República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(11) PI 0703503-9 B1

(22) Data do Depósito: 14/09/2007

(45) Data de Concessão: 03/09/2019

(54) Título: MÉTODO PARA VALIDAR COMPONENTES DE MÁQUINA EM UM TERMINAL DE AUTO-SERVIÇO, UNIDADE DE PROCESSAMENTO DE TERMINAL DE AUTO-SERVIÇO E TERMINAL DE AUTO-SERVIÇO

(51) Int.Cl.: G07F 19/00.

(30) Prioridade Unionista: 15/09/2006 US 11/521,712.

(73) Titular(es): NCR CORPORATION.

(72) Inventor(es): ALEXANDER W. WHYTOCK; MICHAEL J. NEILAN; JAMES HENDERSON.

(57) Resumo: VALIDAÇÃO DE SEGURANÇA DE COMPONENTES DE MÁQUINA É descrito um método para validar componentes de máquina em um terminal de auto-serviço que compreende prover pelo menos um componente de máquina com um identificador legível por máquina e ler dados de identidade provenientes do identificador legível por máquina usando uma unidade de processamento. Os dados de identidade são comparados com dados de identidade armazenados na memória da unidade de processamento para determinar se a identidade de um componente mudou. Se a identidade mudou, a unidade de processamento compara os dados de identidade com dados de origem para determinar se o componente é proveniente de uma fonte confiável.Em uma modalidade, o terminal de auto-serviço é um ATM e os componentes são uma plataforma de criptografia de Número de Identificação Pessoal (PIN), uma unidade de distribuição de dinheiro em espécie e um leitor de cartão.

"MÉTODO PARA VALIDAR COMPONENTES DE MÁQUINA EM UM TERMINAL DE AUTO-SERVIÇO, UNIDADE DE PROCESSAMENTO DE TERMINAL DE AUTO-SERVIÇO E TERMINAL DE AUTO-SERVIÇO"

CAMPO TÉCNICO

A presente invenção diz respeito a validação de segurança para partes componentes de terminais de auto-serviço (SST) e, em particular, mas não exclusivamente, a componentes para caixas eletrônicos automatizados (ATMs).

ANTECEDENTES DA INVENÇÃO

SSTs compreendem máquinas que dispensam produtos para um usuário ou realizam serviços para ele. Um exemplo comum de um SST é um ATM. Quando estas máquinas apresentam uma falha ou têm que sofrer uma manutenção depois que elas forem instaladas em um local, um engenheiro ou operador de manutenção é usualmente enviado para diagnosticar o problema e/ou corrigir a falha. Quando a correção ou a falha exigir instalação de um componente de reposição, há um risco de que o componente de reposição possa ser de um padrão inferior ao do componente inicialmente instalado pelo fabricante do SST.

Tomando o exemplo de um ATM, há um interesse particular de que o componente de reposição seja de um padrão superior já que um ATM é usado como uma interface para transações financeiras. Além do mais, ATMs freqüentemente são alvos de ladrões que podem deliberadamente instalar um componente de reposição com um propósito malicioso, por exemplo, para conseguir acesso à informação de segurança inserida por um usuário subseqüente do ATM.

Em um método da tecnologia anterior, o problema é

resolvido exigindo que um engenheiro certifique-se que os componentes de reposição estão em bom estado de funcionamento imediatamente depois da sua instalação. Este processo procede substancialmente como segue:

Quando um engenheiro é chamado a um SST falho, ele usa um dispositivo no ATM conhecido como um Painel Operador. Um Painel Operador é uma unidade de processamento arranjada para prover uma interface de usuário ao engenheiro e para guiar o engenheiro através dos procedimentos de serviço e diagnóstico. A fim de executar os procedimentos, o engenheiro deve passar por um teste de autorização de segurança. Isto é normalmente alcançado exigindo que o engenheiro use um plugue de segurança USB conhecido neste contexto como uma Chave de Segurança de Serviço.

No momento em que realiza o serviço no SST, pode ser exigido que o engenheiro substitua um componente falho. O SST é arranjado de maneira tal que é exigida certificação de que o componente está completamente funcional antes que o SST retorne à sua operação normal. A certificação é executada pelo engenheiro através do Painel Operador e usando a Chave de Segurança de Serviço. Um problema com este método é que caso o engenheiro não tenha sua Chave de Segurança de Serviço, ou caso a própria Chave esteja falha, então o SST não irá retornar à sua operação normal. Adicionalmente, embora o método garanta que o componente de reposição esteja funcional, ele não garante que o componente de reposição venha de uma fonte confiável.

SUMÁRIO DA INVENÇÃO

De acordo com um primeiro aspecto da invenção, é provido um método para validar componentes de máquina em um terminal de auto-serviço compreendendo: prover pelo menos um componente de máquina com informação de identidade na forma de um identificador legível por máquina lendo dados de identidade provenientes do identificador legível por máquina; comparar os dados de identidade com dados de identidade armazenados para determinar se a identidade de um componente mudou; e, se a identidade mudou, comparar os dados de identidade com dados de origem para determinar se o componente é proveniente de uma fonte confiável.

Isto provê um método conveniente para verificar a qualidade e integridade dos componentes. Percebe-se que os terminais de auto-serviço freqüentemente aceitam dinheiro em espécie e alguns, por exemplo, caixas eletrônicos automatizados (ATMs), são usados para transações financeiras. Isto significa que padrões superiores devem ser mantidos para os componentes dos terminais. Quando um componente for proveniente de uma fonte confiável, pode-se presumir que o padrão superior foi satisfeito. Além do mais, terminais são freqüentemente alvos de pessoas maliciosas e, como tal, é importante ser capaz de verificar se os componentes são genuínos e não podem ser usados para enganar usuários de um terminal.

Preferivelmente, o método é realizado na inicialização do terminal. Isto é conveniente já que, no geral, o terminal será desligado a fim de substituir um de seus componentes. Verificar a origem de qualquer componente substi-

tuído na inicialização significa que todos os componentes que não forem provenientes de uma fonte confiável serão detectados antes que possa ser feito uso do terminal.

Em tal modalidade, o método pode compreender desabilitar o terminal se um componente não for proveniente de uma fonte confiável. Isto é vantajoso já que impede que o terminal fique operacional com componentes não confiáveis.

O método pode compreender adicionalmente substituir os dados de identidade armazenados com os dados de identidade modificados se a identidade mudou. Isto é vantajoso já que a origem de um componente não será determinada no futuro a menos que o componente seja substituído.

Em uma modalidade preferida, o método compreende verificar dados de segurança antes que os dados de identidade armazenados sejam substituídos com dados de identidade modificados. Isto é vantajoso já que ajuda a garantir que qualquer substituição de um componente foi realizada por um operador ou engenheiro autorizado.

De acordo com um segundo aspecto da invenção, é provida uma unidade de processamento de terminal de autoserviço compreendendo uma memória para armazenar dados de identidade, um dispositivo de solicitação arranjado para solicitar dados de identidade de componentes do terminal e um dispositivo de comparação arranjado para comparar dados de identidade recebidos pelo dispositivo de solicitação com dados de identidade armazenados na memória para detectar qualquer mudança nos dados de identidade.

Em uma modalidade, a memória da unidade de proces-

samento compreende dados da origem do componente e o dispositivo de comparação é arranjado para comparar dados de identidade modificados com os dados de origem para determinar se o componente deriva de uma fonte confiável.

Preferivelmente, a unidade de processamento compreende adicionalmente um dispositivo de segurança arranjado para receber dados de segurança de um operador de manutenção e usar os dados de segurança para determinar se um operador de manutenção é um operador autorizado.

Preferivelmente, a unidade de processamento é arranjada para permitir que um terminal com o qual ela está associada opere somente se o componente ou cada um dos componentes for proveniente de uma fonte confiável.

De acordo com um terceiro aspecto da invenção, é provido um terminal de auto-serviço compreendendo uma unidade de processamento de acordo com o segundo aspecto da invenção e compreendendo adicionalmente pelo menos um dos seguintes componentes: uma plataforma de criptografia PIN, uma unidade de distribuição de dinheiro em espécie e um leitor de cartão, o terminal sendo arranjado de maneira tal que dados de identidade associados com o componente ou cada um dos componentes possam ser lidos pela unidade de processamento.

Em uma modalidade preferida, o terminal compreende um de cada um dos componentes supramencionados e a unidade de processamento é arranjada para determinar se cada um dos componentes é proveniente de uma fonte confiável e para permitir que o terminal opere somente se todos os componentes forem provenientes de uma fonte confiável.

Preferivelmente, os dados de identidade associados com o componente ou cada um dos componentes são providos em uma plaqueta de circuito integrado.

Em uma modalidade, o terminal de auto-serviço é um caixa eletrônico automatizado.

De acordo com um quarto aspecto da invenção, é provido um suporte lógico de computador arranjado para realizar o método do primeiro aspecto da invenção.

De acordo com um quinto aspecto da invenção, é provido um suporte lógico de computador, o qual, carregado em uma unidade de processamento, faz com que a unidade de processamento aja como a unidade de processamento do segundo aspecto da invenção.

Os expostos, e ainda outros objetivos, recursos e vantagens da presente invenção ficarão aparentes a partir da seguinte descrição e dos desenhos anexos.

DESCRIÇÃO RESUMIDA DOS DESENHOS

A Figura 1 mostra o painel de um terminal de auto-serviço;

a Figura 2 mostra esquematicamente os componentes internos de um terminal de auto-serviço de acordo com uma modalidade da presente invenção;

a Figura 3 mostra um fluxograma das etapas na 'primeira' inicialização de um ATM; e

a Figura 4 mostra um fluxograma das etapas nas inicializações subseqüentes de um ATM.

DESCRIÇÃO DETALHADA

O terminal de auto-serviço mostrado nas Figuras 1

e 2 é um caixa eletrônico automatizado (ATM) 100. O ATM 100 compreende uma tela 102, uma entrada de cartão 104, dispositivo de entrada de dados na forma de um teclado numérico com 16 botões 106 e botões de seleção de menu 108, e uma saída de distribuição 110.

A Figura 2 mostra os componentes do ATM 100. Os componentes compreendem uma plataforma de criptografia de Número de Identificação Pessoal (PIN) 202, uma unidade de distribuição de dinheiro em espécie 204 e um leitor de cartão 208. O ATM 100 compreende adicionalmente uma unidade de processamento na forma de um núcleo de PC 208. Cada um dos componentes contém neles embutidos uma plaqueta de circuito integrado de identidade 212 compreendendo dados provendo uma identidade de fabricantes. A plataforma de criptografia PIN 202, a unidade de distribuição de dinheiro em espécie 204, o leitor de cartão 206 e a plaqueta de circuito integrado 212 associados com cada um dos componentes 202, 204, 206 são capazes de comunicar com o núcleo do PC 208 através de um barramento de sistema 210.

O núcleo do PC 208 compreende uma memória 214 arranjada para armazenar dados. A memória 214 é capaz de armazenar dados persistentes, isto é, armazenar dados de uma maneira não volátil. O núcleo do PC 208 compreende adicionalmente um dispositivo de solicitação 216 que é arranjado para solicitar e receber dados provenientes das plaquetas de circuito integrado 212 e um dispositivo de comparação 218 arranjado para comparar dados de identidade recebidos pelo dispositivo de solicitação com dados de identidade armazena-

dos na memória 214. O núcleo do PC 208 compreende adicionalmente um dispositivo de segurança 220, arranjado para realizar uma rotina de segurança para verificar a identidade de um operador de manutenção ou engenheiro e para garantir que esta pessoa seja autorizada a instalar um componente de reposição 202, 204, 206.

No uso normal do ATM 100, um usuário insere um cartão portando uma tira magnética e/ou uma plaqueta de circuito integrado de dados criptografados, usualmente um cartão bancário, na entrada de cartão 104. O leitor de cartão 206 lê a tira magnética ou plaqueta de circuito integrado de dados criptografados para obter detalhes associados com o cartão, incluindo dados criptografados do Número de Identificação Pessoal (PIN). Então, a tela 102 é usada para exibir uma mensagem solicitando ao usuário que informe um PIN, o qual o usuário então insere usando o teclado numérico 106. A entrada feita é fornecida à plataforma de criptografia PIN 202, que criptografa o número inserido. O resultado desta criptografia é comparado com os dados PIN criptografados lidos do cartão e, presumindo-se que haja uma correspondência, o usuário pode acessar os serviços através do ATM 100 usando os botões de seleção do menu 108 para selecionar serviços mostrados na tela 102. Se o usuário solicitar dinheiro em espécie, a unidade de distribuição de dinheiro em espécie 204 irá pegar as notas solicitadas de uma série de pilhas de dinheiro provendo diferentes valores e transfere o dinheiro em espécie para a saída de distribuição 110, onde ele pode ser coletado pelo usuário.

Dois exemplos adicionais da inicialização do ATM 100 são agora descritos. O processo na 'primeira' inicialização do ATM 100 é descrito com referência ao fluxograma da Figura 3. Então, o processo de validação para componentes em cada inicialização subseqüente é descrito com referência ao fluxograma da Figura 4.

Antes da 'primeira' inicialização, o ATM 100 é construído usando componentes de origem conhecida para prover a plataforma de criptografia PIN 202, a unidade de distribuição de dinheiro em espécie 204, o leitor de cartão 206 e o núcleo do PC 208 (etapa 302). Neste contexto, uma 'origem conhecida' significa que o fabricante do componente 202, 204, 206 pode ser conhecido e que foi identificado como uma fonte confiável de componentes 202, 204, 206 confiáveis de alta qualidade. O dispositivo de solicitação 216 do núcleo do PC 208 solicita dados de identidade do fabricante provenientes dos componentes 202, 204, 206 através do barramento de sistema 120 (etapa 304). Cada um dos componentes 202, 204, 206 fornece os dados solicitados, que neste exemplo compreende um número serial, na etapa 306. Então, isto é armazenado como dados persistentes na memória 214 do núcleo do PC 208, na etapa 306.

Em cada inicialização subseqüente (etapa 402), o dispositivo de solicitação 216 do núcleo do PC 208 solicita novamente os dados de identidade do fabricante provenientes dos componentes 202, 204, 206 através do barramento de sistema 120 (etapa 404). Cada um dos componentes 202, 204, 206 fornece os dados solicitados para o dispositivo de solicita-

ção 216, na etapa 406. O dispositivo de comparação 218 do núcleo do PC 208 verifica cada uma das identidades fornecidas em função daquelas armazenadas na memória, na etapa 408. Se não houver modificação em qualquer dos dados de identidade, então a inicialização do ATM se completa, na etapa 409. Entretanto, se a identidade de um ou mais dos componentes se modificou, o dispositivo de comparação 218 do núcleo do PC 208 verifica para ver se os novos componentes vêm de uma fonte confiável, na etapa 410.

Nesta modalidade, a identidade de um componente proveniente de uma fonte conhecida está na forma de um número serial que se conforma com um formato pré-determinado que pode ser processado para verificar sua autenticidade. Entretanto, em outras modalidades, o núcleo do PC 208 pode ser arranjado para verificar a identidade em função das identidades armazenadas em uma base de dados, que pode ser remota em relação ao ATM 100.

Se os novos componentes 202, 204, 206 não vierem de uma fonte confiável, então o ATM 100 é desabilitado, na etapa 412. Entretanto, se os novos componentes vierem de uma fonte confiável, então o núcleo do PC 208 solicita que o engenheiro insira dados de segurança para garantir que a instalação do(s) novo(s) componente(s) foi feita por um indivíduo autorizado (etapa 414). Neste exemplo, os dados de segurança são providos na forma de um plugue de segurança USB conhecido neste contexto como uma Chave de Segurança de Serviço.

Na etapa 416, o dispositivo de segurança 220 do

núcleo do PC 208 verifica se a Chave de Segurança de Serviço pertence a um engenheiro autorizado. Se este não for o caso, então o ATM 100 é desabilitado na etapa 418. Se o engenheiro for autorizado, então o núcleo do PC atualiza sua memória 214 com os novos dados de identificação, na etapa 420. Então, a inicialização do ATM 100 se completa, na etapa 422.

Entende-se que a descrição anterior de uma modalidade preferida é dada a título de exemplo somente e que várias modificações podem ser feitas pelos versados na técnica. Por exemplo, as plaquetas de circuito integrado 212 podem ser substituídas por etiquetas de identificação por radiofreqüência (RFID) ou outros dispositivos de armazenamento de dados acessíveis remotamente tais como aqueles legíveis usando tecnologias Bluetooth® ou Infravermelho. Já que estes dispositivos podem ser lidos remotamente, isto elimina a necessidade de um barramento de sistema 214.

REIVINDICAÇÕES

1. Método para validar componentes de máquina em um terminal de auto-serviço (100), que compreende:

i) prover pelo menos um componente de máquina (202, 204, 206) com informação de identidade na forma de um identificador legível por máquina (212);

ii) ler dados de identidade provenientes do identificador legível por máquina (212);

iii) comparar os dados de identidade com dados de identidade armazenados para determinar se a identidade de um componente (202, 204, 206) mudou;

iv) se a identidade mudou, comparar os dados de identidade com dados de origem para determinar se o componente (202, 204, 206) é proveniente de uma fonte confiável;

CARACTERIZADO pelo fato de que compreende ainda:

v) executar as etapas (ii) a (iv) na inicialização do terminal (100); e

vi) desabilitar o terminal (100) se novos componentes (202, 204, 206) não foram provenientes de uma fonte confiável.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que compreende substituir os dados de identidade armazenados com os dados de identidade provenientes de um novo componente (202, 204, 206) se a identidade mudou e se o novo componente (202, 204, 206) mostrou ser proveniente de uma fonte confiável.

3. Método, de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que compreende a etapa de verifi-

car dados de segurança antes que os dados de identidade armazenados sejam substituídos com dados de identidade do novo componente (202, 204, 206).

4. Unidade de processamento (208) de terminal de auto-serviço (100), que compreende uma memória (214) para armazenar dados de identidade de fonte de componente, um dispositivo de solicitação (216) arranjado para solicitar dados de identidade de componentes (202, 204, 206) do terminal (100), e um dispositivo de comparação (218) arranjado para comparar dados de identidade recebidos pelo dispositivo de solicitação (216) com dados de identidade de fonte de componente armazenados na memória (214) para determinar se o componente (202, 204, 206) é proveniente de uma fonte confiável, **CARACTERIZADA** pelo fato de que a unidade de processamento (208) é arranjada para permitir que um terminal (100), como o qual é associada, opere somente se o componente (202, 204, 206), ou cada um dos componentes (202, 204, 206), for proveniente de uma fonte confiável na inicialização do terminal (100).

5. Unidade de processamento, de acordo com a reivindicação 4, **CARACTERIZADA** pelo fato de que compreende adicionalmente um dispositivo de segurança (220) arranjado para receber dados de segurança de um operador de manutenção e usar os dados de segurança para determinar se um operador de manutenção é um operador autorizado.

6. Terminal de auto-serviço (100), que compreende uma unidade de processamento (208) de terminal de auto-serviço compreendendo uma memória (214) para armazenar dados

de identidade, um dispositivo de solicitação (216) arranjado para solicitar dados de identidade de componentes (202, 204, 206) do terminal (100) e um dispositivo de comparação (218) arranjado para comparar dados de identidade recebidos pelo dispositivo de solicitação (216) com dados de identidade armazenados na memória (214) para detectar qualquer mudança nos dados de identidade, compreendendo adicionalmente pelo menos um dos seguintes componentes (202, 204, 206) com dados de identidade associados: uma plataforma de criptografia PIN, uma unidade de distribuição de dinheiro em espécie, e um leitor de cartão; o terminal (100) sendo arranjado de maneira tal que os dados de identidade associados com o componente (202, 204, 206), ou cada um dos componentes (202, 204, 206), possam ser lidos pela unidade de processamento (208), **CARACTERIZADO** pelo fato de que a unidade de processamento (208) é arranjada para determinar se cada um dos componentes (202, 204, 206) é proveniente de uma fonte confiável na inicialização do terminal (100), e para permitir que o terminal (100) opere somente se todos os componentes (202, 204, 206) forem provenientes de uma fonte confiável.

7. Terminal de auto-serviço, de acordo com a reivindicação 6, **CARACTERIZADO** pelo fato de que os dados de identidade associados com o componente (202, 204, 206), ou cada um dos componentes (202, 204, 206), são providos em uma plaqueta de circuito integrado (212).

8. Terminal de auto-serviço, de acordo com a reivindicação 6, **CARACTERIZADO** pelo fato de que é um caixa eletrônico automatizado (ATM) (100).

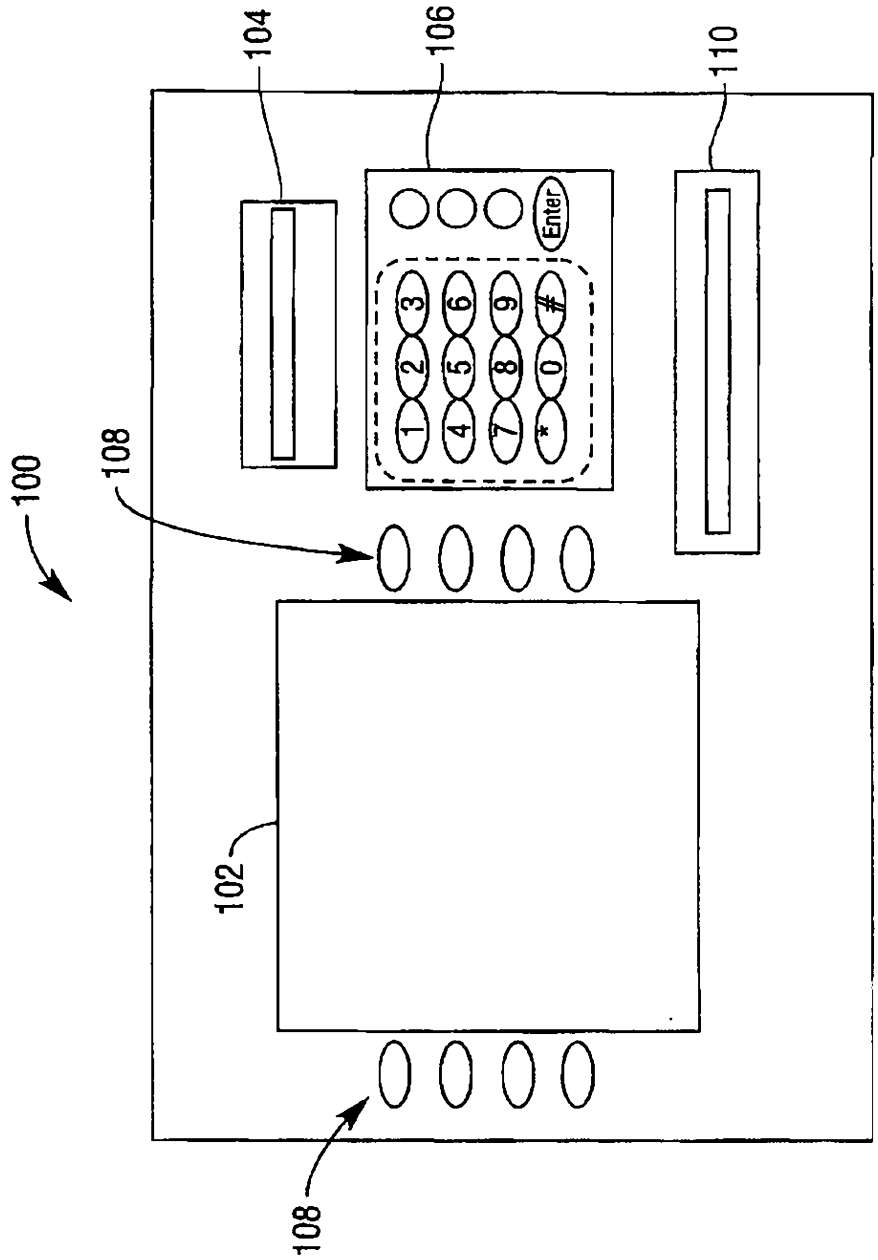


FIG. 1

FIG. 2

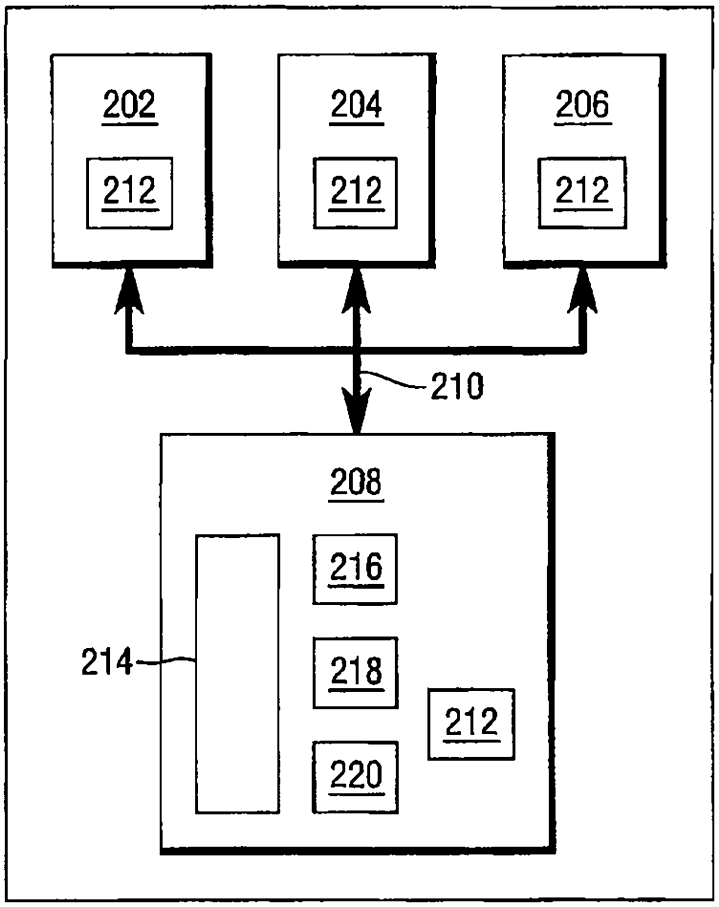
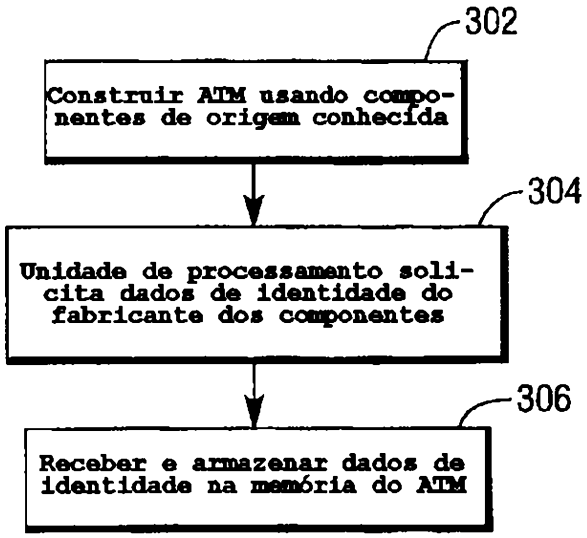


FIG. 3


302
Construir ATM usando componentes de origem conhecida
304
Unidade de processamento solicita dados de identidade do fabricante dos componentes
306
Receber e armazenar dados de identidade na memória do ATM

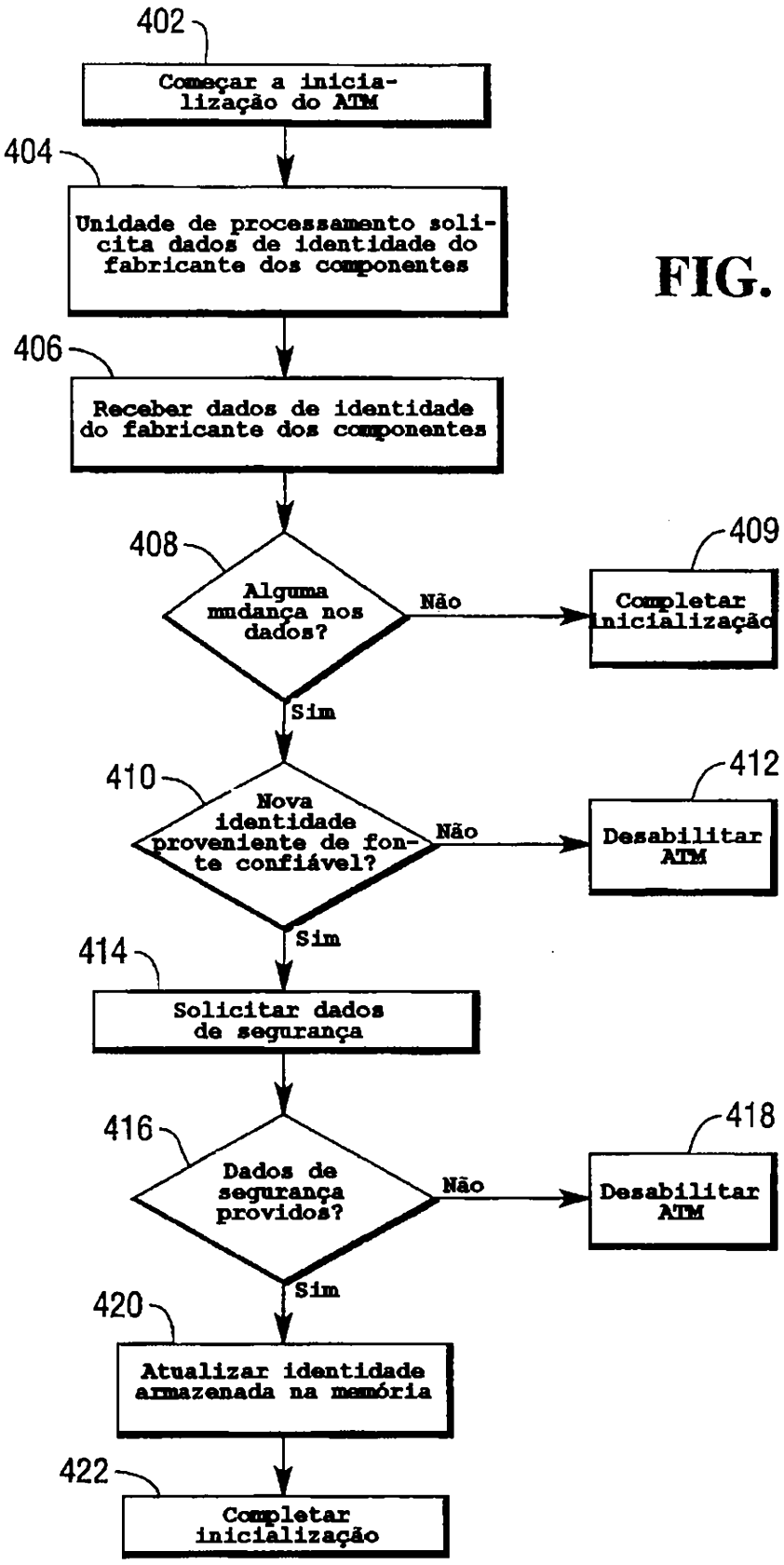

402
Começar a inicialização do ATM
404
Unidade de processamento solicita dados de identidade do fabricante dos componentes
406
Receber dados de identidade do fabricante dos componentes
408
Alguma mudança nos dados?
Não
409
Completar inicialização
Sim
410
Nova identidade proveniente de fonte confiável?
Não
412
Desabilitar ATM
Sim
414
Solicitar dados de segurança
416
Dados de segurança providos?
Não
418
Desabilitar ATM
Sim
420
Atualizar identidade armazenada na memória
422
Completar inicialização

FIG. 4

RESUMO

"MÉTODO PARA VALIDAR COMPONENTES DE MÁQUINA EM UM TERMINAL DE AUTO-SERVIÇO, UNIDADE DE PROCESSAMENTO DE TERMINAL DE AUTO-SERVIÇO E TERMINAL DE AUTO-SERVIÇO"

É descrito um método para validar componentes de máquina em um terminal de auto-serviço que compreende prover pelo menos um componente de máquina com um identificador legível por máquina e ler dados de identidade provenientes do identificador legível por máquina usando uma unidade de processamento. Os dados de identidade são comparados com dados de identidade armazenados na memória da unidade de processamento para determinar se a identidade de um componente mudou. Se a identidade mudou, a unidade de processamento compara os dados de identidade com dados de origem para determinar se o componente é proveniente de uma fonte confiável. Em uma modalidade, o terminal de auto-serviço é um ATM e os componentes são uma plataforma de criptografia de Número de Identificação Pessoal (PIN), uma unidade de distribuição de dinheiro em espécie e um leitor de cartão.