite execução de todos os comandos existindo no chip seguro ou completamente proibir execução de todos eles, e é difícil para o usuário estabelecer diferentes permissões de acesso para cada aplicativo. Mais ainda, o usuário tem de tomar uma decisão em cada ocasião, e há uma questão em que o procedimento de uso é incômodo.

Conseqüentemente, o sistema de processamento de informação descrito mais tarde de acordo com a presente modalidade executa um primeiro processamento de preparação e um segundo processamento de preparação para o controle de acesso descrito mais tarde. Então, o aparelho de processamento de informação de acordo com a presente modalidade executa o processamento de controle de acesso descrito acima. Por conseguinte, o aparelho de processamento de informação pode de modo confiável prevenir o

aplicativo de fazer um acesso ilegal ao chip de IC.

[2. Configuração do sistema de processamento de informação]

Subseqüentemente, o sistema de processamento de informação de acordo com um exemplo de modalidade será descrito. FIG. 2 é um diagrama explicativo para ilustra uma configuração esquemática do sistema de processamento de informação de acordo com um exemplo de modalidade.

Na FIG. 2, o sistema de processamento de informação 1000 inclui o cliente 100 tal com um telefone portátil servindo c objeto em movimento um exemplo de aparelho de processamento de informação, um servidor de divulgação de aplicativo 200, um PC do gerador de aplicativo 300, um PC do emissor de chip seguro 400, e um servidor de emissão de região de acesso 500. O cliente 100, os servidores 200, 500, os PCs 300, 400 são respectivamente conectados a uma rede de comunicação 600.

O cliente 100 pode baixar aplicativos divulgados pelo servidor de divulgação de aplicativo 200. Quando o cliente 100 aceita uma solicitação de emissão de região de acesso descrita mais tarde proveniente de um aplicativo instalado, o cliente 100 solicita ao servidor de emissão de região de acesso 500 para efetuar processamento em tempo real.

O servidor de divulgação de aplicativo 200 divulga o aplicativo gerada no PC do gerador de aplicativo 300. O PC do gerador de aplicativo 300 gera o aplicativo. Quando o PC do gerador de aplicativo 300 gera um aplicativo usando um chip seguro 114 descrito mais tarde, o PC do gerador de aplicativo 300 solicita ao PC do emissor de chip seguro 400 para permitir uso do chip seguro 114. Quando o PC do emissor de chip seguro 400 emite um tíquete de acesso do chip descrito mais tarde, o PC do gerador de aplicativo 300 embute o tíquete de acesso do chip emitido no aplicativo gerado. Então o PC do gerador de aplicativo 300 transmite o aplicativo gerado para o servidor de divulgação de aplicativo 200.

Depois que o PC do emissor de chip seguro 400 aceita do PC

do gerador de aplicativo 300 a solicitação para permitir ao PC do gerador de aplicativo 300 usar o chip seguro 114, o PC do emissor de chip seguro 400 gera um tíquete de acesso do chip, e emite o tíquete de acesso do chip gerado para o PC do gerador de aplicativo 300. Depois que o PC do emissor de chip seguro 400 gera o tíquete de acesso do chip, o PC do emissor de chip seguro 400 registra informação sobre uma região de acesso do tíquete de acesso do chip gerado para o servidor de emissão de região de acesso 500, e registra informação sobre um valor de PIN, i.e., informação secreta, estabelecida para cada região de acesso do tíquete de acesso do chip gerado para o servidor de emissão de região de acesso 500.

Por exemplo, quando o servidor de emissão de região de acesso 500 aceita do cliente 100 uma solicitação de processamento em tempo real para emitir uma região de acesso, o servidor de emissão de região de acesso 500 emite uma região de acesso em uma memória não volátil 120 descrita mais tarde do chip seguro 114 do cliente 100 através do processamento em tempo real, e registra o valor de PIN para cada região de acesso emitida na memória não volátil 120.

O sistema de processamento de informação 1000 executa o primeiro processamento de preparação para o controle de acesso descrito mais tarde da FIG. 5 e o segundo processamento de preparação para controle de acesso da FIG. 6. Então, o cliente 100 pode de modo confiável prevenir o aplicativo do cliente 100 de fazer um acesso ilegal para o chip seguro executando o processamento de controle de acesso descrito mais tarde da FIG. 7.

No sistema de processamento de informação 1000 de acordo com a presente modalidade, ambos do servidor de emissão de região de acesso 500 e do chip seguro 114 têm uma chave e se comunicam cada um com o outro através de comunicação em tempo real com criptografia, assim assegurando segurança do processamento importante tal como emissão de

uma região de acesso. Deve ser notado que os programas no cliente 100 não têm a chave tal que a chave não está comprometida.

Contudo, por exemplo, mesmo quando o cliente 100 está fora da área de serviço, o aplicativo tem de ser capaz de verificar o saldo do dinheiro eletrônico, Conseqüentemente, o chip seguro 114 tem regiões não criptografadas e comando não criptografados.

Contido, se as regiões não criptografadas e comandos são livremente operados pelo aplicativo, bloqueio do usuário pode ser cancelado, e serviços podem ser explorados. De modo a evitar isto, um mecanismo para restringir o uso do chip seguro 114 tem de ser arrumado à parte da comunicação criptografada.

Este mecanismo foi realizado com um módulo de controle do chip seguro simples. Contudo, na presente modalidade, este mecanismo é realizado com um método mais confiável usando o tíquete de acesso do chip confiável.

3. [Configuração do aparelho de processamento de informação]

Subseqüentemente, o exemplo de cliente 100 servindo como o aparelho de processamento de informação da FIG. 2 será descrito. FIG. 3 é um diagrama explicativo para ilustrar um exemplo de configuração esquemática do cliente 100 servindo como o aparelho de processamento de informação da FIG. 2.

Na FIG. 3, o cliente 100 tal como um telefone portátil é um exemplo do aparelho de processamento de informação, e tem um módulo de controle do chip seguro 110, o chip seguro 114, e uma unidade de exibição 122. Em adição, os aplicativos 102, 106 estão instalados no cliente 100. Na presente modalidade, o cliente 100 tem o módulo de controle do chip seguro 110, mas quando o aplicativo instalado no100 tal como o aplicativo 106 em a função do módulo de controle do chip seguro 110, o cliente 100 pode não ter o módulo de controle do chip seguro 110.

O tíquete de acesso do chip 104 está embutido no aplicativo 102, e o tíquete de acesso do chip 108 está embutido no aplicativo 106. O

aplicativo 106 tem o módulo de controle do chip seguro 111 nele.

O módulo de controle do chip seguro 110 tem um API 112. O módulo de controle do chip seguro 110 é adaptado para receber informação transmitida a partir do chip seguro 114. Os módulos de controle do chip seguro 110 , 111 estão conectados à unidade de exibição 122. Em adição, o chip seguro 114 é conectado à unidade de exibição 122. Os módulos de controle do chip seguro 110 , 111 e o chip seguro 114 podem ser conectados a diferentes unidades de exibição.

O chip seguro 114 tem uma unidade de controle de acesso 116, uma unidade de execução de comando 118, e uma memória não volátil 120. A unidade de controle de acesso 116 é adaptada para receber o tíquete de acesso do chip proveniente do aplicativo tendo o tíquete de acesso do chip para acesso ao chip seguro 114. Por outro lado, a unidade de controle de acesso 116 é adaptada para autenticar o tíquete de acesso do chip recebido do aplicativo. Em adição, quando o tíquete de acesso do chip é lega, a unidade de controle de acesso 116 é adaptada para permitir o aplicativo executar um comando com base na informação sobre comandos que o aplicativo é permitida executar e com base na informação sobe regiões de memória do chip de IC que o aplicativo é permitida acessar. A informação sobre os comandos e a informação sobre as regiões de memória estão incluídas no tíquete de acesso do chip. Quando o tíquete de acesso do chip não é lega, a unidade de controle de acesso 116 é adaptada pra transmitir, para fora, informação sobre uma razão por que o tíquete de acesso do chip é determinado não ser legal . Adicionalmente, a unidade de controle de acesso 116 é adaptada para armazenar o conteúdo da tíquete de acesso do chip, e.g., função de memória para armazenamento temporário, e é adaptado para apagar o conteúdo armazenado do tíquete de acesso do chip. Quando o comando emitido pelo aplicativo é executável, a unidade de execução de comando 118 é adaptada para executar o comando. Deve ser notado que, o chip seguro 114

é um chip de IC tendo excelentes propriedades invioláveis.

Por exemplo, quando o módulo de controle do chip seguro 110 recebe um tíquete de acesso do chip 104 proveniente do aplicativo 102 e aceita uma solicitação para início do uso do chip seguro 114, o módulo de controle do chip seguro 110 liga o chip seguro 114. Então, o módulo de controle do chip seguro 110 emite um comando de autenticação do tíquete para a unidade de controle de acesso 116 do chip seguro 114, e transmite o tíquete de acesso do chip 104 para unidade de controle de acesso 116 do chip seguro 114. A unidade de controle de acesso 116 permite execução do comando de autenticação de tíquete, e emite o comando de autenticação de tíquete para a unidade de execução de comando 118.

A unidade de execução de comando 118 executa o comando de autenticação de tíquete emitido pela unidade de controle de acesso 116. Quando a unidade de execução de comando 118 executa o comando de autenticação de tíquete, a unidade de controle de acesso 116 autentica o tíquete de acesso do chip 104 recebido do módulo de controle do chip seguro 110.

Quando o unidade de controle de acesso 116 determina que o tíquete de acesso do chip 104 é legal, o chip seguro 114 notifica ao módulo de controle do chip seguro 110 que o chip seguro 114 aceitou o tíquete de acesso do chip 104. Então, o módulo de controle do chip seguro 110 notifica o aplicativo 102 que o tíquete de acesso do chip 104 foi autenticado.

Depois que o aplicativo 102 é notificado do término da autenticação do tíquete de acesso do chip 104, o aplicativo 102 chama a API 112 do módulo de controle do chip seguro 110, e solicita ao módulo de controle do chip seguro 110 para executar o comando.

Quando o módulo de controle do chip seguro 110 aceita a solicitação para execução do comando do aplicativo 102, o módulo de controle do chip seguro 110 emite o comando para a unidade de controle de acesso 116 do chip seguro 114.

A unidade de controle de acesso 116 verifica se o comando emitido pelo módulo de controle do chip seguro 110 é um comando permitido para ser executado após a autenticação do tíquete de acesso do chip 104, e verifica se a região de acesso do comando emitido pelo módulo de controle do chip seguro 110 é uma região permitida para ser acessado após a que do tíquete de acesso do chip 104. Depois que a unidade de controle de acesso 116 determina que o comando emitido pelo módulo de controle do chip seguro 110 seja um comando permitido para ser executado, e determina que a região de acesso do comando seja uma região permitida para ser acessada, a unidade de controle de acesso 116 permite execução do comando, e emite o comando para a unidade de execução de comando 118. A unidade de execução de comando 118 executa o comando emitido pela unidade de controle de acesso 116.

Quando a unidade de controle de acesso 116 determina que o tíquete de acesso do chip 104 é legal, o memória não volátil 120 armazena o conteúdo do tíquete de acesso do chip 104 para a região de memória. Quando o chip seguro 114 é desligado, a memória não volátil 120 apaga o conteúdo do tíquete de acesso do chip 104 armazenado na região de memória.

[4. Configuração do tíquete de acesso do chip]

Subseqüentemente, um exemplo de tíquete de acesso do chip será descrito. FIG. 4 é um diagrama explicativo para ilustrar um exemplo de configuração esquemática do exemplo de tíquete de acesso do chip. Tabela 1 é um diagrama explicativo para ilustrar a configuração do exemplo de tíquete de acesso do chip em detalhe.

Tabela 1

Número de item	Nome de item	explicação
1	Valor de erros de dados	Valor de erros de dados gerado a partir do valor de PIN e dados dos itens 2,3, 4
2	Comando executável	Lista de comando de chip seguro executada pelo aplicativo
3	Região de acesso	Região no chip seguro usada pelo aplicativo
4	Código de identificação do emissor	Informação para identificar emissor do chip seguro

Na FIG. 4 e na tabela 1, o tíquete de acesso do chip 104 inclui um valor de erros de dados 130, um comando executável 132, uma região de acesso 134, e um código de identificação do emissor 136. O valor de PIN 138 é estabelecido para cada região de acesso 134, e a informação do valor de PIN 138 pode ser gerado, por exemplo, pelo PC do emissor de chip seguro 400 , e pode ser gerado pelo PC do gerador de aplicativo 300.

O comando executável 132 é informação sobre uma lista de comandos do chip seguro 114 executado pelo aplicativo 102. A região de acesso 132 é informação sobre regiões na memória não volátil 120 do chip seguro 114 usada pelo aplicativo 102. O código de identificação do emissor 136 é informação para identificar o emissor do chip seguro 114. O valor de erros de dados 130 é um valor de erros de dados gerado com base no comando executável 132, a região de acesso 134, o código de identificação do emissor 136, e o valor de PIN 138.

[5. Primeiro processamento de preparação para controle de acesso]

O primeiro processamento de preparação para controle de cesso do cliente 100 que é executado pelo sistema de processamento de informação 1000 da FIG. 2 será daqui em diante descrito. FIG. 5 é um exemplo de diagrama seqüencial do primeiro processamento de preparação para controle de acesso do cliente 100 que é executado pelo sistema de processamento de informação 1000 da FIG. 2.

Na FIG. 5, primeiro, o PC do gerador de aplicativo 300 emite uma solicitação para usar a chip seguro 114 para o PC do emissor de chip seguro 400 tal que o aplicativo 102 gerado pode usar o chip seguro 114 do cliente 100 (passo S102). Por exemplo, o PC do gerador de aplicativo 300 reporta para o PC do emissor de chip seguro 400 uma lista desejada de comando do chip seguro 114 que o aplicativo 102 gerado executa e uma lista desejada de regiões na memória não volátil 120 do chip seguro 114 que o aplicativo 102 gerado usa, i.e., acessos.

Subseqüentemente, o PC do emissor de chip seguro 400 tendo recebido a solicitação para uso do chip seguro 114 gera um tíquete de acesso do chip como mostrando na FIG. 4 e na tabela 1 com base no conteúdo da solicitação de uso (passo S104). Então, o PC do emissor de chip seguro 400 emite o tíquete de acesso do chip gerado para o PC do gerador de aplicativo 300 (passo S106).

Subseqüentemente, o PC do gerador de aplicativo 300 embute o tíquete de acesso do chip emitido no passo S106 no aplicativo 102 gerado (passo S108).

Subseqüentemente, o PC do gerador de aplicativo 300 transmite o aplicativo 102 tendo o tíquete de acesso do chip embutido nele para o servidor de divulgação de aplicativo 200 (passo S110). Então, o servidor de divulgação de aplicativo 200 divulga o aplicativo 102 tendo o tíquete de acesso do chip embutido nele (passo S112). Como um resultado, o cliente 100 pode baixar o aplicativo 102 a partir do servidor de divulgação de aplicativo 200.

Depois que o PC do emissor de chip seguro 400 efetua o processamento do passo S104, o servidor de emissão de região de acesso 500 registra informação sobre a região de acesso do tíquete de acesso do chip gerado para o servidor de emissão de região de acesso 500 (passo S114), e registra informação sobre o valor de PIN configurado para o servidor de emissão de região de acesso 500 para cada região de acesso do tíquete de acesso do chip gerado (passo S116).

[6. Segundo processamento de preparação para controle de acesso]

O segundo processamento de preparação para controle de acesso do cliente 100 que é executado pelo servidor de emissão de região de acesso 500 e pelo cliente 100 no sistema de processamento de informação 1000 da FIG. 2 será daqui em diante descrito. FIG. 6 é um exemplo de diagrama seqüencial do segundo processamento de preparação para controle

de acesso do cliente 100 que é executa pelo servidor de emissão de região de acesso 500 e pelo cliente 100 no sistema de processamento de informação 1000 da FIG. 2. Depois que o primeiro processamento de preparação para controle de aceso do cliente 100 mostrado na FIG. 5 é executado, o cliente 100 baixa o aplicativo 102, e o aplicativo 102 é instalado e executado no cliente 100. Assim sendo, este processamento é executado.

Na FIG. 6, quando o aplicativo 102 iniciar no cliente 100, o aplicativo 102 solicita ao módulo de controle do chip seguro 110 para emitir um região de acesso na memória não volátil 120 do chip seguro 114 (passo S202).

Subseqüentemente, o módulo de controle do chip seguro 110 liga o chip seguro 114 (passo S204), e solicita ao servidor de emissão de região de acesso 500 para efetuar processamento em tempo real de modo a emitir uma região de acesso no memória não volátil 120 do chip seguro 114 e registra um valor de PIN para cada região de acesso (passo S206).

Subseqüentemente, o servidor de emissão de região de acesso 500 tendo aceito a solicitação de processamento em tempo real emite a região de acesso usada pelo aplicativo 102 na memória não volátil 120 do chip seguro 114 por meio do módulo de controle do chip seguro 110 através do processamento em tempo real (passo S208). Adicionalmente, o servidor de emissão de região de acesso 500 registra um valor de PIN para cada região de acesso emitida na memória não volátil 120 do chip seguro 114 por meio do módulo de controle do chip seguro 110 através do processamento em tempo real (passo S210).

Subseqüentemente, o módulo de controle do chip seguro 110 notifica o resultado do processamento em tempo real para o aplicativo 102 (passo S212).

[7. Processamento de controle de acesso]

O exemplo de processamento de controle de acesso executado

pelo cliente 100 mostrado na FIG. 3 será daqui em diante descrito. FIG. 7 é um exemplo de diagrama seqüencial ilustrando o processamento de controle de acesso executado pelo cliente 100 da FIG. 3. Este processamento é executado após o segundo processamento de preparação para controle de acesso do cliente 100 da FIG. 6.

Na FIG. 7, primeiramente, o aplicativo 102 transmite o tíquete de acesso do chip 104 para o módulo de controle do chip seguro 110, e solicita início do uso do chip seguro 114 (passo S302).

Subseqüentemente, o módulo de controle do chip seguro 110 liga o chip seguro 114 (passo S304), emite um comando de autenticação de tíquete para o chip seguro 114, e transmite o tíquete de acesso do chip 104 (passo S306).

Subseqüentemente, o chip seguro 114 executa um processamento de autenticação de tíquete de acesso do chip descrito mais tarde mostrado na FIG. 8, e efetua autenticação para determinar se o tíquete de acesso do chip 104 recebido é legal ou não (passo S308).

Subseqüentemente, quando o 194 é determinado se refere lega no passo S308, o chip seguro 114 armazena o conteúdo do tíquete de acesso do chip 104, e notifica o módulo de controle do chip seguro 110 que o tíquete de acesso do chip 104 foi aceito (passo S310). Então, o módulo de controle do chip seguro 110 notifica o aplicativo 102 que o tíquete de acesso do chip 104 foi autenticado (passo S312).

Subseqüentemente, o aplicativo 102 chama uma API de operação de chip para usar o chip seguro 114 (passo S314). Então, quando o aplicativo 102 solicita o módulo de controle do chip seguro 110 para executar o comando do chip seguro 114, o módulo de controle do chip seguro 110 emite um comando para o chip seguro 114 (passo S316).

Subseqüentemente, o chip seguro 114 força a unidade de controle de acesso 116 a verificar se o comando emitido pelo módulo de

controle do chip seguro 110 é um comando permitido para ser executado após a autenticação do tíquete de acesso do chip 104 no passo S308, e também verifica se a região de acesso do comando emitido pelo módulo de controle do chip seguro 110 é uma região permitida pra ser acessada após a autenticação do tíquete de acesso do chip 104 no passo S308 (passo S318).

Subseqüentemente, no passo S318, o chip seguro 114 determina que o comando seja permitido para ser executado, e que a região de acesso do comando é permitida para ser acessada. Por conseguinte, a unidade de execução de comando 118 executa o comando (passo S320).

Subseqüentemente, o chip seguro 114 notifica ao módulo de controle do chip seguro 110 do resultado da execução do comando (passo S322). Então, o módulo de controle do chip seguro 110 notifica ao aplicativo 102 do resultado da execução do comando notificado no passo S322 (passo S324).

Subseqüentemente, o aplicativo 102 solicita ao módulo de controle do chip seguro 110 para terminar o uso do chip seguro 114 (passo S326).

Subseqüentemente, o módulo de controle do chip seguro 110 desliga o chip seguro 114 (passo S328). Quando o chip seguro 114 é desligado, o conteúdo do tíquete de acesso do chip 104 armazenado no passo S310 são apagados. Alternativamente, o módulo de controle do chip seguro 110 pode separadamente emitir um comando para apagar o conteúdo do tíquete de acesso do chip 104 armazenado no passo S310 para o chip seguro 114.

[8. Processamento de autenticação do tíquete de acesso do chip]

FIG. 8 é um fluxograma ilustrando o processamento de autenticação do tíquete de acesso do chip executado no passo S308 da FIG. 7.

Na FIG. 8, primeiramente, a unidade de controle de acesso 116 do chip seguro 114 determina se o formato do tíquete de acesso do chip 104

recebido proveniente do módulo de controle do chip seguro 110 está correto ou não (passo S402). Por exemplo, a unidade de controle de acesso 116 do chip seguro 114 determina se o formato do tíquete de acesso do chip 104 é um formato como mostrado na FIG. 4 que é definido na geração do 194 gerado pelo PC do emissor de chip seguro 400 no passo S104 da FIG. 5.

Quando o formato do tíquete de acesso do chip 104 é determinado estar correto como um resultado da determinação feita no passo S403 (SIM no passo S402), a unidade de controle de acesso 116 do chip seguro 114 verifica o valor de erros de dados 130 do tíquete de acesso do chip 104 (passo S404). Por exemplo, a unidade de controle de acesso 116 do chip seguro 114 efetua a verificação comparando o valor de erros de dados 130 do tíquete de acesso do chip 104 com um valor de erros de dados gerado com base no comando executável 132, na região de acesso região de acesso 134, e no código de identificação do emissor 136 no tíquete de acesso do chip 104 recebido e com base no valor de PIN registrado na região de acesso correspondendo à região de acesso 134 na memória não volátil memória não volátil 120. Alternativamente, a unidade de controle de acesso 116 do chip seguro 114 pode efetuar a verificação comparando o valor de erros de dados 130 do tíquete de acesso do chip 104 com um valor de erros de dados gerado com base no comando executável 132 e na região de acesso 134 no tíquete de acesso do chip 104 recebido, com base no código de identificação do emissor no chip seguro 114, e com base no valor de PIN registrado na região de acesso correspondendo à região de acesso 134 na memória não volátil 120.

Subseqüentemente, a unidade de controle de acesso 116 do chip seguro 114 determina se o valor de erros de dados 130 do tíquete de acesso do chip 104 está correto ou não com base no resultado da verificação no passo S404 (passo S406).

Quando o valor de erros de dados 130 do tíquete de acesso do chip 104 é determinado ser correto como um resultado da determinação no

passo S406 (SIM no passo S406), a unidade de controle de acesso 116 do chip seguro 114 determina se o código de identificação do emissor 136 do tíquete de acesso do chip 104 coincide com o código de identificação do emissor do chip seguro 114 (passo S408).

Quando o código de identificação do emissor 136 do tíquete de acesso do chip 104 é determinado coincidir com o código de identificação do emissor do chip seguro 114 conforme um resultado da determinação no passo S408 (SIM no passo S408), a unidade de controle de acesso 116 do chip seguro 114 autentica o tíquete de acesso do chip 104 como um tíquete de acesso do chip legal (passo S410). Assim sendo, o comando do comando executável 132 do tíquete de acesso do chip 104 é permitido ser executado pelo aplicativo 102, e o uso da região de acesso correspondendo à região de acesso 134 é permitida.

A unidade de controle de acesso 116 do chip seguro 114 determina que o tíquete de acesso do chip 104 é um tíquete de acesso do chip ilegal (passo S412) nos seguintes casos: o formato do tíquete de acesso do chip 104 é determinado ser incorreto como um resultado da determinação no passo S403 (NÃO no passo S402); O valor de erros de dados 130 DO tíquete de acesso do chip 104 é determinado ser incorreto como um resultado da determinação no passo S406 (NÃO no passo S406); ou o código de identificação do emissor 136 do tíquete de acesso do chip 104 é determinado não coincidir com o código de identificação do emissor do chip seguro 114 conforme um resultado da determinação no passo S408 (NÃO no passo S408).

De acordo com o processamento de controle de acesso da FIG. 7, o tíquete de acesso do chip transmitido a partir do aplicativo é autenticado,e quando tíquete de acesso do chip é determinado ser legal, a execução do comando fornecido pelo aplicativo é permitido com base na informação sobre comandos que o aplicativo é permitido executar e com base na informação

sobre regiões de memória do chip seguro que o aplicativo é permitida acessar. A informação sobre os comandos e a informação sobre as regiões de memória estão incluídas no tíquete de acesso do chip. Por conseguinte, o aplicativo pode de forma confiável ser prevenido de fazer um acesso ilegal para o chip seguro 114.

Em um caso onde o emissor de chip seguro estabelece uma região de acesso especial na região de acesso 134 para um aplicativo que gerencia o região de acesso 134, o chip seguro 114 pode permitir o uso de todas as regiões de acesso de uma vez, e pode ser adaptada para fornecer permissão somente para comandos.

Em um caso onde o emissor de chip seguro estabelece uma região de acesso especial na região de acesso 134 que é estabelecida para um aplicativo que usa somente a função do chip seguro 114 que não retransmite a região de acesso (por exemplo, função de comunicação via rádio com um terminal de informação externo incluído no chip seguro 114), o chip seguro 114 pode proibir o uso de todas as regiões de acesso, e pode ser adaptado para fornecer permissão somente para comandos.

Quando a região de acesso 134 não está especificada no tíquete de acesso do chip, o chip seguro 114 pode determinar que o emissor de chip seguro faça a configuração para o aplicativo que gerencia a região de acesso 134 ou determina que o emissor de chip seguro faça a configuração para o aplicativo que usa a função do chip seguro 114 que não responde na região de acesso, e o chip seguro 114 pode ser adaptado para automaticamente efetuar autenticação com o valor de PIN da região de acesso especial

[9. Detalhes do processamento de controle de acesso]

Subseqüentemente, os detalhes do processamento de controle da FIG. 7 será descrito. FIG. 9 é um fluxograma ilustrando os detalhes do processamento de controle de acesso da FIG. 7.

Na FIG. 9, primeiramente, o chip seguro 114 é desligado pelo módulo de controle do chip seguro 110 (passo S502). O chip seguro 114 aceita o comando de autenticação de tíquete emitido pelo módulo de controle do chip seguro 110, e recebe o 194 (passo S504).

Subseqüentemente, a unidade de controle de acesso 116 do chip seguro 114 determina se o tíquete de acesso do chip 104 recebido é um tíquete de acesso do chip lega (passo S506).

Quando o tíquete de acesso do chip 104 recebido é determinado ser um tíquete de acesso do chip legal conforme um resultado da determinação no passo S506 (SIM no passo S506), a unidade de controle de acesso 116 do chip seguro 114 estabelece o estado do chip seguro 114 a fim de possibilitar o comando do comando executável 132 do tíquete de acesso do chip 104 e para possibilitar o uso da região de acesso correspondendo à região de acesso 134 (passo S508), e notifica o módulo de controle do chip seguro 110 que o tíquete de acesso do chip 104 foi aceito (passo S510).

Subseqüentemente, o chip seguro 114 aceita o comando fornecido pelo módulo de controle do chip seguro 110 que aceitou a solicitação para execução do comando do chip seguro 114 a partir do aplicativo 102 (passo S512).

Subseqüentemente, a unidade de controle de acesso 116 do chip seguro 114 determina se o comando emitido pelo módulo de controle do chip seguro 110 é um comando permitido a ser executado quando da autenticação do tíquete de acesso do chip 104 e determina que a região de acesso do comando emitido pelo módulo de controle do chip seguro 110 é uma região permitida para ser acessada quando da autenticação do tíquete de acesso do chip 104 (passo S514).

Quando o comando emitido pelo módulo de controle do chip seguro 110 é determinado ser um comando permitido ser executado e a região de acesso do comando é determinada ser uma região permitida ser acessada

como um resultado da detector no passo S514 (SIM no passo S514), a unidade de controle de acesso 116 do chip seguro 114 permite a execução do comando, e usa a unidade de exibição 122 para exibir uso normal do chip seguro 114 para o usuário. Por exemplo, a unidade de controle de acesso 116 do chip seguro 114 pode exibir normal uso iluminando um LED da unidade de exibição 122, e pode mudar a core e o tipo de LED iluminado de acordo com o comando.

Subseqüentemente, a unidade de execução de comando 118 do chip seguro 114 executa o comando de qual execução é permitida pela 115 do chip seguro 114 (passo S518). Então, o chip seguro 114 replica o resultado da execução do comando para o módulo de controle do chip seguro 110 (passo S520).

Quando o tíquete de acesso do chip 104 recebido não é determinado ser um tíquete de acesso do chip legal conforme um resultado da determinação no passo S506 (NÃO no passo S506), o chip seguro 114 replica informação indicando a falha da autenticação do tíquete de acesso do chip 104 para o módulo de controle do chip seguro 110 (passo S522).

Quando, conforme um resultado da determinação no passo S514, o comando emitido pelo módulo de controle do chip seguro 110 é determinado não ser um comando permitido para ser executado, ou a região de acesso do comando é determinada não ser uma região permitida para ser acessada (NÃO no passo S514), a unidade de controle de acesso 116 do chip seguro 114 proíbe a execução do comando, e usa a unidade de exibição 122 para exibir uso ilegal do chip seguro 114 para o usuário (passo S524). Por exemplo, a unidade de controle de acesso 116 do chip seguro 114 pode exibir uso ilegal iluminando um LED da unidade de exibição 122, e pode mudar a cor e o tipo do LED iluminado de acordo com o comando.

[10. Processamento de mudança do valor de PIN]

Um processamento de mudança do valor de PIN executado

pelo servidor de emissão de região de acesso 500 e pelo cliente 100 no sistema de processamento de informação 1000 da FIG. 2 será daqui em diante descrito. FIG. 10 é um diagrama seqüencial ilustrando o processamento de mudança do valor de PIN executado pelo servidor de emissão de região de acesso 500 e pelo cliente 100 no sistema de processamento de informação 1000 da FIG. 2. Este processamento é executado de modo a prevenir acesso ilegal ao chip seguro 114 fazendo uso do valor de PIN 138 comprometido ou roubado quando o valor de PIN 138 está comprometido ou roubado. Este processamento é executado após os seguintes passos serem efetuados: o cliente 100 baixa um aplicativo 150 atualizado; e posteriormente o aplicativo 102 atualizado é instalada no cliente 100

Na FIG. 10, primeiramente quando o aplicativo 150 atualizado é ativada no cliente 100, o aplicativo 150 atualizado solicita ao módulo de controle do chip seguro 110 para mudar o valor de PIN registrado para cada região de acesso na memória não volátil 120 do chip seguro 114 (passo S602).

Subseqüentemente, o módulo de controle do chip seguro 110 liga o chip seguro 114 (passo S604), e solicita o servidor de emissão de região de acesso 500 para efetuar processamento em tempo real para atualizar o valor de PIN registrado para cada região de acesso no memória não volátil 120 do chip seguro 114 (passo S606).

Subseqüentemente, o servidor de emissão de região de acesso 500 tendo aceito a solicitação de processamento em tempo real confirma se a região de acesso usada pelo aplicativo 102 já foi emitida na memória não volátil 120 do chip seguro 114 através do processamento em tempo real por meio do módulo de controle do chip seguro 110 (passo S608). Adicionalmente, o servidor de emissão de região de acesso 500 atualiza o valor de PIN registrado para cada região de acesso na memória não volátil 120 do chip seguro 114 através do processamento em tempo real proporção meio do módulo de controle do chip seguro 110 (passo S610).

Subseqüentemente, o módulo de controle do chip seguro 110 notifica o aplicativo 102 do resultado do processamento em tempo real (passo S612).

De acordo com o processamento de mudança do valor de PIN da FIG. 10, quando o valor de PIN 138 está comprometido ou roubado, o valor de PIN 138 pode ser mudado. Por conseguinte, o processamento de mudança do valor de PIN previne acesso ilegal ao chip seguro 114 que é feito fazendo uso do valor de PIN 138.

[11. Modificação do processamento de autenticação de tíquete de acesso do chip]

Uma modificação do processamento de autenticação de tíquete de acesso do chip executado no passo S308 da FIG. 7 será daqui em diante descrito, FIG. 11 é um fluxograma ilustrando um exemplo de modificação do processamento de autenticação de tíquete de acesso do chip executado no passo S308 da FIG. 7.

Na FIG. 11, o chip seguro 114 determina se o formato do tíquete de acesso do chip 104 recebido proveniente do 11 está correto ou não (passo S702).

Quando o formato da tíquete de acesso do chip 104 é determinado estar correto conforme um resultado da determinação no passo S702 (SIM no passo S702), o chip seguro 114 determina se o código de identificação do emissor 136 do tíquete de acesso do chip 104 coincide com o código de identificação do emissor do chip seguro 114 (passo S704).

Quando o código de identificação do emissor 136 do tíquete de acesso do chip 104 é determinado coincidir com o código de identificação do emissor do chip seguro 114 conforme um resultado da determinação no passo S704 (SIM no passo S704), o chip seguro 114 determina se a região de acesso região de acesso 134 do tíquete de acesso do chip 104 existe ou não na memória não volátil 120 (passo S706).

Quando a região de acesso 134 do tíquete de acesso do chip 104 é determinado existe na memória não volátil 120 conforme um resultado da determinação no passo S706 (SIM no passo S706), o chip seguro 114 verifica o valor de erros de dados 130 do tíquete de acesso do chip 104 (passo S708).

Subseqüentemente, o chip seguro 114 determina se o valor de erros de dados 130 do tíquete de acesso do chip 104 está correto ou não conforme um resultado da verificação no (passo S710).

Quando o valor de erros de dados 130 do tíquete de acesso do chip 104 é determinado estar correto conforme um resultado da determinação no passo S710 (SIM no passo S710), o chip seguro 114 autentica o tíquete de acesso do chip 104 como um tíquete de acesso do chip legal, e replica informação indicando "autenticado com sucesso" para o módulo de controle do chip seguro 110 (passo S712).

Quando o formato do tíquete de acesso do chip 104 não é determinado estar correto conforme um resultado da determinação no passo S702 (NÃO no passo S702), o chip seguro 114 replica um código de erro indicando "tíquete ilegal" para o módulo de controle do chip seguro 110 (passo S714).

Quando o código de identificação do emissor 136 do tíquete de acesso do chip 104 é determinado não coincidir com o código de identificação do emissor do chip seguro 114 conforme um resultado da determinação no passo S704 (NÃO no passo S704), o tíquete de acesso do chip 104 replica um código de erro indicando "emissor errado" e o código de identificação do emissor da chip seguro 114 para o módulo de controle do chip seguro 110 (passo S716). Alternativamente, no passo S714, somente o código de erro indicando "emissor errado" pode ser transmitido para o módulo de controle do chip seguro 110.

Quando a região de acesso 134 do tíquete de acesso do chip

104 é determinado existe na memória não volátil 120 conforme um resultado da determinação no passo S706 (NÃO no passo S706), o chip seguro 114 replica um código de erro indicando "nenhuma região" para o módulo de controle do chip seguro 110 (passo S718).

Quando o valor de erros de dados 130 da tíquete de acesso do chip 104 não é determinado estar correto conforme um resultado da determinação no passo S710 (NÃO no passo S710), o chip seguro 114 replica um código de erro indicando "truncamento computacional errado" para o módulo de controle do chip seguro 110 (passo S720).

De acordo com para processamento de autenticação de tíquete de acesso do chip da FIG. 11, quando a autenticação do tíquete de acesso do chip 104 no chip seguro 114 falha, o chip seguro 114 replica um código de erro para o módulo de controle do chip seguro 110. Então, o módulo de controle do chip seguro 110 executa processamento de acordo com o código de erro recebido como a seguir.

[12. Processamento efetuado de acordo com códigos de erros]

O processamento executado pelo cliente 100 da FIG. 3 de acordo com o código de erro vai ser daqui em diante descrito. FIG. 12 é um fluxograma ilustrando exemplo de processamento efetuado de acordo com o código de erro que é executado pelo cliente 100 da FIG. 3. Este processamento é executado depois que o chip seguro 114 replica um código de erro para o módulo de controle do chip seguro 110 no processamento de autenticação de tíquete de acesso do chip da FIG. 11.

Na FIG. 12, primeiramente, o módulo de controle do chip seguro 110 do cliente 100 determina se o código de erro recebido processo do chip seguro 114 é ou não um código de erro indicando "tíquete ilegal" (passo S802).

Quando o código de erro é determinado ser um código de erro indicando "tíquete ilegal" conforme um resultado da determinação no passo

S802 (SIM no passo S802), o módulo de controle do chip seguro 110 usa a unidade de exibição 122 para avisar o usuário que o aplicativo ilegal está sendo executado para operar o chip seguro 114 (passo S804). No passo S804, a operação do aplicativo ilegal que enviou o tíquete de acesso do chip 104 pode ser forçosamente parada, e o aplicativo ilegal pode ser forçosamente eliminado.

Quando o código de erro não é determinado ser um código de erro indicando "tíquete ilegal" conforme um resultado da determinação no passo S802 (NÃO no passo S802), o módulo de controle do chip seguro 110 determina se o código de erro é ou não um código de erro indicando "emissor errado" (passo S806).

Quando o código de erro é determinado ser um código de erro indicando "emissor errado" conforme um resultado da determinação no passo S806 (SIM no passo S806), o módulo de controle do chip seguro 110 usa a unidade de exibição 122 para notificar ao usuário que o emissor do aplicativo é diferente do emissor do chip seguro 114 para ser operado (passo S808). No passo S808, quando o módulo de controle do chip seguro 110 recebe o código de erro indicando "emissor errado" assim como o código de identificação do emissor do chip seguro 114, o módulo de controle do chip seguro 110 pode pesquisar, com base no código de identificação do emissor, uma fonte a partir da qual o aplicativo fornecendo o mesmo serviço para o emissor corrente do chip seguro 114 pode ser baixada, e pode forçar um navegador a exibir a fonte para solicitar ao usuário para substituir ou atualizar o aplicativo, ou pode automaticamente baixar o aplicativo para substituir ou atualizar o aplicativo.

Quando o código de erro não é determinado ser um código de erro indicando "emissor errado" conforme um resultado da determinação no passo S806 (NÃO no passo S806), o módulo de controle do chip seguro 110 determina se o código de erro é ou não um código de erro indicando "nenhuma região" (passo S810).

Quando o código de erro é determinado ser um código de erro indicando "nenhuma região" conforme um resultado da determinação no passo S810 (SIM no passo S810), o módulo de controle do chip seguro 110 usa a unidade de exibição 122 para notifica ao usuário que a região não foi ainda emitido na chip seguro 114 (passo S812). No passo S812, o módulo de controle do chip seguro 110 pode trocar informação com o aplicativo 102, e pode emitir a região solicitando ao servidor de emissão de região de acesso 500 para efetuar processamento em tempo real para emitir a região de acesso.

Quando o código de erro é determinado não se refere um código de erro indicando "nenhuma região" conforme um resultado da determinação no passo S810 (NÃO no passo S810), o código de erro é um código de erro indicando "truncamento computacional errado". Neste caso, o tíquete de acesso do chip 104 do aplicativo 102 ou o valor de PIN no chip seguro 114 não pode o último. Conseqüentemente, o módulo de controle do chip seguro 110 notifica ao usuário que pode ser necessário atualizar o aplicativo 102 ou o valor de PIN (passo S814). No passo S814, o módulo de controle do chip seguro 110 pode trocar informação com o aplicativo 102, e verifica se uma nova versão do aplicativo foi ou não liberado. Quando a nova versão do aplicativo foi liberada, o módulo de controle do chip seguro 110 pode baixar e atualizar o aplicativo. O módulo de controle do chip seguro 110 pode atualizar o valor de PIN solicitando ao servidor de emissão de região de acesso 500 para efetuar processamento em tempo real para mudar o valor de PIN.

De acordo com o processamento efetuado em acordo com o código de erro mostrado na FIG. 12, o usuário pode entender a razão por que o tíquete de acesso do chip é determinado não ser legal. Daí em diante, processamento requerido pode ser automaticamente executado, Por conseguinte, a usabilidade para o usuário pode ser melhorado.

Quando o aplicativo é atualizado, a região é emitida, ou o

valor de PIN é atualizado no processamento efetuado de acordo com o código de erro mostrado na FIG. 12, o módulo de controle do chip seguro 110 pode emitir o comando de autenticação de tíquete do tíquete de acesso do chip para o chip seguro 114 de novo, e pode forçar o chip seguro 114 para efetuar o processamento de autenticação de tíquete de acesso do chip de novo. Nesta ocasião, quando o módulo de controle do chip seguro 110 recebe o mesmo código de erro que um anterior do chip seguro 114, o módulo de controle do chip seguro 110 usar a122 para notificar o usuário da ocorrência de anormalidade, e termina o aplicativo.

Modalidades da presente divulgação podem ser realizada fornecendo um meio de armazenamento armazenando códigos de programa do software para realizar as funções de cada uma das modalidades exemplo descritas acima para um sistema ou um aparelho e forçando o computador (ou CPU, MPU, ou o similar) do sistema ou do aparelhos a ler e executa códigos de programa armazenados no meio de armazenamento.

Neste caso, os códigos de programa lidos do meio de armazenamento realiza as funções de cada uma das modalidades exemplo descritas acima.

Exemplos dos meios de armazenamento para fornecer os códigos de programa incluem um disco flexível (marca comercial registrada), um disco rígido, um disco magnético – óptico, um disco óptico tal como CD-ROM, CD-R, CD-RW, DVD-ROM, DVD-RAM, DVD-RW e DVD+RW, uma fita magnética, um cartão de memória não volátil, e uma ROM. Alternativamente, os códigos de programa podem ser baixados via uma rede.

Adicionalmente, as funções de cada uma das modalidades exemplo descritas acima podem ser realizadas não somente executando os códigos de programas lidos pelo computador, mas também forçando um OS (sistema operacional) ou o similar que é executado no computador para efetuar uma parte ou todos dos processamentos efetivos com base em

instruções dos códigos de programa.

Adicionalmente, as funções de cada uma das modalidades exemplo descritas acima podem ser realizadas escrevendo os códigos de programa lidos do meio de armazenamento em uma memória fornecida em um cartão de expansão de função inserido em um computador ou em uma unidade de expansão de função conectada ao computador e então forçando uma CPU ou o similar fornecido no cartão de expansão ou na unidade de expansão para efetuar uma parte ou todos dos processamentos efetivos com base em instruções dos códigos de programa.

Deve ser entendido que várias mudanças e modificações para as modalidades presentemente preferidas aqui descritas serão aparentes para aqueles com habilidade na técnica. Tais mudanças e modificações podem ser feitas sem fugir do espírito e escopo da presente questão e sem diminuir suas vantagens pretendidas. É, por conseguinte, pretendido que tais mudanças e modificações sejam cobertas pelas reivindicações anexas.

REIVINDICAÇÕES

1. Chip de circuito integrado, caracterizado pelo fato de compreender:

uma unidade de controle de autenticação configurada para autenticar uma solicitação usando informação de autenticação,

onde pelo menos uma dentre a solicitação e a informação de autenticação é recebida a partir de fora do chip de circuito integrado.

2. Chip de circuito integrado de acordo com a reivindicação 1, caracterizado pelo fato de que a solicitação inclui pelo menos um dentre um comando executável, uma região de acesso, e um código de identificação de emissor.

3. Chip de circuito integrado de acordo com a reivindicação 1, caracterizado pelo fato de que a informação de autenticação inclui um valor de erros de dados.

4. Chip de circuito integrado de acordo com a reivindicação 1, caracterizado pelo fato de que um dispositivo de emissão do chip de circuito integrado gera pelo menos uma da solicitação e da informação de autenticação.

5. Chip de circuito integrado de acordo com a reivindicação 4, caracterizado pelo fato de que o dispositivo de emissão emite a pelo menos uma dentre a solicitação e a informação de autenticação para um gerador de aplicativo.

6. Chip de circuito integrado de acordo com a reivindicação 4, caracterizado pelo fato de que o dispositivo de emissão registra informação relacionada a uma região de acesso da solicitação com um servidor de emissão de região de acesso.

7. Chip de circuito integrado de acordo com a reivindicação 4, caracterizado pelo fato de que o dispositivo de emissão registra um valor de PIN relacionado a uma região de acesso da solicitação com um servidor de

emissão de região de acesso.

8. Chip de circuito integrado de acordo com a reivindicação 1, caracterizado pelo fato de que o chip de circuito integrado executa um comando com base em:

(i) informação sobre comandos que um aplicativo é permitido executar e

(ii) informação sobre regiões de memória do chip de circuito integrado que o aplicativo é permito acessar.

9. Chip de circuito integrado de acordo com a reivindicação 1, caracterizado pelo fato de que um módulo de controle de chip:

recebe a solicitação a partir de um aplicativo,

liga o chip de circuito integrado,

emite um comando de autenticação para o chip de circuito integrado, e

transmite a solicitação para o chip de circuito integrado.

10. Chip de circuito integrado de acordo com a reivindicação 9, caracterizado pelo fato de que a solicitação é recebida no chip de circuito integrado, e em resposta à solicitação, o circuito integrado conduz um acesso para a localização da memória.

11. Chip de circuito integrado de acordo com a reivindicação 9, caracterizado pelo fato de que:

a solicitação é autenticada para determinar se a solicitação é legal,

a solicitação é determinada para ser legal,

a solicitação é aceita,

o chip de circuito integrado notifica o módulo de controle do chip que a solicitação foi aceita, e

o módulo de controle do chip notifica o aplicativo que a solicitação foi autenticada.

12. Chip de circuito integrado de acordo com a reivindicação 11, caracterizado pelo fato de que:

o aplicativo chama um API de operação de chip para usar o chip de circuito integrado,

o módulo de controle de chip emite um comando executável ao chip de circuito integrado,

a unidade de controle de autenticação verifica se o comando executável é permito ser executado e se a região de acesso do comando executável é permitido ser acessado.

13. Chip de circuito integrado de acordo com a reivindicação 12, caracterizado pelo fato de que:

o chip de circuito integrado executa o comando executável,

o chip de circuito integrado notifica o módulo de controle do chip do resultado da execução do comando executável,

o módulo de controle do chip notifica o aplicativo do resultado da execução do comando executável,

o aplicativo solicita o módulo de controle do chip para terminar o uso do chip de circuito integrado, e

o módulo de controle do chip desliga o chip de circuito integrado.

14. Chip de circuito integrado de acordo com a reivindicação 13, caracterizado pelo fato de que a solicitação e a informação de autenticação são apagadas.

15. Chip de circuito integrado de acordo com a reivindicação 1, caracterizado pelo fato de que seguindo a autenticação da solicitação, informação que é legalmente acessada pela solicitação é exibida em uma unidade de exibição.

16. Aparelho de processamento de informação, caracterizado pelo fato de compreender:

um chip de circuito integrado incluindo uma unidade de controle de autenticação configurado para autenticar uma solicitação usando informação de autenticação,

onde pelo menos uma dentre a solicitação e a informação de autenticação é recebida de fora do chip de circuito integrado.

17. Aparelho de processamento de informação de acordo com a reivindicação 16, caracterizado pelo fato de que o aparelho de processamento de informação é um telefone portátil.

18. Sistema de processamento de informação, caracterizado pelo fato de compreender:

um aparelho de processamento de informação incluindo um chip de circuito integrado incluindo uma unidade de controle de autenticação configurada para autenticar uma solicitação usando informação de autenticação,

onde pelo menos uma dentre a solicitação e a informação de autenticação é recebida de fora do chip de circuito integrado.

19. Método, caracterizado pelo fato de compreender

autenticar, através de um chip de circuito integrado incluindo uma unidade de controle de autenticação, uma solicitação usando informação de autenticação,

onde pelo menos uma dentre a solicitação e a informação de autenticação é recebida de fora do chip de circuito integrado.

20. Meio de armazenamento, caracterizado pelo fato de que armazena um programa que, quando executado, força um chip de circuito integrado incluindo uma unidade de controle de autenticação a autenticar uma solicitação usando informação de autenticação,

onde pelo menos uma dentre a solicitação e a informação de autenticação é recebida de fora do chip de circuito integrado.

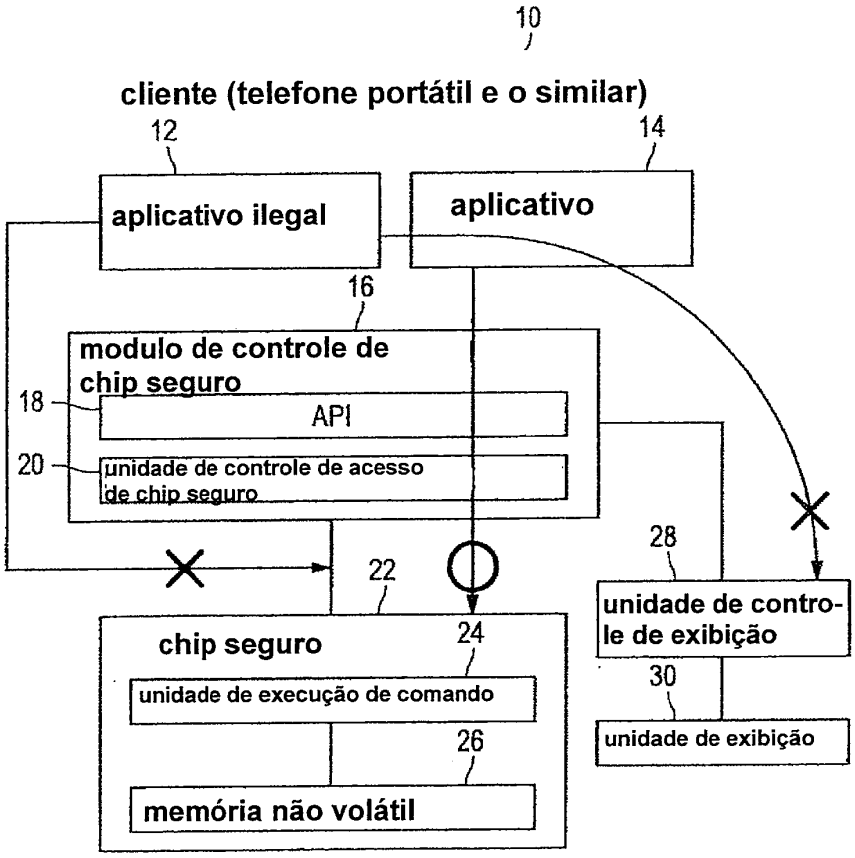
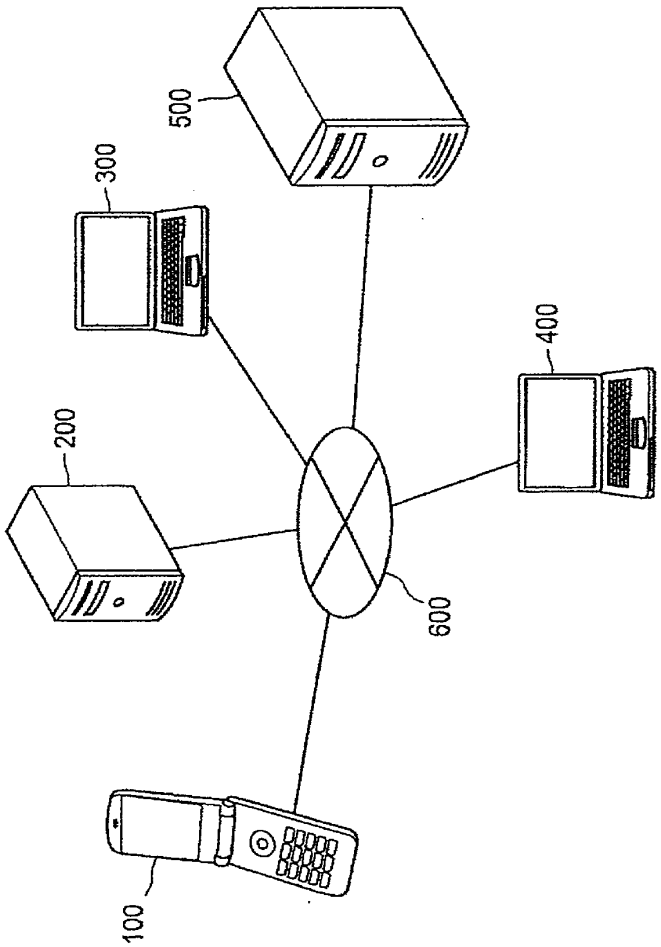

10
cliente (telefone portátil e o similar)
12
14
aplicativo ilegal
aplicativo
16
modulo de controle de chip seguro
18
API
20
unidade de controle de acesso de chip seguro
28
22
unidade de controle de exibição
chip seguro
24
unidade de execução de comando
30
unidade de exibição
26
memória não volátil

FIG.1

FIG.2



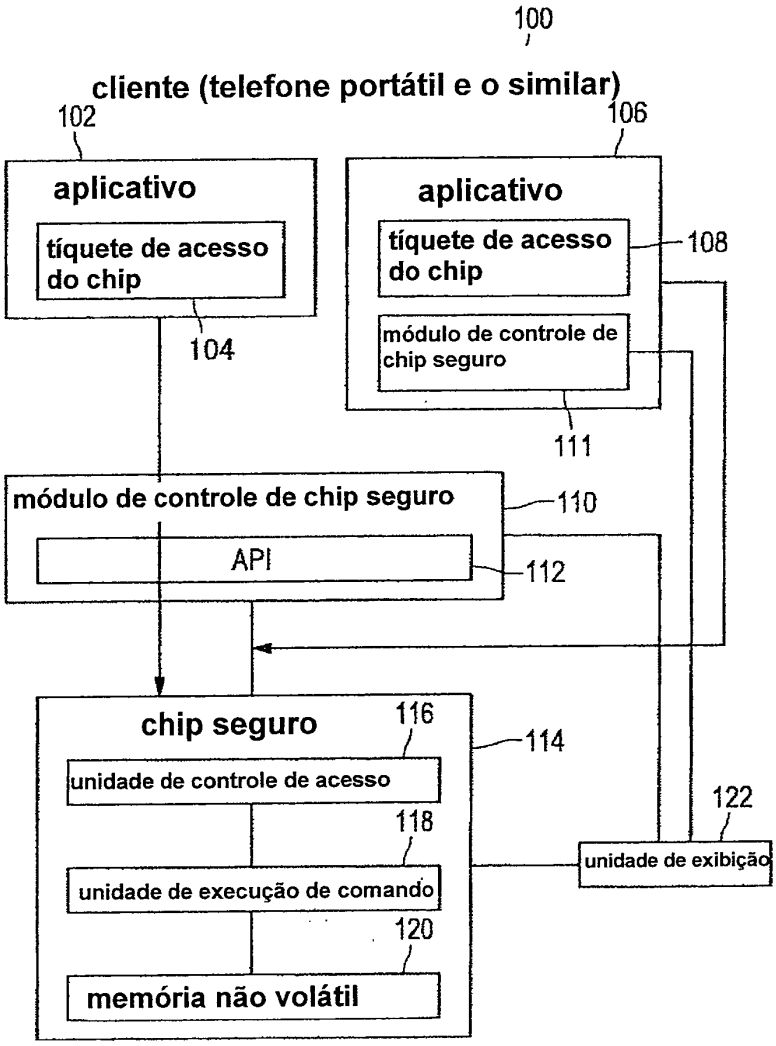

100
cliente (telefone portátil e o similar)
102
aplicativo
tíquete de acesso do chip
104
106
aplicativo
tíquete de acesso do chip
108
módulo de controle de chip seguro
111
módulo de controle de chip seguro
110
API
112
chip seguro
116
114
unidade de controle de acesso
118
unidade de execução de comando
120
memória não volátil
122
unidade de exibição

FIG.3

FIG. 4

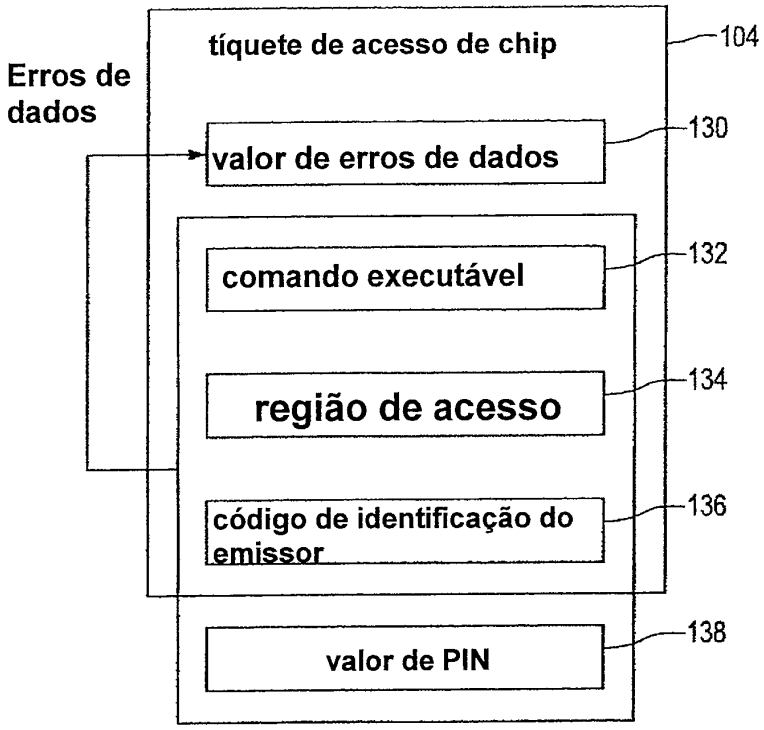

Erros de dados
tíquete de acesso de chip
104
valor de erros de dados
130
comando executável
132
região de acesso
134
código de identificação do emissor
136
valor de PIN
138

FIG.5

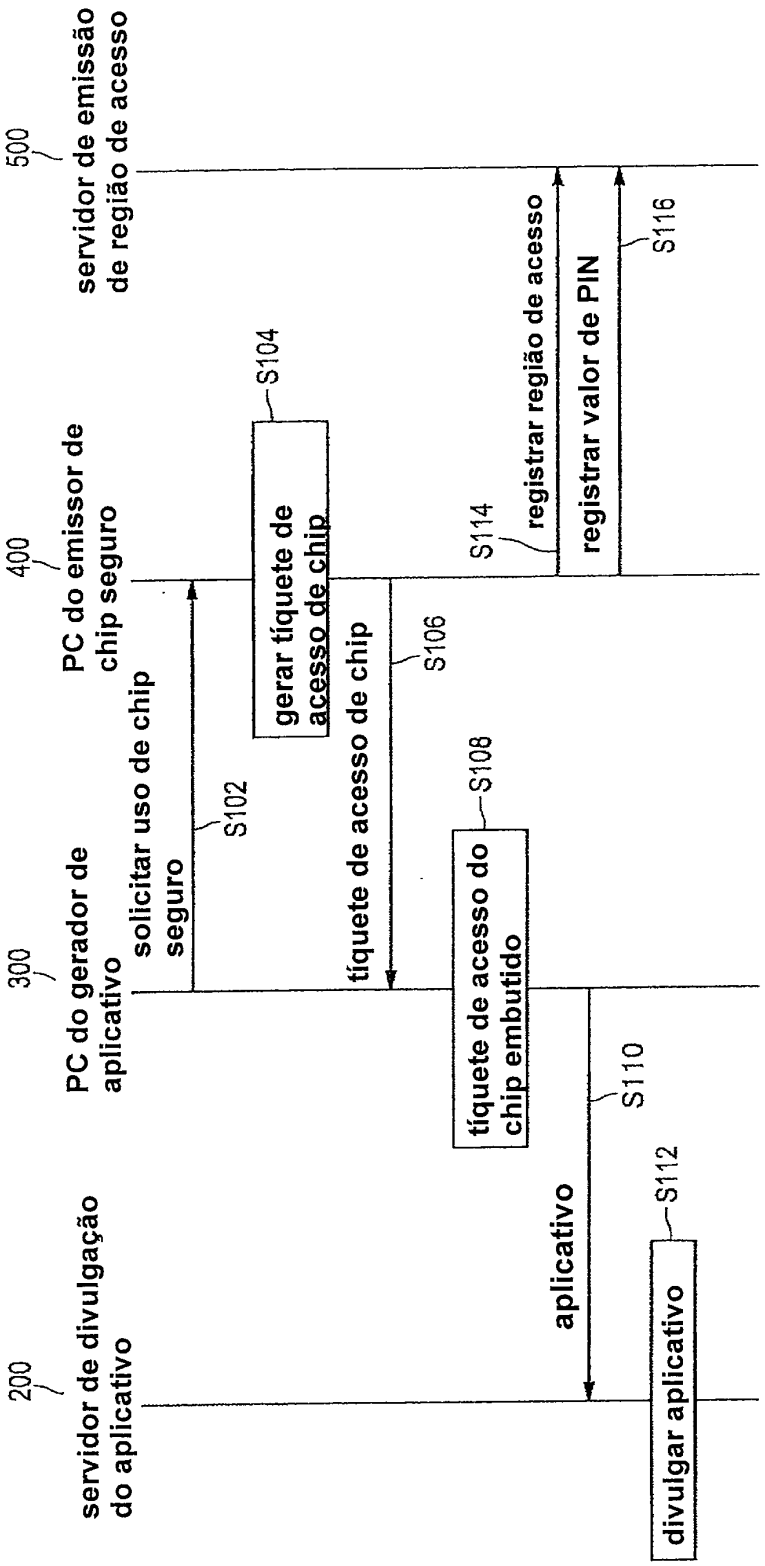

200
servidor de divulgação do aplicativo
300
PC do gerador de aplicativo
400
PC do emissor de chip seguro
500
servidor de emissão de região de acesso
solicitar uso de chip seguro
S102
gerar tíquete de acesso de chip
S104
tíquete de acesso de chip
S106
tíquete de acesso do chip embutido
S108
aplicativo
S110
divulgar aplicativo
S112
registrar região de acesso
S114
registrar valor de PIN
S116

FIG. 6

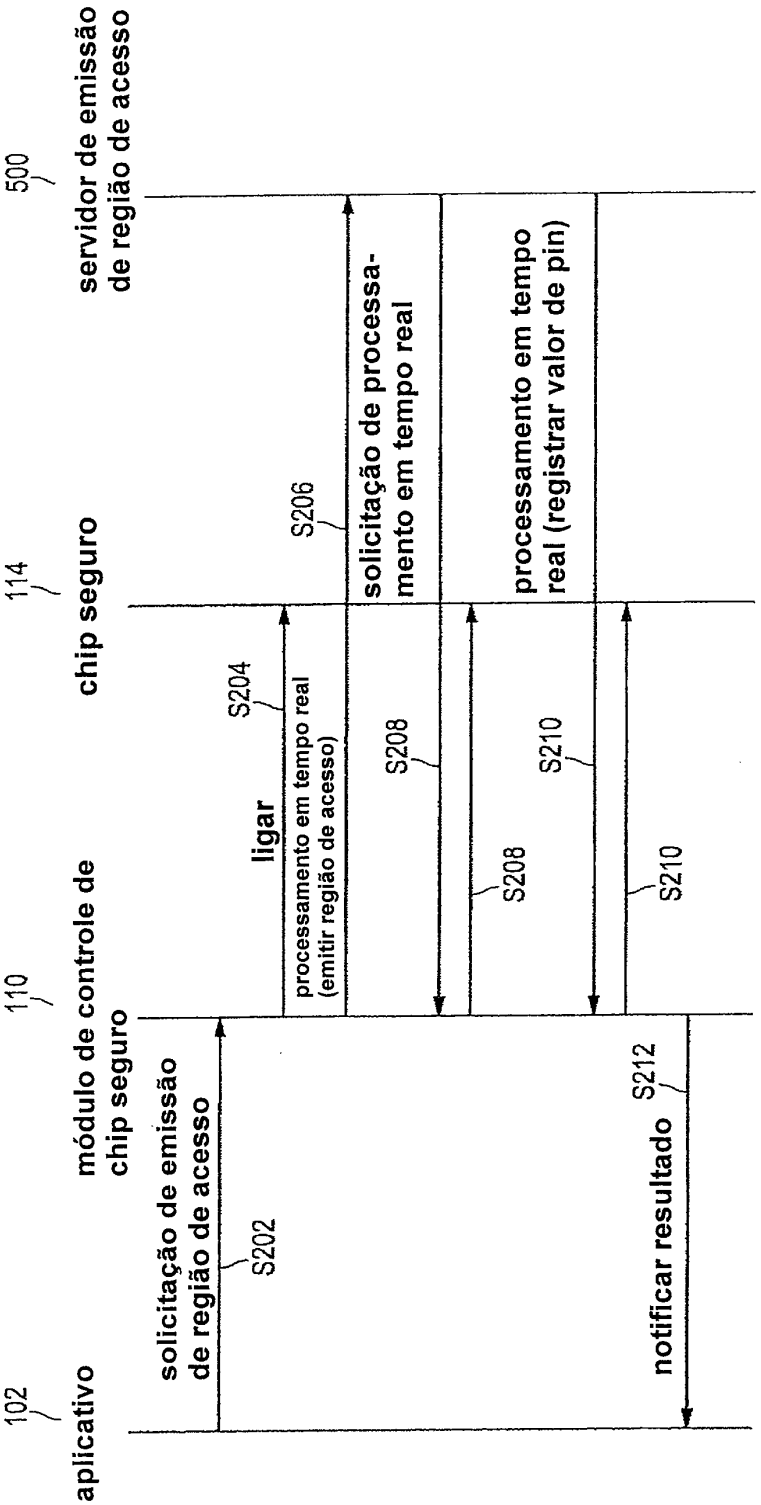

102
aplicativo
110
módulo de controle de chip seguro
114
chip seguro
500
servidor de emissão de região de acesso
solicitação de emissão de região de acesso
S202
ligar
S204
processamento em tempo real (emitir região de acesso)
S206
solicitação de processamento em tempo real
S208
S208
processamento em tempo real (registrar valor de pin)
S210
S210
notificar resultado
S212

FIG.7

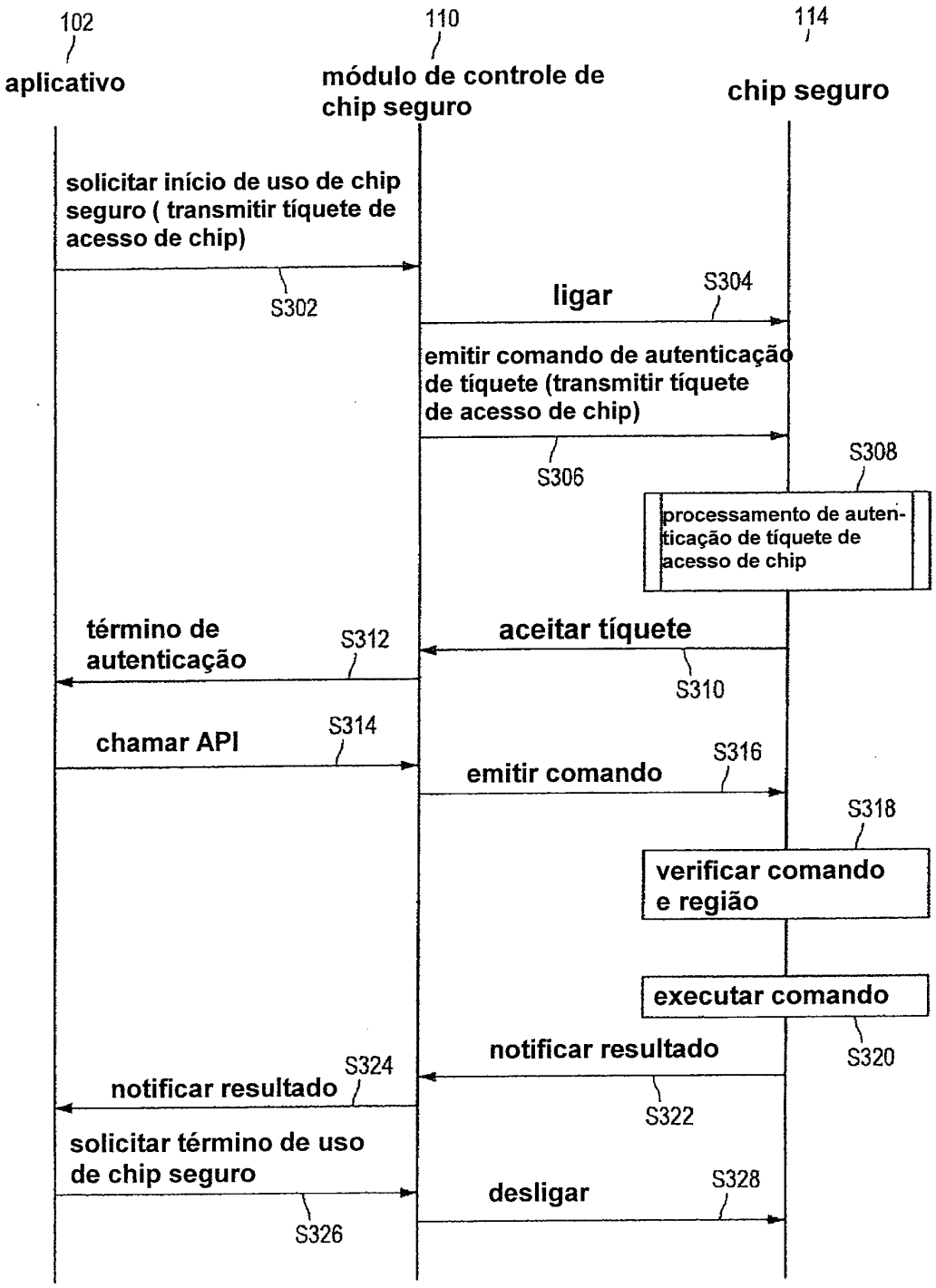

102
aplicativo
110
módulo de controle de chip seguro
114
chip seguro
solicitar início de uso de chip seguro (transmitir tíquete de acesso de chip)
S302
ligar
S304
emitir comando de autenticação de tíquete (transmitir tíquete de acesso de chip)
S306
S308
processamento de autenticação de tíquete de acesso de chip
término de autenticação
S312
aceitar tíquete
S310
chamar API
S314
emitir comando
S316
S318
verificar comando e região
executar comando
S320
notificar resultado
S324
notificar resultado
S322
solicitar término de uso de chip seguro
S326
desligar
S328

FIG. 8

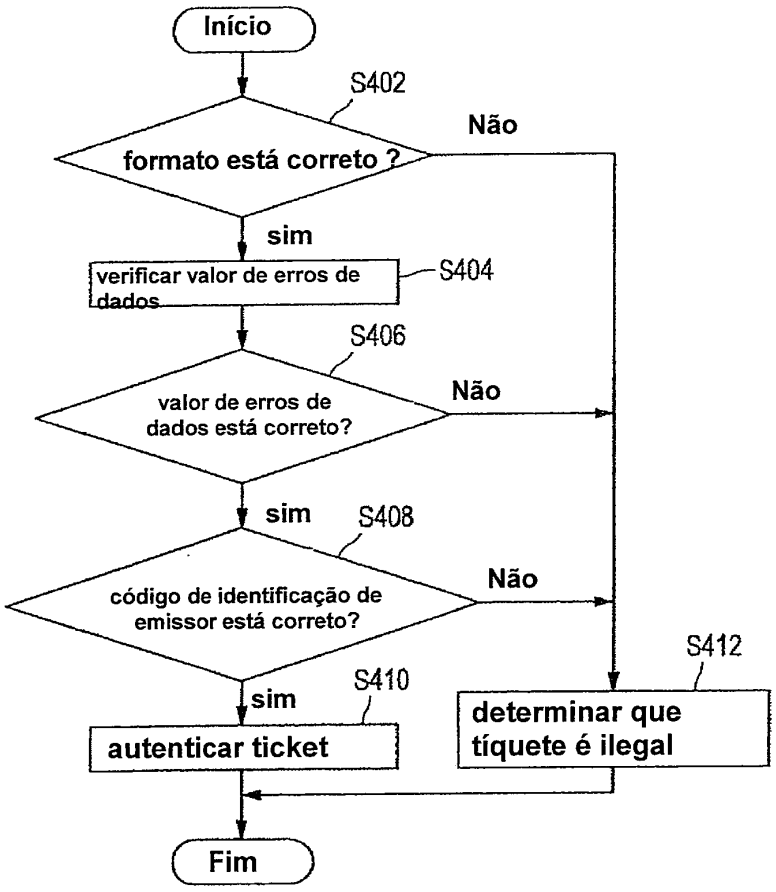

Início
S402
formato está correto ?
Não
sim
verificar valor de erros de dados
S404
S406
valor de erros de dados está correto?
Não
sim
S408
código de identificação de emissor está correto?
Não
S412
sim
S410
autenticar ticket
determinar que tíquete é ilegal
Fim

FIG.9

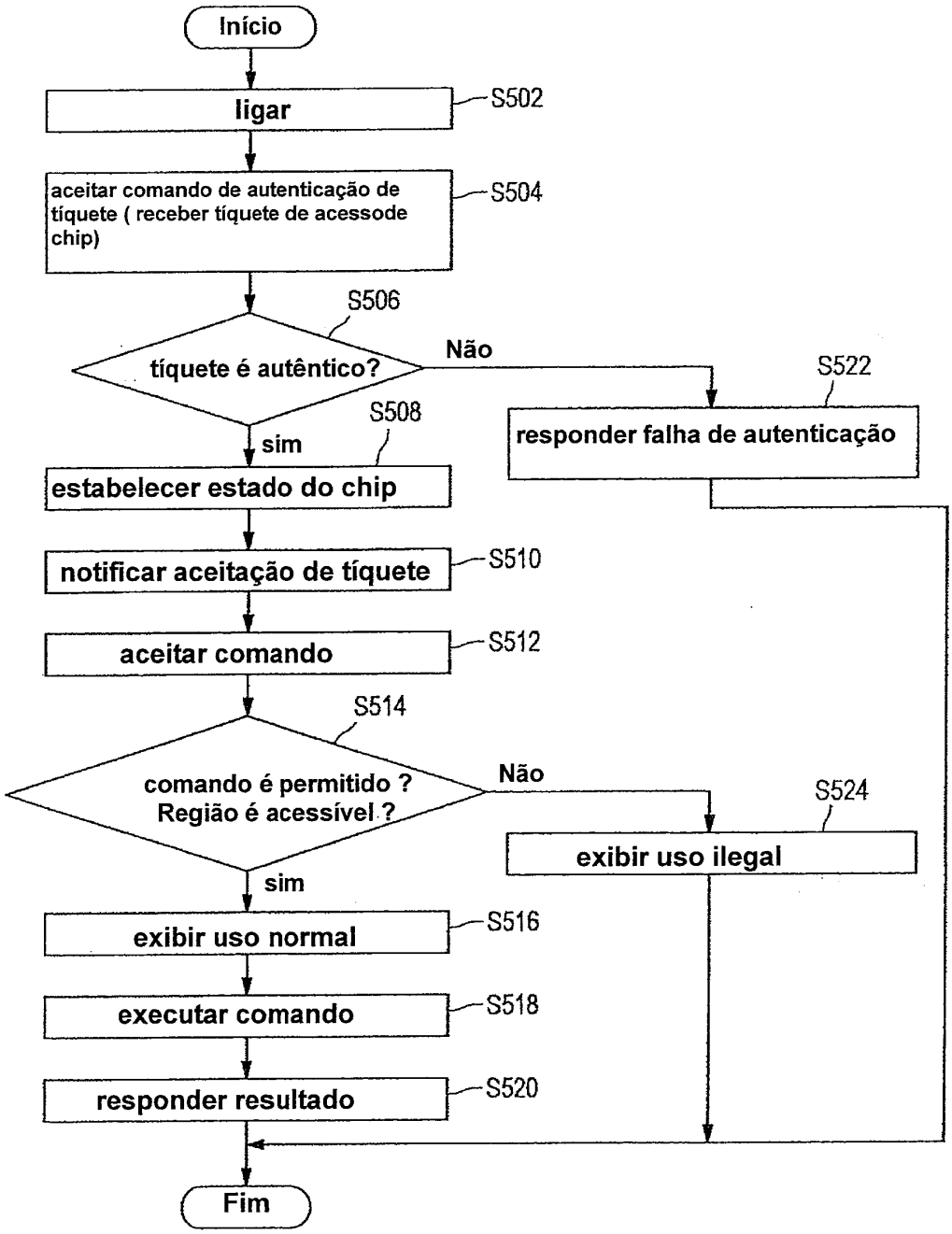

Início
ligar
S502
aceitar comando de autenticação de tíquete (receber tíquete de acessode chip)
S504
S506
tíquete é autêntico?
Não
S522
responder falha de autenticação
sim
S508
estabelecer estado do chip
notificar aceitação de tíquete
S510
aceitar comando
S512
S514
comando é permitido ?
Região é acessível ?
Não
S524
exibir uso ilegal
sim
exibir uso normal
S516
executar comando
S518
responder resultado
S520
Fim

FIG.10

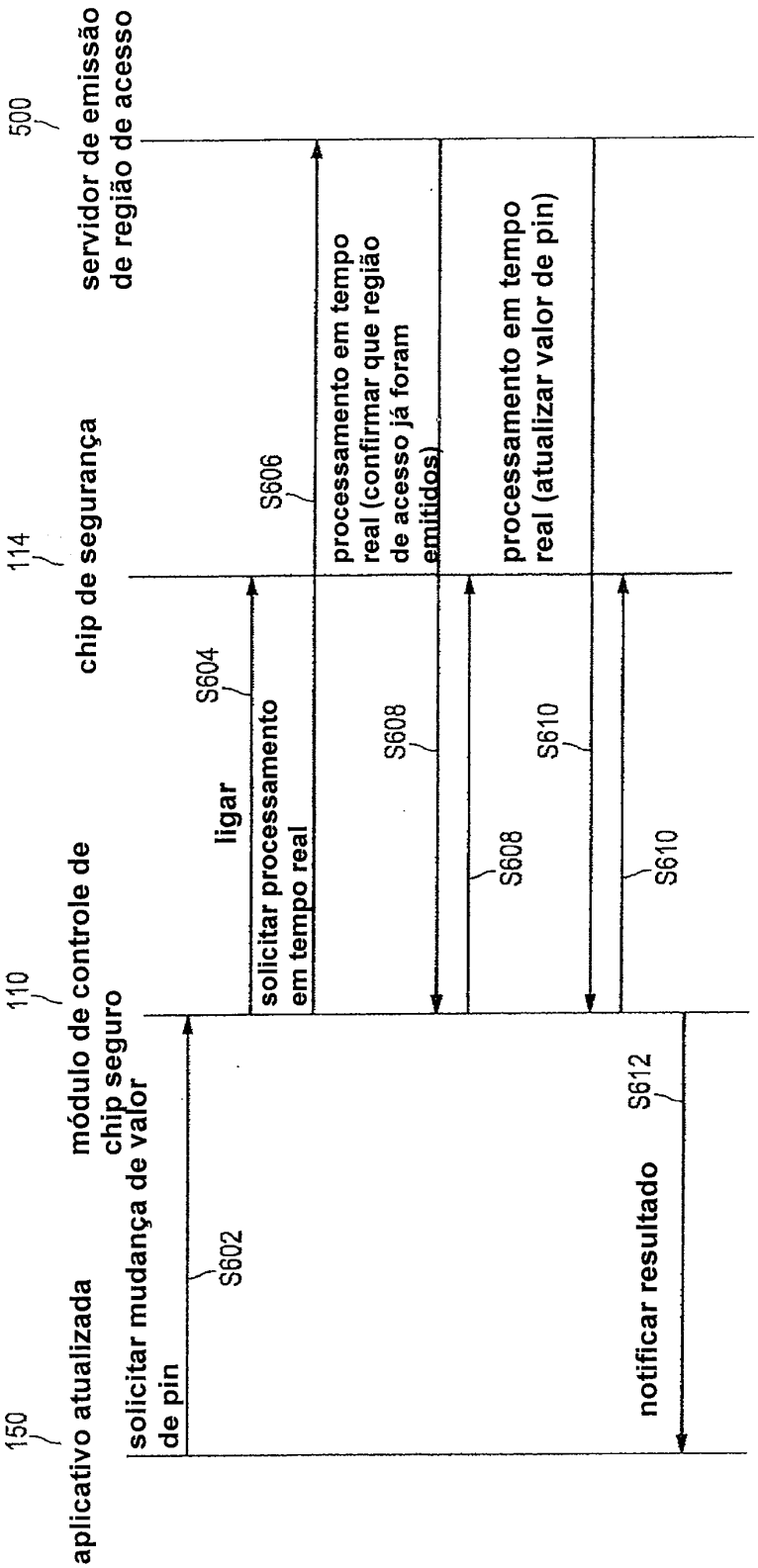

150
aplicativo atualizada
110
módulo de controle de chip seguro
114
chip de segurança
500
servidor de emissão de região de acesso
solicitar mudança de valor de pin
S602
ligar
S604
solicitar processamento em tempo real
S606
processamento em tempo real (confirmar que região de acesso já foram emitidos)
S608
S608
processamento em tempo real (atualizar valor de pin)
S610
S610
notificar resultado
S612

FIG. 11

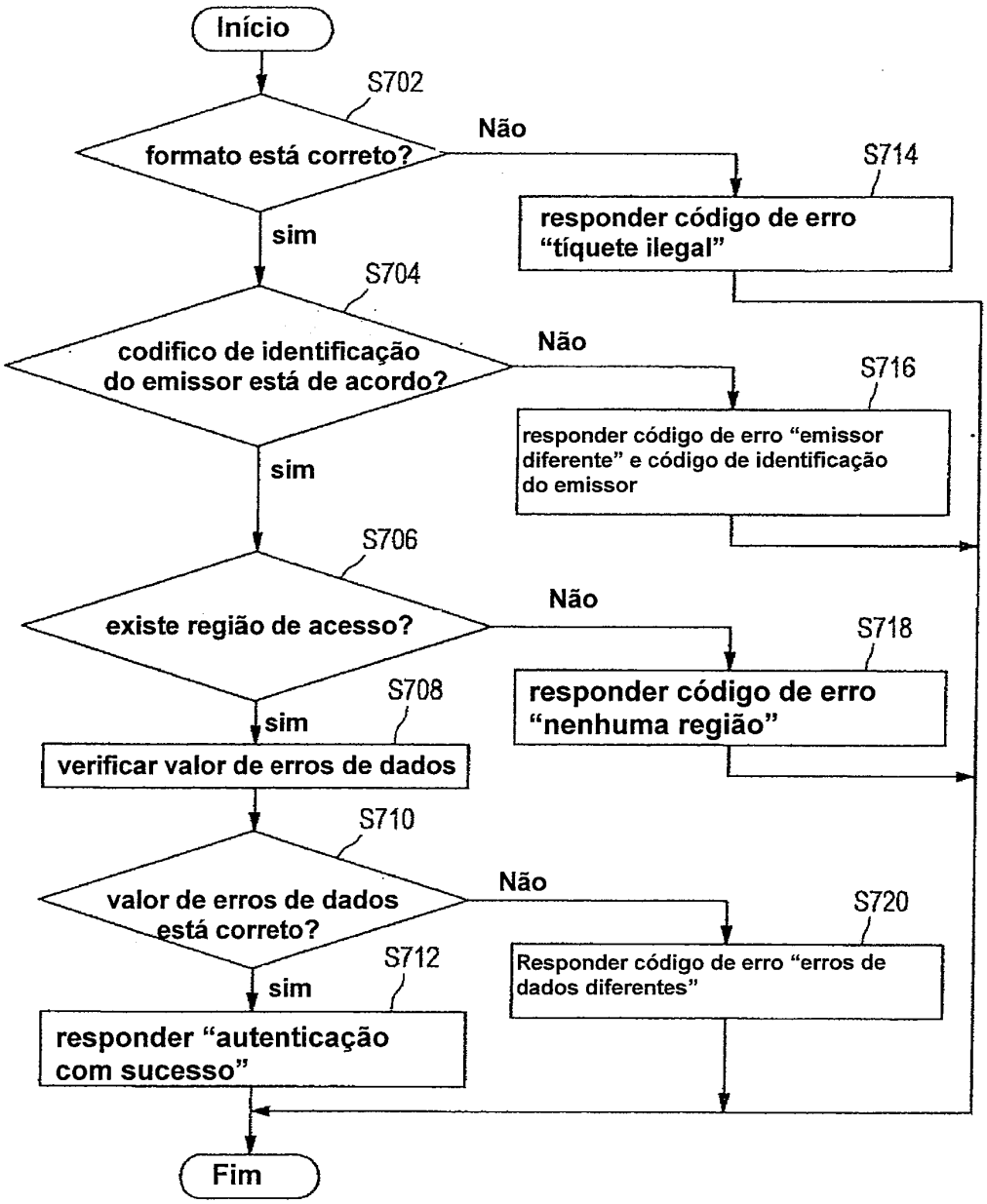
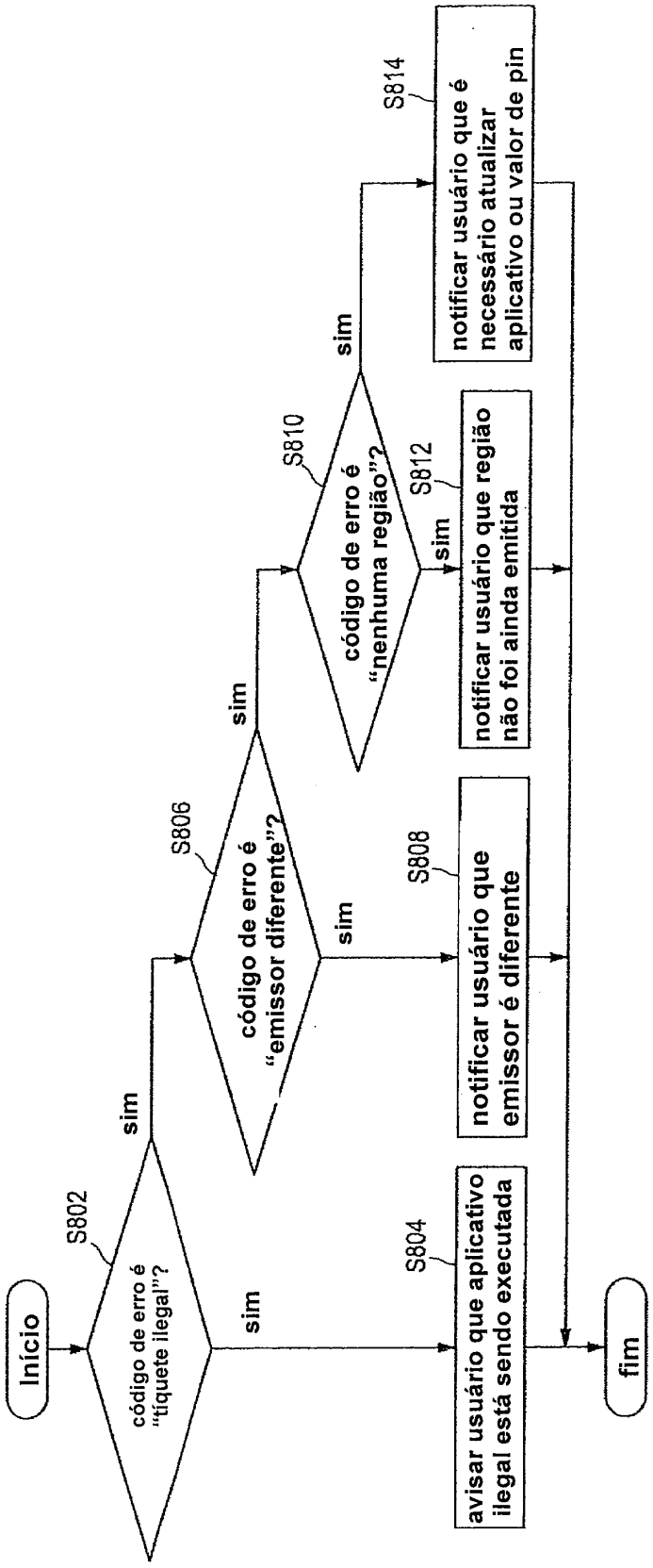

Início
S702
formato está correto?
Não
S714
responder código de erro "tíquete ilegal"
sim
S704
codifico de identificação do emissor está de acordo?
Não
S716
responder código de erro "emissor diferente" e código de identificação do emissor
sim
S706
existe região de acesso?
Não
S718
responder código de erro "nenhuma região"
sim
S708
verificar valor de erros de dados
S710
valor de erros de dados está correto?
Não
S720
Responder código de erro "erros de dados diferentes"
sim
S712
responder "autenticação com sucesso"
Fim

FIG. 12


Início
código de erro é "tíquete ilegal"?
S802
sim
sim
avisar usuário que aplicativo ilegal está sendo executada
S804
código de erro é "emissor diferente"?
S806
sim
sim
notificar usuário que emissor é diferente
S808
código de erro é "nenhuma região"?
S810
sim
sim
notificar usuário que região não foi ainda emitida
S812
notificar usuário que é necessário atualizar aplicativo ou valor de pin
S814
fim

RESUMO

"CHIP DE CIRCUITO INTEGRADO, APARELHO DE PROCESSAMENTO DE INFORMAÇÃO, SISTEMA DE PROCESSAMENTO DE INFORMAÇÃO, MÉTODO, E, MEIO DE ARMAZENAMENTO"

Um chip de IC, um aparelho de processamento de informação, sistema, método, e programa são fornecidos. Um chip de IC inclui uma unidade de controle de autenticação configurado para autenticar uma solicitação usando informação de autenticação, A solicitação e/ou a informação de autenticação é recebida a partir de fora do chip de IC.