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

(11) BR 112016005345-1 B1

(22) Data do Depósito: 01/07/2014

(45) Data de Concessão: 28/06/2022

(54) Título: DISPOSITIVO DE COMUNICAÇÃO MÓVEL, E, MÉTODO PARA OPERAR UM DISPOSITIVO DE COMUNICAÇÃO MÓVEL

(51) Int.Cl.: G06F 9/455.

(30) Prioridade Unionista: 12/09/2013 US 14/025,556.

(73) Titular(es): THE BOEING COMPANY.

(72) Inventor(es): ALLON J. STERN; JOHN HALEY.

(86) Pedido PCT: PCT US2014045017 de 01/07/2014

(87) Publicação PCT: WO 2015/038219 de 19/03/2015

(85) Data do Início da Fase Nacional: 10/03/2016

(57) Resumo: DISPOSITIVO DE COMUNICAÇÃO MÓVEL, E, MÉTODO PARA OPERAR UM DISPOSITIVO DE COMUNICAÇÃO MÓVEL. É provido um dispositivo de comunicação móvel. O dispositivo de comunicação móvel inclui um primeiro módulo de plataforma confiável, um segundo módulo de plataforma confiável, um processador e um meio de armazenamento. O meio de armazenamento inclui instruções que fazem com que o processador estabeleça uma raiz de confiança para uma primeira persona e uma segunda persona, em que a primeira persona inclui um primeiro sistema operacional e um primeiro ambiente de execução confiável, e a segunda persona inclui um segundo sistema operacional e um segundo ambiente de execução confiável. As instruções também fazem com que o processador armazene medições definindo a raiz de confiança para a primeira persona no primeiro módulo de plataforma confiável, armazene medições definindo a raiz de confiança para a segunda persona no segundo módulo de plataforma confiável e carregue a primeira persona e a segunda persona usando as raízes de confiança para as primeira e segunda personas.

“DISPOSITIVO DE COMUNICAÇÃO MÓVEL, E, MÉTODO PARA OPERAR UM DISPOSITIVO DE COMUNICAÇÃO MÓVEL”

FUNDAMENTOS

[001] O campo da presente descrição refere-se em geral a dispositivos de comunicação móveis e, mais especificamente, a um dispositivo de comunicação móvel que habilita a operação confiável de um ou mais sistemas operacionais isolados, virtualizados, executados nele.

[002] Dispositivos de comunicação móveis tais como telefones inteligentes, telefones celulares e assistentes digitais pessoais (PDAs) têm crescido em uso e popularidade dentre uma variedade de tipos de usuários diferentes. Pelo menos alguns dispositivos conhecidos incluem uma Unidade de Processamento Central (CPU) que pode ser virtualizada para executar simultaneamente sistemas operacionais múltiplos (OSs) em um dispositivo. Por exemplo, um programa de software conhecido como um hipervisor pode ser usado para separar os diferentes OSs, gerenciando operações de acesso de entrada/entrada (I/O) transmitidas entre os OSs e dispositivos de hardware incluídos no sistema de computador. Mais especificamente, o hipervisor facilita a separação de hardware básico, tal como a CPU e periféricos associados (por exemplo, dispositivos de visualização, telas de toque e interfaces de comunicações) dos OSs que "rodam" no hardware.

[003] Embora a virtualização do dispositivo possa facilitar a separação de um conjunto de software de outro conjunto de software em dispositivos de computação conhecidos, a plataforma básica pode ser suscetível a uma variedade de vulnerabilidades de segurança. Devido a isto, tem se tornado crescentemente importante para aqueles na indústria de computador, para aumentar a segurança de dispositivos de computação conhecidos. Deste modo, pode ser desejável incorporar segurança reforçada a uma arquitetura de virtualização de dispositivo.

BREVE DESCRIÇÃO

[004] Em um aspecto, é provido um dispositivo de comunicação móvel. O dispositivo de comunicação móvel inclui um primeiro módulo de plataforma confiável, um segundo módulo de plataforma confiável, um processador e um meio de armazenamento. O meio de armazenamento inclui instruções que fazem com que o processador estabeleça uma raiz de confiança para uma primeira *persona* e uma segunda *persona*, em que a primeira *persona* inclui um primeiro sistema operacional e um primeiro ambiente de execução confiável, e a segunda *persona* inclui um segundo sistema operacional e um segundo ambiente de execução confiável. As instruções também fazem com que o processador armazene medições definindo a raiz de confiança para a primeira *persona* no módulo de plataforma confiável, armazene medições definindo a raiz de confiança para a segunda *persona* no segundo módulo de plataforma confiável e carregue a primeira *persona* e a segunda *persona* usando as raízes de confiança para a primeira e segunda *persona*s.

[005] Em um outro aspecto, é provido um método para operar um dispositivo de comunicação móvel. O método inclui estabelecer uma raiz de confiança para uma primeira *persona* e uma segunda *persona*, onde a primeira *persona* inclui um primeiro sistema operacional e um primeiro ambiente de execução confiável e a segunda *persona* inclui um segundo sistema operacional e um segundo ambiente de execução confiável. O método também inclui armazenar medições definindo a raiz de confiança para a primeira *persona* no primeiro módulo de plataforma confiável, armazenar medições definindo a raiz de confiança para a segunda *persona* no segundo módulo de plataforma confiável e carregar a primeira *persona* e a segunda *persona* usando as raízes de confiança para a primeira e segunda *persona*s.

[006] Em um outro aspecto, é provido um meio legível por computador não transitório armazenando instruções legíveis por computador para operar um dispositivo de comunicação móvel. O dispositivo de

comunicação móvel inclui um processador, um primeiro módulo de plataforma confiável e um segundo módulo de plataforma confiável. As instruções executáveis por computador fazem com que o processador estabeleça uma raiz de confiança para uma primeira *persona* e uma segunda *persona*, onde a primeira *persona* inclui um primeiro sistema operacional e um primeiro ambiente de execução confiável e a segunda *persona* inclui um segundo sistema operacional e um segundo ambiente de execução confiável. As instruções executáveis por computador também fazem com que o processador armazene medições definindo a raiz de confiança para a primeira *persona* no primeiro módulo de plataforma confiável, armazene medições definindo a raiz de confiança para a segunda *persona* no segundo módulo de plataforma confiável e carregue a primeira *persona* e a segunda *persona* usando as raízes de confiança para a primeira e segunda *persona*s.

BREVE DESCRIÇÃO DOS DESENHOS

[007] Figura 1 é uma vista em perspectiva frontal de um exemplo de um dispositivo de comunicação móvel.

[008] Figura 2 é uma vista em perspectiva posterior do dispositivo de comunicação móvel mostrado na Figura 1.

[009] Figura 3 é uma ilustração esquemática de um exemplo de arquitetura de hardware que pode ser usado com o dispositivo de comunicação móvel mostrado na Figura 1.

[0010] Figura 4 é uma ilustração esquemática de um exemplo de arquitetura de software que pode ser usado no dispositivo de comunicação móvel mostrado na Figura 1.

[0011] Figura 5 é um fluxograma de um exemplo de método para reivindicar a propriedade de uma *persona* que pode ser usada com o dispositivo de comunicação móvel mostrado na Figura 1.

[0012] Figura 6 é uma ilustração esquemática de um exemplo de sistema para uso ao autorizar uma operação a ser realizada no dispositivo de

comunicação móvel mostrado na Figura 1.

[0013] Figura 7 é um fluxograma de um exemplo de método para atualizar software de *persona* que pode ser usado com o dispositivo de comunicação móvel mostrado na Figura 1.

[0014] Figura 8 é um fluxograma de um exemplo de método para transição de propriedade de uma *persona* que pode ser usado com o dispositivo de comunicação móvel mostrado na Figura 1.

[0015] Figura 9 é um fluxograma de um exemplo de método para carregar uma nova *persona* que pode ser usado com o dispositivo de comunicação móvel mostrado na Figura 1.

DESCRIÇÃO DETALHADA

[0016] Os sistemas e métodos aqui descritos podem ser usados para operar um dispositivo de comunicação móvel. No exemplo de implementação, o dispositivo de comunicação móvel é gerenciado por uma arquitetura de hardware e software que usa criptografia, tal como criptografia baseada em códigos públicos e privados, para facilitar a operação segura de sistemas executados nele. Mais especificamente, o dispositivo de comunicação móvel suporta sistemas operacionais virtualizados múltiplos que "rodam" simultaneamente no dispositivo e cada um apresenta raízes de confiança separadas. Deste modo, o acesso dos sistemas operacionais virtualizados ao hardware no dispositivo é forçado por determinadas políticas de segurança para habilitar a operação confiável do dispositivo.

[0017] Figuras 1 e 2 ilustram um exemplo de dispositivo de comunicação móvel 10. No exemplo de implementação, o dispositivo de comunicação móvel 10 é provido para suportar comunicação de voz com outro dispositivo, tal como um outro dispositivo de comunicação móvel. Ainda mais, o dispositivo de comunicação móvel 10 pode incluir uma variedade de outras funcionalidades, incluindo acesso de rede, gerar mensagens SMS, hospedagem de uma ou mais aplicações, processamento de

dados, criptografia e/ou outras funções. O dispositivo de comunicação móvel 10 pode ser um telefone inteligente, configurado para se comunicar através de uma ou mais redes celulares. Em uma implementação alternativa, o dispositivo de comunicação móvel 10 pode operar exclusivamente através de uma rede não celular tal como uma rede via satélite e/ou WiFi.

[0018] Conforme mostrado, o dispositivo de comunicação móvel 10 inclui um invólucro 12 e dispositivos de apresentação múltiplos 14 dispostos pelo menos parcialmente no invólucro 12. O dispositivo de apresentação 14 emite informação tal como, porém, não limitado a dados relacionados a operação do dispositivo de comunicação móvel 10, comandos, dados requisitados, mensagens, um ou mais dispositivos de entrada (tais como um teclado virtual), e/ou qualquer outro tipo de dados para um usuário. Em vários exemplos, o dispositivo de apresentação 14 pode incluir, por exemplo, um visor de cristal líquido (LCD), um visor de diodo emissor de luz (LED), um diodo emissor de luz (LED), um flash de câmera, um visor de diodo emissor de luz orgânico (OLED) e/ou um visor de "tinta eletrônica". Em algumas implementações, dispositivos de apresentação múltiplos 14 podem ser incluídos para apresentar dados a um usuário visualmente e/ou audivelmente. No exemplo de implementação, o dispositivo de apresentação 14 inclui uma saída de áudio para uso em comunicação de voz.

[0019] O dispositivo de comunicação móvel 10 inclui adicionalmente dispositivos de entrada múltiplos 16 dispostos pelo menos parcialmente dentro do invólucro 12. Cada dispositivo de entrada 16 pode ser configurado para receber seleções, requisições, comandos, dados de informação e/ou qualquer outro tipo de entradas, de acordo com um ou mais dos métodos e/ou processos aqui descritos. Os dispositivos de entrada 16 incluem, por exemplo, botões, um teclado, um microfone, uma vibração, um dispositivo apontador, uma caneta, um painel sensível ao toque (por exemplo, uma almofada de toque ou uma tela de toque), um giroscópio, um acelerômetro, um compasso

digital, um detector de posição, uma câmera, uma segunda câmera, um sensor de luz ambiente e/ou uma interface de entrada de áudio. No exemplo de implementação, um único componente, tal como uma tela de toque 18 funciona ambos como dispositivo de apresentação 14 e dispositivo de entrada 16.

[0020] Em uma implementação, o dispositivo de comunicação móvel 10 inclui recursos de segurança que facilitam a operação segura do dispositivo de comunicação móvel 10. Recursos de segurança incluem um dispositivo de entrada 16, tal como um botão de segurança 17 e um dispositivo de apresentação 14 tal como uma pluralidade de LEDs. Mais especificamente, o dispositivo de comunicação móvel 10 inclui um primeiro LED 19 e um segundo LED 21. Como será descrito em mais detalhe abaixo, os recursos de segurança podem ser usados para alterar e/ou verificar um estado operacional, confiável do dispositivo de comunicação móvel 10. Em uma implementação alternativa, o dispositivo de comunicação móvel 10 pode incluir qualquer tipo e/ou número de dispositivos de apresentação que habilitam os recursos de segurança a funcionar conforme descrito aqui.

[0021] O dispositivo de comunicação móvel 10 inclui um painel traseiro 20 encaixado com o invólucro 12. O painel traseiro 20 define uma seção transversal substancialmente consistente com o invólucro 12, formando deste modo uma unidade substancialmente integrada ao invólucro 12 quando acoplada a ele. O painel traseiro 20 é removível do dispositivo de comunicação móvel 10 para prover acesso a um ou mais aspectos do dispositivo de comunicação móvel 10.

[0022] Figura 3 é uma ilustração esquemática de um exemplo de arquitetura de hardware que pode ser usado com o dispositivo de comunicação móvel 10 (mostrado na Figura 1). No exemplo de implementação, o dispositivo de comunicação móvel 10 inclui uma memória 22 e um processador 24 acoplado à memória 22 para executar instruções

programadas. O processador 24 pode incluir uma ou mais unidades de processamento (por exemplo, em uma configuração multi núcleo) e/ou incluir um acelerador criptográfico (não mostrado). O dispositivo de comunicação móvel 10 é programável para executar uma ou mais operações aqui descritas, programando a memória 22 e/ou processador 24. Por exemplo, o processador 24 pode ser programado codificando uma operação como instruções executáveis e provendo as instruções executáveis à memória 22.

[0023] O processador 24 pode incluir, porém não está limitado a uma unidade de processamento central (CPU), um micro controlador, um processador de computador de conjunto de instrução reduzido (RISC), uma plataforma de aplicação de mídia aberta (OMAP), um circuito integrado específico da aplicação (ASIC), um circuito lógico programável (PLC) e/ou outros circuitos ou processadores capazes de executar as funções aqui descritas. Os métodos descritos aqui podem ser codificados como instruções executáveis realizadas em um meio legível por computador incluindo, sem limitação, um dispositivo de armazenamento e/ou um dispositivo de memória. Tais instruções, quando executadas pelo processador 24, fazem com que o processador 24 executa pelo menos uma porção das funções aqui descritas. Os exemplos acima são apenas típicos, e então não são destinados a limitar de modo algum a definição e/ou significado do termo processador.

[0024] A memória 22, conforme descrito aqui, consiste de um ou mais dispositivos que habilitam informação, tal como instruções executáveis e/ou outros dados a serem armazenados e recuperados. A memória 22 pode incluir um ou mais meios legíveis por computador tais como, sem limitação, memória de acesso randômico dinâmica (DRAM), memória de acesso randômico dinâmico síncrono (SDRAM), memória de acesso randômico estática (SRAM), um disco de estado sólido e/ou um disco rígido. A memória 22 pode ser configurada para armazenar, sem limitação, instruções executáveis, sistemas operacionais, aplicações, recursos, *scripts* de instalação

e/ou qualquer outro tipo de dados adequados para uso com os métodos e sistemas aqui descritos.

[0025] Instruções para sistemas e aplicações operacionais estão localizadas de uma forma funcional na memória 22 não transitória para execução pelo processador 24, para realizar um ou mais dos processos aqui descritos. Estas instruções nas diferentes implementações, podem ser realizadas em diferentes meios legíveis por computador físicos ou tangíveis, tais como a memória 22 ou outra memória, tal como meios legíveis por computador 26, que podem incluir, sem limitação, um controlador *flash* e/ou controlador *thumb*. Adicionalmente, instruções são localizadas de uma forma funcional nos meios legíveis por computador 26 não transitórios, que podem incluir, sem limitação, memória de mídia inteligente (SM), memória *flash* compacta (CF) memória digital segura (SD), memória de bastão de memória (MS), memória de cartão multimídia (MMC), memória de cartão multimídia embutido (e-MMC) e de micro controlador. Os meios legíveis por computador 26 podem ser inseríveis seletivamente e/ou removíveis do dispositivo de comunicação móvel 10 para permitir acesso e/ou execução pelo processador 24. Em algumas implementações, os meios legíveis por computador 26 não são removíveis.

[0026] Referindo-se novamente à Figura 3, o dispositivo de comunicação móvel 10 pode incluir um componente GPS 30, que é configurado para prover dados de localização ao processador 24. Os dados de localização permitem que o processador 24 determine a localização do dispositivo de comunicação móvel 10 e/ou proveja funcionalidade, dependendo da localização do dispositivo de comunicação móvel 10, tal como, por exemplo, funcionalidade de navegação. Em uma implementação alternativa, dados de localização podem ser obtidos para o dispositivo de comunicação móvel 10, usando uma rede celular, identificando estações base ou dispositivos 802.11 e/ou Bluetooth próximas, e/ou uma combinação destas.

[0027] Em algumas implementações, o dispositivo de comunicação móvel 10 inclui adicionalmente pelo menos um cripto-processador. Mais especificamente, o dispositivo de comunicação móvel 10 inclui um primeiro módulo de plataforma confiável (TPM) 60 e segundo TPM 62. Os TPMs criptografam pelo menos uma porção de dados acessados pelo processador 24 para comunicação para/a partir do dispositivo de comunicação móvel 10 e/ou para armazenamento nele. Consequentemente, alguns dados podem ser segregados de outras aplicações e/ou operações do dispositivo de comunicação móvel 10, e mantidos a um nível mais alto de segurança do que tais aplicações/operações. Deste modo, os TPMs 60 e 62 facilitam habilitar inicialização confiável, inicialização medida, inicialização segura, comprovação remota e armazenamento de códigos protegidos, por exemplo.

[0028] Adicionalmente, o dispositivo de comunicação móvel inclui um elemento seguro 64 acoplado ao processador 24. Mais especificamente, o elemento seguro 64 pode ser integrado ao dispositivo de comunicação móvel 10 como pelo menos um dentre um cartão de circuito integrado universal (UICC), um cartão microSD, e/ou embutido dentro do dispositivo de comunicação móvel 10. O elemento seguro 64 é um ambiente de armazenamento e execução resistente a intrusões que pode ser usado como um dispositivo de armazenamento de código e/ou âncora confiável de hardware para uma plataforma em execução no dispositivo de comunicação móvel 10. Mais especificamente, o elemento seguro 64 armazena códigos de criptografia de dados, chave de acessos e informações de configuração de hardware e software. Adicionalmente, o elemento seguro 64 gera pares de código público e facilita restringir a exportação de códigos privados associados. Em uma implementação alternativa, o elemento seguro 64 pode ser implementado como um TPM.

[0029] O dispositivo de comunicação móvel 10 também inclui uma memória supervisora de segurança 66. A memória supervisora de segurança

66 armazena dados reativos a intrusões que podem incluir uma pluralidade de códigos, e podem ser usados para acondicionar dados dentro do elemento seguro 64 e/ou primeiro TPM 60 ou segundo TPM 62. Em operação, os dados reativos à intrusão podem ser apagados de tal modo que os dados acondicionados não podem ser recuperados na detecção de um evento de intrusão. A memória supervisora de segurança 66 pode manter qualquer quantidade de dados reativos a intrusão que habilite o dispositivo de comunicação móvel 10 a funcionar conforme descrito aqui.

[0030] O dispositivo de comunicação móvel 10 inclui adicionalmente um controlador de celular 31 acoplado ao processador 24. O controlador de celular 31 permite que o dispositivo de comunicação móvel 10 se comunique com uma ou mais redes celulares (não mostradas) para prover comunicação de voz e/ou dados com a rede celular. Neste exemplo, o dispositivo de comunicação móvel 10 inclui dois soquetes 33A e 33B de cartão de módulo de identidade de assinante (SIM) acoplados ao controlador de celular 31. Desta maneira, o dispositivo de comunicação móvel 10 é capaz de receber dois cartões SIM associados a duas contas de celular diferentes, selecionáveis por um usuário do dispositivo de comunicação móvel 10. Por exemplo, o dispositivo de comunicação móvel 10 pode acessar uma conta de celular pessoal e uma conta de celular de negócios, permitindo que o usuário selecione entre elas para separar o uso pessoal e o uso comercial. Deveria ser verificado que um número diferente de soquetes de cartão SIM pode ser incluído em outras implementações.

[0031] Adicionalmente, o dispositivo de comunicação móvel 10 inclui um controlador USB 35 acoplado ao processador 24. Conforme mostrado na Figura 3, o controlador USB 35 é acessível através do conector 37. Desta maneira, um ou mais dispositivos diferentes podem se comunicar com o dispositivo de comunicação móvel 10. Similarmente, o dispositivo de comunicação móvel 10 inclui adicionalmente um controlador 39 de interface

multimídia de alta definição (HDMI) acoplado a um processador 24 e acessível através de um conector 41. Em pelo menos uma implementação, os conectores 37 e/ou 41 podem prover conexões micro-USB e/ou micro-HDMI ao dispositivo de comunicação móvel 10.

[0032] Adicionalmente ou alternativamente, o dispositivo de comunicação móvel 10 pode incluir um ou mais dentre um controlador Bluetooth, um controlador ZigBee e/ou um controlador WiFi para prover um ou mais canais de comunicação sem fio. Embora o componente GPS 30, primeiro TPM 60, segundo TPM 62 e controlador de celular 31 sejam providos pelo menos parcialmente em hardware, deveria ser adicionalmente verificado que um ou mais componentes integrados no dispositivo de comunicação móvel 10 podem ser providos através de software e/ou firmware associados ao processador 24. Em um exemplo, o processador 24 provê uma barreira de segurança de interface aérea, configurada para analisar protocolos de interface aérea de nível baixo do dispositivo de comunicação móvel 10 e permitir ou negar transmissões de rede baseadas em identidades e características de rede aprovadas. Neste exemplo, os dados do protocolo aéreo a partir do controlador de celular 31, contendo identidades e características de rede celular são providos ao processador 24 e analisados pelo processador 24 para determinar se o dispositivo de comunicação móvel 10 deveria ter permissão para conduzir transmissões de rede via redes celulares identificadas pelo controlador de celular 31. Neste exemplo, o nível de análise provido adiciona segurança de rede ao dispositivo de comunicação móvel 10 tendo o processador 24 autenticado adicionalmente as conexões de rede do controlador de celular 31, além de usar mecanismos de autenticação de protocolo de rede celular padrão do controlador de celular 31 por si próprios. Deveria ser notado que outros componentes da interface aérea do dispositivo de comunicação móvel 10 tais como, por exemplo, um controlador Bluetooth e/ou um controlador WiFi, podem também ser monitorados pela barreira de

segurança da interface de rádio enlace. Em uma implementação alternativa, o primeiro TPM 60 e o segundo TPM 62 podem ser implementados em software.

[0033] Deveria ser verificado que outras implementações de dispositivo de comunicação móvel podem incluir mais ou menos componentes integrados ou externos ao processador 24.

[0034] Figura 4 é uma ilustração esquemática de um exemplo de arquitetura de software 100 que pode ser usado com o dispositivo de comunicação móvel 10 (mostrado na Figura 1). No exemplo de implementação, a arquitetura de software 100 inclui um sistema operacional 104 instalado sobre um hardware de plataforma 102 que inclui o processador 24 e a memória 22. O hardware de plataforma 102 inclui os componentes do dispositivo de comunicação móvel 10 descritos acima. A arquitetura de software 100 também inclui uma camada de software de virtualização, tal como um hipervisor 106, que é executado no topo do sistema operacional 104 (isto é, um hipervisor do tipo 2) e um supervisor de segurança 108 acoplado em comunicação com o hipervisor 106. Em uma implementação alternativa, o hipervisor 106 pode ser instalado e operar no hardware de plataforma 102 (isto é, um hipervisor do tipo 1). O hipervisor 106 suporta uma pluralidade de espaços de execução de máquina virtual de tal modo que uma pluralidade de máquinas virtuais pode ser simultaneamente instanciada e executada.

[0035] O hipervisor 106 virtualiza uma primeira *persona* 110 e uma segunda *persona* 120 que pode ser executada e "rodar" no topo do hipervisor 106. A primeira *persona* 110 inclui um primeiro sistema operacional de *persona* (OS) 112 e um primeiro ambiente de execução confiável (TEE) 114 e a segunda *persona* 120 inclui um segundo sistema operacional de *persona* 122 e um segundo ambiente de execução confiável 124.

[0036] A primeira *persona* 110 e a segunda *persona* 120 possuem, cada uma, uma âncora de confiança definida que pode ser usada para validar

confiança e autorizar ações executadas por cada *persona*. Mais especificamente, a primeira *persona* 110 possui uma primeira âncora de confiança e uma segunda *persona* 120 possui uma segunda âncora de confiança que é separada da primeira âncora de confiança. Conforme usado aqui, o termo "âncora de confiança" refere-se a um ou mais códigos de criptografia secretos (isto é, um certificado criptográfico) que define o proprietário da *persona* e que pode ser usado para assinar ativos de *persona*. Inversamente, conforme usado aqui, os termos "proprietário" e/ou "propriedade" refere-se a uma pessoa ou entidade que possui controle administrativo sobre uma *persona*, mantendo a âncora de confiança. Em algumas implementações, o certificado raiz da âncora de confiança pode ser usado para assinar uma autoridade de certificado intermediária que assina os ativos do pacote da *persona*.

[0037] Cada âncora de confiança segue de volta até uma autoridade de certificado raiz, que pode ser uma organização de empreendimento e/ou pode ser definida de uma maneira leve para um único usuário em um computador de mesa. Deste modo, os recursos da primeira *persona* 110 podem ser mantidos separados da segunda *persona* 120, e políticas de acesso que tenham sido acordadas e assinadas por cada âncora de confiança podem ser reforçadas. A autoridade de certificado raiz pode ser armazenada off-line e em uma localização segura. Adicionalmente, a âncora de confiança pode incluir diversas autoridades de certificado intermediário apresentando capacidades definidas especificamente. Exemplos de capacidades incluem, porém não estão limitados ao direito de definir um sistema operacional, direito de definir um TEE, o direito de definir políticas de segurança, o direito de definir outras autoridades de certificados intermediários e/ou certificados de usuário, capacidades de cópia de segurança, política de cópia de segurança, a habilidade de atualizar um sistema operacional, a habilidade de atualizar um TEE, funcionalidade de gerenciamento de dispositivo móvel (MDM) e

importação ou exportação de código.

[0038] O software confiável da primeira *persona* 110 e da segunda *persona* 120 é executado, cada um em um contexto que é isolado do outro, sob condições padrão. Mais especificamente, conforme descrito acima, o hipervisor 106 facilita separar e isolar o primeiro TEE 114 e o segundo TEE 124 um do outro. Deste modo, cada *persona* não será afetada por outros sistemas operacionais em execução no dispositivo de comunicação móvel 10. Adicionalmente, a primeira *persona* 110 e a segunda *persona* 120 podem ser configuradas para estabelecer confiança mútua entre o primeiro TEE 114 e o segundo TEE 124. Estabelecer tal confiança mútua habilita a formação de um caminho de comunicação confiável entre a primeira *persona* 110 e a segunda *persona* 120. A comunicação entre o primeiro TEE 114 e o segundo TEE 124 pode somente ser permitida por acordo mútuo nas políticas de segurança da primeira *persona* 110 e da segunda *persona* 120. Adicionalmente, uma guarda de alta garantia (não mostrada) pode ser implementada para facilitar a restrição de um fluxo de dados entre a primeira *persona* 110 e a segunda *persona* 120. Por exemplo, a guarda de alta garantia pode facilitar a restrição do fluxo dos dados sensíveis e/ou classificados entre a primeira *persona* 110 e a segunda *persona* 120, enquanto permite o fluxo de dados não classificados entre elas.

[0039] Embora a primeira *persona* 110 e os elementos desta sejam descritos em detalhe adicional abaixo, deveria ser entendido que a mesma descrição pode se aplicar à segunda *persona* 120 e aos elementos desta. No exemplo de implementação, o primeiro OS de *persona* 112 está em um ambiente de execução possuindo recursos e controladores de dispositivo virtual que habilitam a execução de um sistema operacional pleno. Um exemplo de sistema operacional pleno pode incluir, porém não está limitado a um sistema operacional de Projeto de Fonte Aberta Android® (AOSP). O primeiro OS de *persona* 112 pode incluir uma biblioteca que habilita o

primeiro OS de *persona* 112 a se comunicar com o primeiro TEE 114. Adicionalmente, uma pluralidade de aplicações 130 pode ser requerida de uma fonte externa (não mostrada) e executada no topo do primeiro OS de *persona* 112.

[0040] O primeiro TEE 114 é um ambiente de execução leve que é separado do e está em comunicação com o primeiro OS de *persona* 112. O primeiro TEE 114 é um ambiente seguro que provê uma área que pode ser usada para armazenar dados sensíveis e executar aplicações sensíveis. Em implementações alternativas, o primeiro TEE 114 pode ser um ambiente de execução possuindo recursos e controladores de dispositivo virtual que habilitam a execução de um sistema operacional pleno e/ou podem ser executados em uma peça separada de hardware. Adicionalmente, a primeira *persona* 110 pode incluir mais de um ambiente de execução confiável.

[0041] O primeiro TEE 114 tem acesso direto a uma interface de módulo de identidade de assinante (SIM) ISO7816 e/ou TPM. Mais especificamente, o primeiro TPM 60 (mostrado na Figura 3) é designado à primeira *persona* 110, e o segundo TPM 62 (mostrado na Figura 3) é designado à segunda *persona* 120. Como tal, o primeiro TPM 60 pode ser usado como uma âncora de confiança de hardware para um proprietário de uma primeira *persona* 110 e o segundo TPM 62 pode ser usado como uma âncora de confiança de hardware para um proprietário da segunda *persona* 120. Adicionalmente, o primeiro TEE 114 tem acesso direto ao primeiro TPM 60 e aos serviços de ambiente de execução confiáveis tais como autenticação, acesso o armazenamento de código, configuração de rede privada virtual (VPN) e/ou software de protocolo de voz sobre IP (VoIP), por exemplo. Isolar tais caminhos de dados sensíveis dentro do primeiro TEE 114 e afastados do primeiro OS de *persona* 112 facilita assegurar a operação confiável do dispositivo de comunicação móvel 10, enquanto mantém controle dos

serviços TEE com o proprietário da *persona*. Adicionalmente, permitir que o primeiro TEE 114 controle o primeiro TPM 60 facilita isolar a informação sensível do primeiro OS de *persona* 112, de tal modo que a informação está em um ambiente mais seguro protegido.

[0042] Adicionalmente, o primeiro TEE 114 pode ter acesso a serviços criptográficos, de tal modo que operações criptográficas podem ser realizadas em benefício do primeiro OS de *persona* 112, sem expô-lo a um código de texto simples. Mais especificamente, o primeiro TEE 114 pode usar módulos de criptografia em um primeiro TPM 60, que habilitam criptografia acelerada de hardware não certificado, criptografia certificada suíte B e/ou FIPS-140-2. O dispositivo de comunicação móvel 10 pode também incluir um módulo VPN e/ou um módulo VoIP. O módulo VPN habilita a primeira *persona* 110 a autenticar um VPN e se comunicar com criptografia sem autenticação ou códigos de criptografia sendo visíveis ao código não confiável. Adicionalmente, o módulo VoIP habilita a primeira *persona* 110 a estabelecer e autenticar uma chamada VoIP e se comunicar com criptografia sem autenticação ou códigos de criptografia sendo visíveis a código não confiável.

[0043] A confiança do primeiro OS de *persona* 112 e do segundo OS de *persona* 122 é definida pela integridade de uma imagem de inicialização de cada *persona* carregada pelo hardware de plataforma 102. Por exemplo, a confiança do primeiro TEE 114 é definida pela integridade de sua imagem estática, quando carregada pelo hardware de plataforma 102, com será descrito em mais detalhe abaixo. Mais especificamente, o código carregado no primeiro TEE 114 é validado em uma âncora de confiança durante o carregamento, e a imagem é imutável uma vez que esteja carregada. Como a imagem é imutável, o primeiro TEE 114 pode ser somente alterado carregando uma nova imagem assinada através do primeiro TEE 114. Adicionalmente, o primeiro OS de *persona* 112 e o segundo OS de *persona*

122 pode usar recursos fora de seu próprio ambiente de execução para gerenciar sua integridade. Por exemplo, o carregamento dos sistemas operacionais pode ser criptografado e validado e o acesso dos sistemas operacionais a recursos de hardware pode ser limitado e reforçado através de configurações fora de seu controle.

[0044] A arquitetura de software 100 também inclui um carregador de inicialização primário 140 que carrega o sistema operacional 104, um primeiro carregador de inicialização secundário 142 que carrega o primeiro OS de *persona* 112 e um segundo carregador de inicialização secundário 144 que carrega o segundo OS de *persona* 122. No exemplo de implementação, o dispositivo de comunicação móvel 10 usa um processador que facilita o estabelecimento da confiança de plataforma durante o processo de inicialização. Mais especificamente, o processador habilita a validação de assinatura dos carregadores de inicialização para facilitar o estabelecimento de confiança durante o carregamento de cada sistema operacional. Por exemplo, o dispositivo de comunicação móvel 10 usa uma combinação de valores de sinal numérico (*hash*) e validação de assinatura de tal modo que uma cadeia de confiança permanece intacta à medida que se estende da plataforma de hardware 102 para a primeira *persona* 110 e segunda *persona* 120.

[0045] Em operação, o processador 24 carrega carregador de inicialização primário 140 se este for digitalmente assinado por uma raiz de confiança do fabricante do dispositivo. Conforme usado aqui, o termo "raiz de confiança do fabricante do dispositivo" refere-se a um ou mais códigos de criptografia secretos (isto é, um certificado criptográfico) usados por um fabricante do dispositivo para assinar ativos que vem instalados no dispositivo de comunicação móvel 10. A cadeia de confiança continua intacta através do hipervisor 106, para facilitar o estabelecimento de ambiente de execução isolados, validar componentes dentro do dispositivo de comunicação móvel

10 e/ou armazenar medições nos módulos de plataforma confiável para uso posterior pelo código de usuário para se vincular ao estado confiável.

[0046] O controle do primeiro TPM 60 é transferido para a primeira *persona* 110 e o controle do segundo TPM 62 é transferido para a segunda *persona* 120, de tal modo que os aspectos de inicialização medidos dos TPMs 60 e 62 podem ser usados pela primeira *persona* 110 e segunda *persona* 120. Mais especificamente, os TPMs 60 e 62 são inicializados pelo software de inicialização confiável do dispositivo de comunicação móvel 10, e o controle é então transferido para cada *persona* para seu uso exclusivo, depois das *personas* terem sido carregadas. Se uma *persona* usa um TPM para inicialização confiável, então as alterações de hardware e/ou software podem resultar na incapacidade de recuperar códigos que tenham sido vinculados às configurações originais, de tal modo que a *persona* pode não ser reinicializada sem reinicialização do dispositivo inteiro.

[0047] Durante o processo de inicialização, os TPMs medem (isto é, *hash*) os componentes críticos de software e firmware usados dentro do dispositivo de comunicação móvel 10. Por exemplo, uma raiz de confiança para medição pode ser estabelecida quando as medições para o carregador de inicialização primário 140, sistema operacional 104, hipervisor 106, supervisor de segurança 108, carregador de inicialização 142 e primeiro OS de *persona* 112 são estendidos no primeiro TPM 60. As medições podem ser armazenadas dentro dos registros de configuração de plataforma (PCRs) localizados no primeiro TPM 60 e podem ser usados para validar uma imagem do sistema operacional em uma âncora de confiança associada no instante da inicialização. Deste modo, a integridade do sistema pode ser verificada antes de permitir o acesso a informação sensível que pode ser vinculada aos PCRs.

[0048] As *personas* podem ser responsáveis por sua própria integridade, uma vez que o controle sofre transição de confiança do fabricante

do dispositivo durante o carregamento de inicialização. Por exemplo, é responsabilidade do primeiro OS de *persona* 112 validar aplicações 130 que estão instaladas e "rodam" no primeiro OS de *persona* 112. Deste modo, no caso em que uma aplicação intrusa (não mostrada) compromete a integridade de um sistema operacional convidado em execução no dispositivo de comunicação móvel 10, o compromisso não afetará a integridade dos outros sistemas operacionais convidados se estes não tiverem uma relação de confiança com o sistema operacional compromissado.

[0049] O supervisor de segurança 108 é acoplado em comunicação com o primeiro e segundo OSs de *persona* 112 e 122. O supervisor de segurança 108 é um sistema operacional que facilita o armazenamento e execução de políticas de segurança para uso na operação do dispositivo de comunicação móvel 10. O supervisor de segurança 108 "roda" em um ambiente isolado e pode ter acesso a recursos de plataforma, interfaces adicionais e/ou capacidades adicionais. Em algumas implementações, a primeira *persona* 110 e a segunda *persona* 120 são separadas através de um mecanismo confiável (isto é, virtualização de CPU) de tal modo que o proprietário de uma *persona* não pode configurar uma política de segurança de uma *persona* que não é de propriedade daquele proprietário de *persona*. Por exemplo, a política de segurança da primeira *persona* 110 pode ser configurada somente por um proprietário da primeira *persona* e a política de segurança da segunda *persona* 120 pode somente ser configurada por um proprietário da segunda *persona*. Mais especificamente, cada política de segurança pode ser assinada pelo código privado do proprietário da *persona* e a assinatura pode ser validada pelo dispositivo de comunicação móvel 10 usando um código público correspondente do proprietário da *persona*, antes do supervisor de segurança 108 aplicar a política de segurança à *persona* associada. As políticas de propriedade e segurança para a primeira *persona* 110 e segunda *persona* 120 são armazenadas em um arquivo de configuração

que pode ser mantido pelo supervisor de segurança 108. Adicionalmente, as políticas de propriedade e segurança são validadas por certificados criptográficos. Deste modo, cada proprietário de *persona* pode definir o sistema operacional, ambiente de execução confiável e política de segurança para a *persona* que possui.

[0050] As políticas de segurança da primeira *persona* 110 e segunda *persona* 120 podem ser definidas pelos proprietários de *persona* e podem ser definidas, armazenadas e reforçadas em isolamento do código de *persona*. As políticas de segurança definem como cada *persona* associada pode acessar dispositivos físicos no dispositivo de comunicação móvel 10. Por exemplo, as políticas de segurança restringem o acesso de uma *persona* a um ou mais dispositivos físicos, definem orientações para o acesso exclusivo de uma *persona* a um ou mais dispositivos físicos, e/ou define orientações para acesso a dispositivo compartilhado para a primeira *persona* 110 e segunda *persona* 120. Mais especificamente, as orientações para acesso a um dispositivo compartilhado podem habilitar o compartilhamento do dispositivo de tal modo que somente a *persona* no controle de uma interface de usuário tem acesso ao dispositivo compartilhado. Adicionalmente, as regras especificadas em uma ou mais políticas de segurança para acesso a um dispositivo compartilhado podem habilitar o compartilhamento do dispositivo, de tal modo que uma *persona* em execução no segundo plano pode ainda ter acesso ao dispositivo compartilhado. Deste modo, as regras definidas pelas políticas de segurança habilitam os proprietários de *persona* a adaptar o dispositivo de comunicação móvel 10 em uma variedade de configurações para adequar as suas necessidades.

[0051] A imagem de linha de base e/ou sistemas de arquivo da primeira *persona* 110 podem ser criptografados e armazenados em meios internos e/ou removíveis. Adicionalmente, o volume de inicialização da primeira *persona* 110 pode ser criptografado de tal modo que a autenticação

pré-inicialização a partir do processo de inicialização confiável pode ser requerida antes da primeira *persona* 110 poder inicializar e acessar dados sensíveis armazenados nela. Mais especificamente, durante o processo de inicialização confiável, um usuário pode ser orientado a entrar com credenciais antes da primeira *persona* 110 ter permissão para inicializar. O usuário pode desejar verificar um estado do dispositivo de comunicação móvel 10 antes de entrar com suas credenciais. Por exemplo, o usuário pode requerer verificação de que o dispositivo de comunicação móvel 10 está em um estado confiável, antes de entrar com uma chave de acesso e/ou número de identificação pessoal (PIN), para assegurar que a tela de entrada é autêntica. Conforme descrito acima, o dispositivo de comunicação móvel 10 inclui recursos de segurança tais como o botão de segurança 17 e/ou LEDs 19 e 21 (mostrados na Figura 1). Os recursos de segurança são isolados no hardware que é inacessível a partir de código não confiável em execução no dispositivo de comunicação móvel 10, para facilitar a verificação de que a tela de entrada é autêntica.

[0052] Em operação, um usuário pode atuar o botão de segurança 17 quando um diálogo de autenticação aparece na tela de toque 18 (mostrada na Figura 1). A atuação do botão de segurança 17 exibe a informação de raiz de confiança para o dispositivo de comunicação móvel 10 e/ou exibe a informação de raiz de configuração para o software requisitando que o diálogo de autenticação apareça. Por exemplo, a informação de raiz de confiança pode incluir uma informação de raiz de confiança para o dispositivo de comunicação móvel 10 e ou para uma *persona* em execução no dispositivo de comunicação móvel 10. Deste modo, o usuário pode verificar a informação de raiz de confiança e entrar de modo seguro com as credenciais requisitadas. Em uma implementação alternativa, o diálogo de autenticação pode ser verificado quando os LEDs 19 e 21 estão ativados em uma configuração predeterminada.

[0053] Em uma implementação, o usuário pode desejar alterar um estado operacional do dispositivo de comunicação móvel. Mais especificamente, o usuário pode desejar efetuar transição de um foco do dispositivo de comunicação móvel 10 entre *personas* em execução no dispositivo de comunicação móvel 10. Por exemplo, atuar o botão de segurança 17 facilita a transição do foco entre a primeira *persona* 110 e a segunda *persona* 120. Ainda mais, o primeiro LED 19 é designado à primeira *persona* 110 e o segundo LED 21 é designado à segunda *persona* 120. O primeiro LED 19 pode ser ativado e o segundo LED 21 pode ser desativado quando a primeira *persona* 110 está em foco e o segundo LED 21 pode ser ativado e o primeiro LED 19 pode ser desativado quando a segunda *persona* 120 está em foco. Deste modo, o primeiro LED 19 e o segundo LED 21 provêm realimentação visual ao usuário, com base no estado operacional do dispositivo de comunicação móvel 10.

[0054] Pelo menos um dentre os TPMs 60 e 62 possuem um recurso de presença física que orienta um usuário a verificar sua presença em relação ao dispositivo de comunicação móvel 10. Por exemplo, o recurso de presença física pode ser implementado para verificar que uma operação em execução no dispositivo de comunicação móvel 10 não está sendo realizada remotamente. Deste modo, o botão de segurança 17 pode ser pressionado para verificar a presença física do usuário.

[0055] Figura 5 é um fluxograma de um exemplo de método para reivindicar a propriedade de uma *persona* que pode ser usada com o dispositivo de comunicação móvel 10. No exemplo de implementação, o dispositivo de comunicação móvel 10 usa raízes de confiança criptográficas para definir a propriedade da primeira *persona* 110 e segunda *persona* 120. Por exemplo, a primeira *persona* 110 pode ser configurada para uso por uma entidade e a segunda *persona* 120 pode ser configurada para uso por outra entidade. Um emissor (isto é, um empreendimento) do dispositivo de

comunicação móvel 10 pode emitir um ou mais dispositivos de comunicação móveis 10 para um usuário (por exemplo, um cliente e/ou um empregado). Em tal implementação, a primeira *persona* 110 pode ser configurada para uso em negócios e a segunda *persona* 120 pode ser configurada para uso pessoal. Em uma implementação alternativa, o dispositivo de comunicação móvel 10 pode ser configurado para separar as *personas* designando SIMs separados, serviços separados, e/ou isolando dados, os sistemas operacionais e as comunicações celulares da primeira *persona* 110 e segunda *persona* 120.

[0056] Utilizar raízes de confiança criptográficas habilita o dispositivo de comunicação móvel 10 a verificar a integridade de uma configuração de *persona*, e limitar direitos de modificação da *persona* a partes autorizadas. Por exemplo, o dispositivo de comunicação móvel 10 pode ser provido a um usuário final com pelo menos uma *persona* padrão (isto é, uma *persona* sem proprietário definido) instalada nele. A *persona* padrão é assinada por uma âncora de confiança padrão pelo fabricante, o que indica que a *persona* é não modificada e que possui uma política padrão designada a ela. O usuário final pode então usar a *persona* padrão, mas não pode pessoaliza-la sem primeiramente obter a propriedade definindo uma raiz de confiança.

[0057] Um operador 200 reivindica propriedade de uma *persona*, tal como uma segunda *persona* 120, criando 212 uma raiz de confiança para a *persona* em uma estação de trabalho de um Gerenciador de *Persona* (PM) 202. Em algumas implementações, o PM 202 pode também habilitar o operador 200 a editar e/ou definir a política de segurança para a *persona* e/ou atualizar as imagens da *persona* e/ou um ambiente de execução confiável, tal como o segundo TEE 124. O operador 200 requisita que um Gerenciamento de Dispositivo (DM) 204 gere 214 um ingresso de reivindicação para reivindicar um sistema operacional, tal como o segundo OS de *persona* 122, para transferir a propriedade da âncora de confiança padrão para a raiz de

confiança criada 212. A transferência então autorizada 216 e o dispositivo de comunicação móvel 10 é reinicializada 218.

[0058] Durante a reinicialização 218, o operador 200 acopla um cabo de Barramento Serial Universal (USB) entre o DM 204 e o dispositivo de comunicação móvel 10, e o dispositivo de comunicação móvel 10 detecta a conexão USB e entra em um modo de programação, de tal modo que os sistemas operacionais da *persona* não carregam. O operador 200 então requisita 220, a partir da estação de trabalho, que o DM 204 execute software para transferir a *persona* para o novo proprietário. A requisição é direcionada 222 na direção de um supervisor de segurança 206 e pode definir uma nova âncora de confiança da *persona*. O supervisor de segurança 206 então usa o ingresso de reivindicação gerado 214 para requisitar 224 autorização do operador 200 para verificar sua identidade, e o operador 200 entre 226 com uma chave de acesso de dispositivo predeterminada em resposta à requisição de autorização 224. A requisição 224 pode também ser assinada pela raiz de confiança criada 212.

[0059] O dispositivo de comunicação móvel 10 então apresenta uma requisição de autenticação 228 do supervisor de segurança 206 para um usuário entrar com suas credenciais para destravar o elemento de segurança 208. Se a *persona* é confirmada como sendo sem proprietário pela âncora de confiança padrão, o ativo da *persona* antiga emite sinal numérico e as assinaturas são transferidas 234 para o DM 204. O DM 204 verifica as assinaturas e assina novamente os sinais numéricos com o novo código de assinatura da *persona* que é autorizada a assinar os ativos relevantes. Adicionalmente, o código de *persona* que permite acesso aos códigos de mídia da *persona* é alterado. Assinaturas de substituição são então transferidas 236 do DM 204 para o dispositivo de comunicação móvel 10, e o dispositivo de comunicação móvel 10 valida as assinaturas e substitui as assinaturas antigas nos ativos da *persona* pelas novas assinaturas.

[0060] Um arquivo de transição da *persona* é então criado 238, e o arquivo de configuração para a *persona* é verificado quanto a validade e conflitos com outros arquivos de configuração que já estão no dispositivo de comunicação móvel 10. O processo avança se o arquivo de configuração é validado, e a atualização de software é interrompida se houver um conflito entre arquivos de configuração. A autenticação da *persona* do usuário é atualizada 240 na autorização para avançar, de tal modo que os códigos de mídia podem ser acessados pela nova raiz de confiança e retornados 242 ao DM 204.

[0061] O DM 204 assina os ativos que estão sendo atualizados e retorna os sinais numéricos assinados. Por exemplo, ativos que estão sendo atualizados podem apresentar assinaturas que são atualizadas como sinais numéricos reassinados e/ou podem ser atualizados 246 com novas assinaturas. O arquivo de transição da *persona* é verificado 244 após cada atualização, para habilitar processo a ser reiniciado a partir de uma atualização interrompida. Depois da atualização estar completa, dados de armazenamento temporária são liberados 248 para a memória *flash* 210, o arquivo de transição de *persona* é apagado 250 e o dispositivo de comunicação móvel 10 é reinicializado 252.

[0062] Figura 6 é uma ilustração esquemática de um exemplo de sistema 300 para uso ao autorizar uma operação a ser realizada no dispositivo de comunicação móvel 10. No exemplo de implementação, uma entidade pode necessitar ser autorizada antes de ter permissão para modificar software instalado em um dispositivo de computação visado, tal como o dispositivo de comunicação móvel 10. Por exemplo, uma vez que uma *persona* tenha sido carregada no dispositivo de comunicação móvel 10, um fixador de dispositivo retém a autoridade para remover e/ou substituir aquela *persona*, porém o proprietário da *persona* tem a autoridade para modificar isto. Deste modo, uma entidade atuando em benefício do proprietário da *persona* pode

necessitar ser autorizada como tendo permissões predeterminadas autorizadas para ela, pelo proprietário da *persona*, para modificar uma *persona*. Conforme usado aqui, o termo "fixador de dispositivo" refere-se a uma entidade que usa uma *persona* padrão para operar o dispositivo de comunicação móvel 10.

[0063] Um computador administrador, tal como o gerenciador de dispositivo (DM) 302, pode gerar e transmitir uma requisição para um servidor de autorização 304 para autorização para realizar uma operação no dispositivo de comunicação móvel 10. A requisição é um arquivo que especifica os parâmetros para a operação a ser realizada no dispositivo de comunicação móvel 10. Exemplos de parâmetros incluem, porém não estão limitados a identificação de um dispositivo de computação visado (por exemplo, o dispositivo de comunicação móvel 10), a operação a ser realizada no dispositivo de computação visado, um período de tempo no qual a operação será realizada e uma localização geográfica do dispositivo de computação visado. Ainda mais, a requisição é assinada por um primeiro código privado de um par de código público privado designado a um administrador. Em algumas implementações, a requisição pode ser transmitida via mídia removível (não mostrada).

[0064] O servidor de autorização 304 recebe a requisição do DM 302 e verifica a assinatura do DM 302 com o código público do primeiro par de código público privado. O servidor de autorização 304 também determina se os parâmetros para a operação ser realizada se alinham com a política de segurança para o dispositivo de comunicação móvel 10. Parâmetros autorizados podem ser armazenados em uma base de dados de autorização 306, que é acessível pelo servidor de autorização 304. O servidor de autorização 304 então gera uma resposta de autorização se a requisição tiver sido autorizada. A resposta de autorização pode incluir a requisição a partir do DM 302 e uma senha de autorização criado pelo servidor de autorização 304. A senha de autorização pode ser usada para autorizar a operação requerida.

Em algumas realizações, a senha de autorização pode ter um período de autorização predeterminado, no qual a operação requisitada pode ser realizada, pode ser restrita a conceder autorização para um dispositivo de computação visado particular e/ou pode autorizar o desempenho de uma única ou operações múltiplas no dispositivo de comunicação móvel 10. Como um exemplo somente, a senha de autorização pode incluir autorização para realizar a operação em um dispositivo de computação visado predeterminado, e/ou autorização para realizar uma operação predeterminada no dispositivo de computação visado. Ainda mais, a senha de autorização pode ser gerada pelo menos antes de receber a requisição para realizar a operação no dispositivo de comunicação móvel 10 ou em resposta à verificação da requisição para executar a operação no dispositivo de comunicação móvel 10. A resposta de autorização pode então ser assinada por um segundo código privado de um par de código público privado associado ao computador servidor de autorização e transmitido ao computador administrador. Em uma implementação alternativa, a resposta de autorização pode ser assinada por um operador de autenticação. Por exemplo, a requisição pode ser enfileirada e, assinada, autorizada ou negada pelo operador de autenticação. Em algumas realizações, a resposta de autorização pode ser transmitida através de mídia removível (não mostrada).

[0065] O DM 302 recebe a resposta de autorização e determina se a senha de autorização autoriza a operação requisitada. Por exemplo, o DM 302 pode verificar a resposta de autorização com um código público do segundo par de código público, privado, onde a resposta de autorização é assinada com um código privado do segundo par de código público, privado. O DM 302 então transmite o arquivo de resposta de autorização ao dispositivo de comunicação móvel 10 para requisitar que uma operação seja realizada se a requisição tiver sido autorizada. Transmitir a resposta de autorização pode incluir assinar a resposta de autorização com o código privado do primeiro par

de código público, privado. O dispositivo de comunicação móvel 10 recebe a resposta de autorização e verifica as assinaturas com um código público do primeiro par de código público, privado associado ao computador administrador e determina se os parâmetros especificados na resposta de autorização se alinham com a política de segurança para o dispositivo de comunicação móvel 10. O dispositivo de comunicação móvel 10 permite que a operação requisitada prossiga se as assinaturas são verificadas e os parâmetros se alinham. A operação privilegiada pode então ser realizada no dispositivo de comunicação móvel 10. Em uma implementação alternativa, a resposta de autorização pode incluir uma cadeia de certificado para uma raiz de confiança de autorização. Adicionalmente, em uma implementação alternativa, a senha de autorização pode ser gerada e transmitida via mídia removível.

[0066] Figura 7 é um fluxograma de um exemplo de método para atualizar software de *persona* que pode ser usado com o dispositivo de comunicação móvel 10. No exemplo de implementação, o operador 400 pode atualizar um OS de *persona* existente, tal como a segunda *persona* 120, acoplando um cabo USB a partir de uma estação de trabalho 402 do Gerenciamento de Dispositivo (DM) para o dispositivo de comunicação móvel 10. O software de gerenciamento de dispositivo é executado e o operador 400 direciona o dispositivo de comunicação móvel 10 para reinicialização 410. Durante a reinicialização 410, o dispositivo de comunicação móvel 10 detecta a conexão USB e entra em um modo de programação, de tal modo que os sistemas operacionais da *persona* não carregam. O operador 400 então direciona o software DM 412 para requisitar 414 uma atualização para um OS de *persona* no dispositivo de comunicação móvel 10. A estação de trabalho DM 402 contata um servidor de autorização para obter uma senha de autorização. A senha de autorização pode ser armazenada em cache e/ou carregado a partir de uma fonte off-line. O

supervisor de segurança 404 pode então autorizar 416 a requisição 414 e atualização de *persona* 418 pode prosseguir. Em algumas implementações, o software de DM alertará o operador 400 e se recusará a realizar o processo de atualização se uma senha de autorização válida não estiver presente.

[0067] A estação de trabalho DM 402 inclui um código secreto compartilhado que pode ser usado para destravar o elemento seguro 406. Somente códigos de criptografia de armazenamento relacionados à *persona* autorizada podem ser recuperados a partir do elemento seguro 406, usando a autenticação provida pelo código secreto compartilhado. O dispositivo de comunicação móvel 10 então valida a senha de autorização para verificar que o operador 400 tem os privilégios para realizar a operação requisitada. O usuário é autenticado 420 pelo elemento seguro 406 e a operação é abortada se o operador 400 não possui as credenciais adequadas.

[0068] O software DM então requisita 422 dados de geometria de dispositivo da *persona*, a partir do dispositivo de comunicação móvel 10. Os dados de geometria do dispositivo podem incluir, porém não estão limitados a um tamanho dos componentes do OS e TEE de uma *persona*. A atualização de software avança se a geometria da *persona* coincide com a geometria do dispositivo, e a atualização de software é interrompida e um erro é indicado se houver uma incompatibilidade. Em uma implementação alternativa, o número de revisão dos pacotes de propriedade da *persona* pode também ser provido e assim o proprietário da *persona* pode verificar a compatibilidade da atualização.

[0069] O software DM começa o processo de carga transmitindo 424 o software a ser atualizado ao dispositivo de comunicação móvel 10. Em uma implementação, a atualização de software começa transmitindo 426 a configuração da *persona* se esta for incluída na atualização. O supervisor de segurança 404 então examina e avalia a geometria do arquivo de configuração, raiz de confiança e assinatura para determinar se ocorrerá um

conflito com outros arquivos de configuração que já estão carregados no dispositivo de comunicação móvel 10. A atualização de software prossegue se o arquivo de configuração é validado 428 e/ou se o arquivo de configuração não estiver sendo atualizado, e a atualização de software é interrompida se houver um conflito entre arquivos de configuração. Adicionalmente, um sistema operacional atualizado e/ou um ambiente de execução confiável pode ser carregado 430 e 432 em um dispositivo de comunicação móvel 10.

[0070] As atualizações de software transmitidas são armazenadas em uma memória flash 408 e validadas na âncora de confiança. Um arquivo de transição de *persona* é então criado 434 para indicar qual software deve ser atualizado, o software é escrito na memória flash 408 e um ponto de verificação é criado no arquivo de transição depois de cada atualização. Por exemplo, o novo arquivo de configuração é escrito 436 na memória flash 408 e o arquivo de transição é verificado 438, o novo sistema de arquivos de OS de *persona* é escrito 404 na memória flash 408 e o arquivo de transição é verificado 442, e o novo sistema de arquivo TEE de *persona* é escrito 444 na memória flash 408 e o arquivo de transição é verificado 446. Na implementação típica, os sistemas de arquivo *flash* alvo são programados a partir dos conteúdos da memória armazenados anteriormente e são criptografados durante a transferência usando códigos de armazenamento a partir do arquivo de configuração. Depois da atualização estar completa, os dados de armazenamento temporária são liberados 448 para a memória flash 408, o arquivo de transição de *persona* é apagado 450 e o dispositivo de comunicação móvel 10 é reinicializado 452.

[0071] Figura 8 é um fluxograma de um exemplo de método para transição de propriedade de uma *persona* que pode ser usado com o dispositivo de comunicação móvel 10. A propriedade de uma *persona* carregada no dispositivo de comunicação móvel 10 pode sofrer transição para um novo proprietário, sem atualizar os dados da *persona*. Na implementação

típica, o novo proprietário gera 510 um ingresso de transferência dentro do gerenciador de dispositivo (DM) (Novo RoT) 502. O ingresso de transferência pode ser um bloco de dados que detalha o dispositivo específico a sofrer transição e a raiz de confiança atual esperada. O bloco de dados é então enviado ao proprietário atual da *persona* e o proprietário atual da *persona* verifica a informação dentro do (DM) (Novo RoT) 502 do proprietário da *persona* atual.

[0072] O operador 500 trabalhando em benefício do proprietário da *persona* atual, obtém então uma senha de autorização indicando se o operador e o proprietário da *persona* atual são autorizados 512, 514 pelo (DM) (Antigo RoT) 503 para transferir a *persona*. A senha de autorização é então anexada e assina o ingresso de transferência, e o ingresso de transferência assinado é transferido e armazenado 516 na memória flash 508. O ingresso de transferência assinado pode também ser retornado ao novo proprietário da *persona* prospectivo juntamente com o código de autenticação para o compartimento da *persona* dentro do elemento seguro 506. Em tal implementação, o código de autenticação pode ser envolto usando o novo código público do operador DM do novo proprietário da *persona* que é anexado ao ingresso de transferência. O operador trabalhando em benefício do novo proprietário da *persona* pode então usar o ingresso de transferência envolto para iniciar o processo de transferência. Mais especificamente, o dispositivo de comunicação móvel 10 pode verificar as credenciais do novo proprietário da *persona* e autorizar a transferência.

[0073] O operador 500 então acopla um cabo USB de uma estação de trabalho do (DM) (Novo RoT) 502 ao dispositivo de comunicação móvel 10. O software de gerenciamento de dispositivo é executado e o operador 500 direciona o dispositivo de comunicação móvel 10 para reinicialização 518. Durante a reinicialização 518, o dispositivo de comunicação móvel 10 detecta a conexão USB e entra em um modo de programação, de tal modo que os

sistemas operacionais da *persona* não carregam. O operador 500 então instrui o software DM para transição de uma *persona* de propriedade do proprietário de *persona* atual para o novo proprietário da *persona*. O ingresso de transferência inclui informação requerida para a autorização e um certificado de infraestrutura de código público (PKI) do operador 500 que serve para autenticar a requisição assinada pela raiz de confiança para o proprietário anterior da *persona* submetida a transição.

[0074] O software DM usa o código secreto do operador 500 para desempacotar o código de autenticação a partir do ingresso de transferência. O código de autenticação pode ser então usado 520 para requisitar 522 transferência de *persona* e para autenticar 524 o operador para destravar o elemento seguro 506 no dispositivo de comunicação móvel 10. Em tal implementação, a autenticação 524 somente habilita o armazenamento de códigos de criptografia relacionados à *persona* autorizada a ser recuperada a partir do elemento seguro 506.

[0075] A transição inclui adicionalmente transferir 530 os sinais numéricos de ativo da *persona* antiga para o DM 502. O DM 502 verifica as assinaturas e reassina os sinais numéricos com o código de assinatura da nova *persona* que é autorizada a assinar os ativos relevantes. Adicionalmente, o código de *persona* que permite acesso aos códigos de mídia da *persona* é alterado, e o novo valor é transmitido para o DM 502. As assinaturas de substituição são então transferidas 532 do DM 502 para o dispositivo de comunicação móvel 10, e o dispositivo de comunicação móvel 10 valida as assinaturas e substitui as assinaturas antiga nos ativos da *persona* pelas novas assinaturas.

[0076] Um arquivo de transição de *persona* é então criado 534, e o arquivo de configuração para a *persona* é verificado quanto à validade e conflitos com outros arquivos de configuração que já estão carregados no dispositivo de comunicação móvel 10. O processo avança, se o arquivo de

configuração é validado, e a atualização de software é interrompida se há um conflito entre arquivos de configuração. A autenticação de *persona* do usuário é atualizada 536 na autorização para prosseguir, de tal modo que códigos de mídia podem ser acessados pela nova raiz de confiança e retornados 538 ao DM 502.

[0077] O DM 502 assina os ativos que estão sendo atualizados e retorna os sinais numéricos assinados. Por exemplo, ativos que estão sendo autorizados podem apresentar assinaturas que são atualizadas com sinais numéricos reassinados e/ou podem ser atualizados 542 com novas assinaturas. O arquivo de transição da *persona* é submetido a ponto de verificação 504 após cada atualização para habilitar o processo a ser reiniciado a partir de uma atualização interrompida. Depois da atualização estar completa, dados de armazenamento temporária são liberados 544 para a memória flash 508, o arquivo de transição da *persona* é apagado 546 e o dispositivo de comunicação móvel 10 é reinicializado 548.

[0078] Após a propriedade da *persona* ter sido transferida para o novo proprietário da *persona*, uma nova relação de confiança pode necessitar ser estabelecida entre a *persona* submetida a transição e quaisquer *personas* que tenham uma relação de confiança com o proprietário da *persona* anterior. Mais especificamente, a configuração da *persona* das outras *personas* em execução no dispositivo de comunicação móvel 10 pode ter que ser atualizada para estabelecer uma relação de confiança com o proprietário da nova *persona*, para manter a mesma funcionalidade que com o proprietário da *persona* anterior.

[0079] Figura 9 é um fluxograma de um exemplo de método para carregar uma nova *persona* que pode ser usado com o dispositivo de comunicação móvel 10. No exemplo de implementação, o operador 600 acopla um cabo USB de uma Estação de Trabalho do Dispositivo Gerenciador (DM) 602 ao dispositivo de comunicação móvel 10. O software de

gerenciamento de dispositivo é executado e o operador 600 direciona o dispositivo de comunicação móvel 10 para reinicialização 612. Durante a reinicialização 612, o dispositivo de comunicação móvel 10 detecta a conexão USB e entra em um modo de programação, de tal modo que os sistemas operacionais da *persona* não carregam. O operador 600 então é orientado 614 para autorizar a conexão USB com uma chave de acesso do dispositivo mantida pelo proprietário do dispositivo, e a chave de acesso do dispositivo é inserida 616 e autenticada 618 para destravar o elemento seguro 606. Em uma implementação alternativa, o dispositivo de comunicação móvel 10 pode ser reinicializado e reiniciado para uma configuração de fábrica.

[0080] O software DM então requisita 620 dados de geometria do dispositivo da *persona*, a partir do dispositivo de comunicação móvel 10, e o operador 600 direciona a Estação de Trabalho DM 602 para carregar 622 o pacote da *persona* em um compartimento da *persona* específica. Os dados de geometria do dispositivo podem incluir, porém não estão limitados a um tamanho dos componentes OS e TEE de uma *persona*. A atualização de software prossegue se a geometria da *persona* coincide com a geometria do dispositivo, e a atualização do software é interrompida é um erro é indicado se houver uma incompatibilidade. Em uma implementação alternativa, o número de revisão dos pacotes de propriedade da *persona* pode também ser provido e assim o proprietário da *persona* pode verificar compatibilidade da atualização.

[0081] O software DM inicia o processo de carregamento, transmitindo o software a ser carregado para o dispositivo de comunicação móvel 10. Em uma implementação, o carregamento do software começa transmitindo 624 o arquivo de configuração da *persona* para o dispositivo de comunicação móvel 10. O supervisor de segurança 604 então examina e avalia a geometria do arquivo de configuração, raiz de confiança e assinatura para determinar se ocorrerá um conflito com outros arquivos de configuração

que já estão carregados no dispositivo de comunicação móvel 10. O carregamento de software avança se o arquivo de configuração é validado 626 e o carregamento de software é interrompido se há um conflito entre arquivos de configuração. Em algumas implementações, um novo OS de *persona* e um novo TEE são carregados 628 e 630 no dispositivo de comunicação móvel 10.

[0082] O software transmitido é armazenado na memória flash 608 e validado na âncora de confiança. Um arquivo de transição de *persona* é então criado 632 e escrito para indicar sobrescrita. A indicação de sobrescrita é um valor de sentinela escrito de uma maneira persistente, de tal modo que medidas de recuperação apropriadas podem ser tomadas para recuperar de falha, se o processo de atualização é interrompido. Mais especificamente, códigos de mídia de armazenamento no elemento seguro 606 para a *persona* são deletados 634, e o arquivo de configuração de *persona* antiga é apagado 636, os sistemas de arquivos *flash* da *persona* são apagados 638 e o módulo de plataforma confiável (TPM) 610 é submetido a liberação forçada 640.

[0083] A nova *persona* pode então ser carregada no dispositivo de comunicação móvel 10 de uma maneira persistente. Mais especificamente, o novo arquivo de configuração é escrito 642 sobre a memória flash 608, dados de autenticação de usuário são lidos 644 pelo supervisor de segurança 604 e o usuário é autenticado 646 para destravar o elemento seguro 606. Um código de criptografia público (PEK) de um par de código público, privado pode então ser criado 648 e exportado 650 para o proprietário da *persona*, a partir do elemento seguro 606. O proprietário da *persona* assina o PEK com sua autoridade certificada e o carregamento de software 654 prossegue, se o arquivo de configuração é validado 652. O PEK é então retornado e armazenado no elemento seguro 606.

[0084] O código secreto do par de código público, privado PEK é armazenado e protegido dentro do elemento seguro 606, de tal modo que este não será exportado do elemento seguro 606. Isto habilita um proprietário da

persona a verificar, pela resposta assinada pelo código privado, que uma requisição para executar um serviço veio de um dispositivo autorizado. O PEK pode ser criado no instante em que a propriedade da *persona* é definida e pode ser usado para autenticar uma atualização de software, requisição e/ou pacote, por exemplo. Em uma implementação alternativa, um segundo par de código público, privado pode ser criado e usado para criptografia, de tal modo que um proprietário da *persona* pode criptografar dados objetivando um dispositivo específico, e de tal modo que outros dispositivos não seriam capazes de decriptografar os dados.

[0085] O novo sistema de arquivo OS da *persona* é então escrito 658 na memória flash 608, o novo sistema de arquivo TEE da *persona* é escrito 660 na memória flash 608 e uma nova partição de dados da *persona* é criada 662. Os sistemas de arquivo *flash* alvo são programados a partir dos conteúdos da memória armazenados anteriormente, e são criptografados durante a transferência usando os códigos de armazenamento a partir do arquivo de configuração. Após a atualização estar completa, o arquivo de transição da *persona* é deletado 664 e o dispositivo de comunicação móvel 10 é reinicializado 666.

[0086] Adicionalmente, a descrição compreende realizações de acordo com as seguintes cláusulas:

Cláusula 1. Um meio legível por computador não transitório armazenando instruções executáveis em computador, para operar um dispositivo de comunicação móvel que inclui um processador, um primeiro módulo de plataforma confiável e um segundo módulo de plataforma confiável, as instruções executáveis pelo computador fazem com que o processador:

estabeleça uma raiz de confiança para uma primeira *persona*, a primeira *persona* incluindo um primeiro sistema operacional e um primeiro ambiente de execução confiável;

estabeleça uma raiz de confiança para uma segunda *persona*, a segunda *persona* incluindo um segundo sistema operacional e um segundo ambiente de execução confiável;

armazene medições definindo a raiz de confiança para a primeira *persona* no primeiro módulo de plataforma confiável;

armazene medições definindo a raiz de confiança para a segunda *persona* no segundo módulo de plataforma confiável; e

carregue a primeira *persona* e a segunda *persona* usando as raízes de confiança para a primeira e segunda *persona*s.

Cláusula 2. O meio legível por computador não transitório de acordo com a Cláusula 1, compreendendo adicionalmente instruções executáveis por computador que fazem com que o processador:

estabeleça confiança mútua entre o primeiro ambiente de execução confiável e o segundo ambiente de execução confiável, de tal modo que a primeira *persona* é acoplada em comunicação com a segunda *persona*.

Cláusula 3. O meio legível por computador não transitório de acordo com a Cláusula 1, compreendendo adicionalmente instruções executáveis por computador que fazem com que o processador:

carregue um sistema operacional básico com um carregador de inicialização assinado por uma raiz de confiança do fabricante.

Cláusula 4. O meio legível por computador não transitório de acordo com a Cláusula 1, compreendendo adicionalmente instruções executáveis por computador que fazem com que o processador:

transfira controle do primeiro módulo de plataforma confiável para a primeira *persona* e transfira controle do segundo módulo de plataforma confiável para a segunda *persona*, após a primeira e segunda *personas* terem sido carregadas.

Cláusula 5. O meio legível por computador não transitório de acordo com a Cláusula 1, compreendendo adicionalmente instruções

executáveis por computador que fazem com que o processador:

defina uma política de segurança para a primeira *persona* e a segunda *persona*, em que as políticas de segurança definem como a primeira *persona* e a segunda *persona* acessam dispositivos físicos no dispositivo de comunicação móvel; e

reforce as políticas de segurança com um supervisor de segurança.

[0087] Esta descrição escrita usa exemplos para divulgar várias implementações, incluindo o melhor modo, e também para habilitar qualquer pessoa especialista na técnica a praticar as várias implementações, incluindo produzir e utilizar quaisquer dispositivos ou sistemas e realizando quaisquer métodos incorporados. O escopo patenteável da descrição é definido pelas reivindicações e pode incluir outros exemplos que ocorre aos especialistas na técnica. Tais outros exemplos são destinados a estar dentro do escopo das reivindicações se tiverem elementos estruturais que não diferem da linguagem literal das reivindicações, ou se incluem elementos estruturais equivalentes com diferenças não substanciais a partir da linguagem literal das reivindicações.

REIVINDICAÇÕES

1. Dispositivo de comunicação móvel, caracterizado pelo fato de que compreende:

um primeiro módulo de plataforma confiável (60);

um segundo módulo de plataforma confiável (62);

um processador (24); e

um meio de armazenamento não-transitório (22) compreendendo instruções que fazem com que dito processador (24):

estabeleça uma primeira raiz de confiança para uma primeira *persona* (110), a primeira *persona* (110) compreendendo um primeiro sistema operacional (112) e um primeiro ambiente de execução confiável (114);

estabeleça uma segunda raiz de confiança para uma segunda *persona* (120), a segunda *persona* (120) compreendendo um segundo sistema operacional (122) e um segundo ambiente de execução confiável (124), em que a primeira raiz de confiança é separada da segunda raiz de confiança;

armazene medições definindo a primeira raiz de confiança para a primeira *persona* (110) no primeiro módulo de plataforma confiável (60);

armazene medições definindo a segunda raiz de confiança para a segunda *persona* (120) no segundo módulo de plataforma confiável (62); e

carregue a primeira *persona* (110) e a segunda *persona* (120) usando as raízes de confiança para as primeira e segunda *persona*s, em que a primeira *persona* pode acessar componentes do dispositivo de comunicação móvel de acordo com a primeira raiz de confiança e a segunda *persona* pode acessar componentes do dispositivo de comunicação móvel de acordo com a segunda raiz de confiança.

2. Dispositivo de acordo com a reivindicação 1, caracterizado pelo fato de que dito meio de armazenamento (22) compreende adicionalmente instruções que fazem com que dito processador (24)

estabeleça confiança mútua entre o primeiro ambiente de execução confiável (110) e o segundo ambiente de execução confiável (120) de modo que a primeira *persona* (110) seja acoplada em comunicação com a segunda *persona* (120).

3. Dispositivo de acordo com a reivindicação 2, caracterizado pelo fato de que compreende adicionalmente uma guarda de alta garantia que facilita restringir transferência de dados entre a primeira *persona* (110) e a segunda *persona* (120) quando a primeira *persona* (110) está acoplada em comunicação com a segunda *persona* (120).

4. Dispositivo de acordo com a reivindicação 1, caracterizado pelo fato de que dito meio de armazenamento (22) compreende adicionalmente instruções que fazem com que dito processador (24) transfira controle do primeiro módulo de plataforma confiável (60) à primeira *persona* (110) e transfira controle do segundo módulo de plataforma confiável (62) à segunda *persona* (120) após as primeira e segunda *persona*s terem sido carregadas.

5. Dispositivo de acordo com a reivindicação 4, caracterizado pelo fato de que o primeiro ambiente de execução confiável (114) tem acesso exclusivo ao primeiro módulo de plataforma confiável (60) e o segundo ambiente de execução confiável (124) tem acesso exclusivo ao segundo módulo de plataforma confiável (62).

6. Dispositivo de acordo com a reivindicação 1, caracterizado pelo fato de que dito meio de armazenamento (22) compreende adicionalmente instruções que fazem com que dito processador (24) valide uma imagem do primeiro sistema operacional (112) e segundo sistema operacional (122) com as raízes de confiança associadas para a primeira *persona* (110) e segunda *persona* (120) durante o carregamento.

7. Dispositivo de acordo com a reivindicação 1, caracterizado pelo fato de que dito meio de armazenamento (22) compreende

adicionalmente instruções que fazem com que dito processador (24) execute a primeira *persona* (110) e a segunda *persona* (120) em contextos que estão isoladas uma da outra.

8. Método para operar um dispositivo de comunicação móvel (10), dito método caracterizado pelo fato de que compreende:

estabelecer uma primeira raiz de confiança para uma primeira *persona* (110), a primeira *persona* (110) incluindo um primeiro sistema operacional (112) e um primeiro ambiente de execução confiável (114);

estabelecer uma segunda raiz de confiança para uma segunda *persona* (120), a segunda *persona* (120) incluindo um segundo sistema operacional (122) e um segundo ambiente de execução confiável (124), em que a primeira raiz de confiança é separada da segunda raiz de confiança;

armazenar medições definindo a primeira raiz de confiança para a primeira *persona* (110) no primeiro módulo de plataforma confiável (60);

armazenar medições definindo a segunda raiz de confiança para a segunda *persona* (120) no segundo módulo de plataforma confiável (62); e

carregar a primeira *persona* (110) e a segunda *persona* (120) usando as raízes de confiança para a primeira e segunda *persona*s, em que a primeira *persona* pode acessar componentes do dispositivo de comunicação móvel de acordo com a primeira raiz de confiança e a segunda *persona* pode acessar componentes do dispositivo de comunicação móvel de acordo com a segunda raiz de confiança.

9. Método de acordo com a reivindicação 8, caracterizado pelo fato de que compreende adicionalmente estabelecer confiança mútua entre o primeiro ambiente de execução confiável (114) e o segundo ambiente de execução confiável (124), de tal modo que a primeira *persona* (110) é

acoplada em comunicação com a segunda *persona* (120).

10. Método de acordo com a reivindicação 8, caracterizado pelo fato de que carregar a primeira *persona* (110) e a segunda *persona* (120) compreende carregar um sistema operacional subjacente com um carregador de inicialização (144) assinado por uma raiz de confiança fabricante de dispositivo.

11. Método de acordo com a reivindicação 8, caracterizado pelo fato de que estabelecer as raízes de confiança para a primeira (110) e segunda (120) *personas* compreende validar uma imagem do primeiro sistema operacional (112) e do segundo sistema operacional (122) com as raízes de confiança para a primeira (110) e segunda (120) *personas*, durante o carregamento.

12. Método de acordo com a reivindicação 8, caracterizado pelo fato de que compreende adicionalmente transferir o controle do primeiro módulo de plataforma confiável (60) para a primeira *persona* (110) e transferir controle do segundo módulo de plataforma confiável (62) para a segunda *persona* (120), após a primeira e segunda *personas* terem sido carregadas.

13. Método de acordo com a reivindicação 8, caracterizado pelo fato de que, estabelecer uma raiz de confiança para as primeira e segunda *personas*, compreende:

medir componentes de software usados para estabelecer as raízes de confiança da primeira (110) e segunda (120) *personas*; e

estender as medições no primeiro (60) e segundo (62) módulos de plataforma confiável, em que as medições para a primeira âncora de confiança se estendem no primeiro módulo de plataforma confiável (60) e as medições para a segunda âncora de confiança se estendem no segundo módulo de plataforma confiável (62).

14. Método de acordo com a reivindicação 8, caracterizado

pelo fato de que compreende adicionalmente:

definir uma política de segurança para a primeira *persona* (110) e a segunda *persona* (120), em que as políticas de segurança definem como a primeira *persona* (110) e a segunda *persona* (120) acessam dispositivos físicos no dispositivo de comunicação móvel (10); e

reforçar as políticas de segurança com um supervisor de segurança (108).

15. Método de acordo com a reivindicação 14, caracterizado pelo fato de que reforçar as políticas de segurança compreende pelo menos um dentre:

habilitar acesso exclusivo para uma dentre a primeira *persona* (110) e a segunda *persona* (120) para pelo menos um dos dispositivos físicos;

habilitar acesso compartilhado entre a primeira *persona* (110) e a segunda *persona* (120) para pelo menos um dos dispositivos físicos; e

negar acesso de pelo menos um dos dispositivos físicos a uma dentre a primeira *persona* (110) e a segunda *persona* (120).

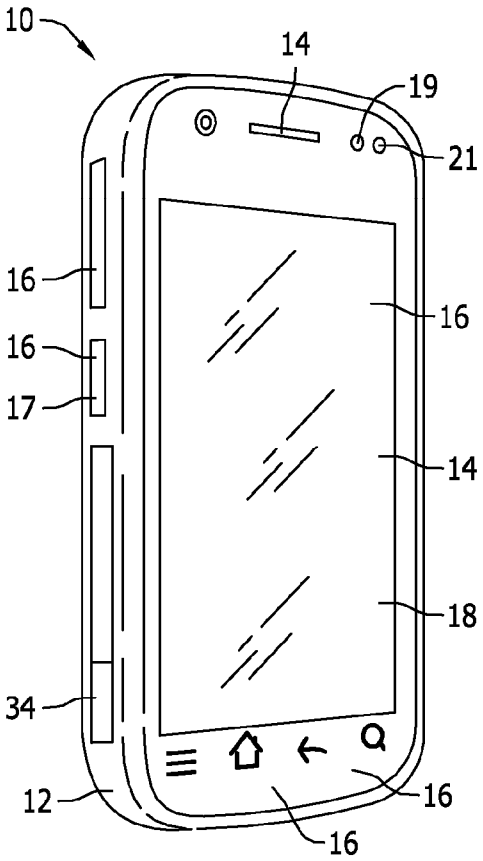

FIG. 1

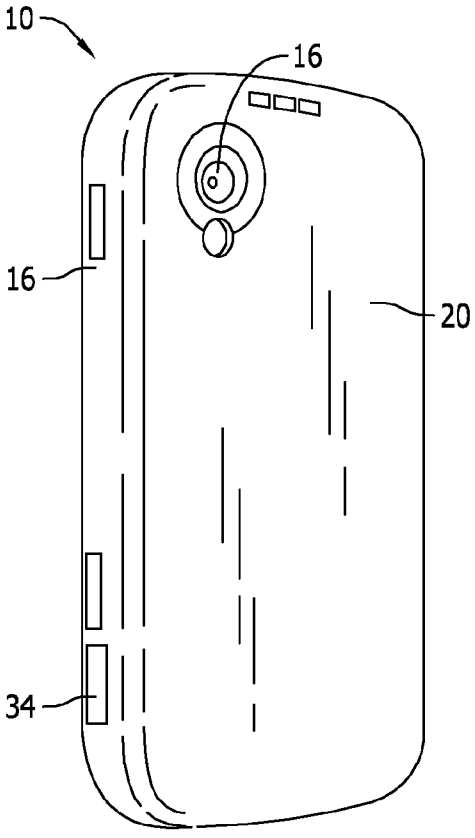

FIG. 2

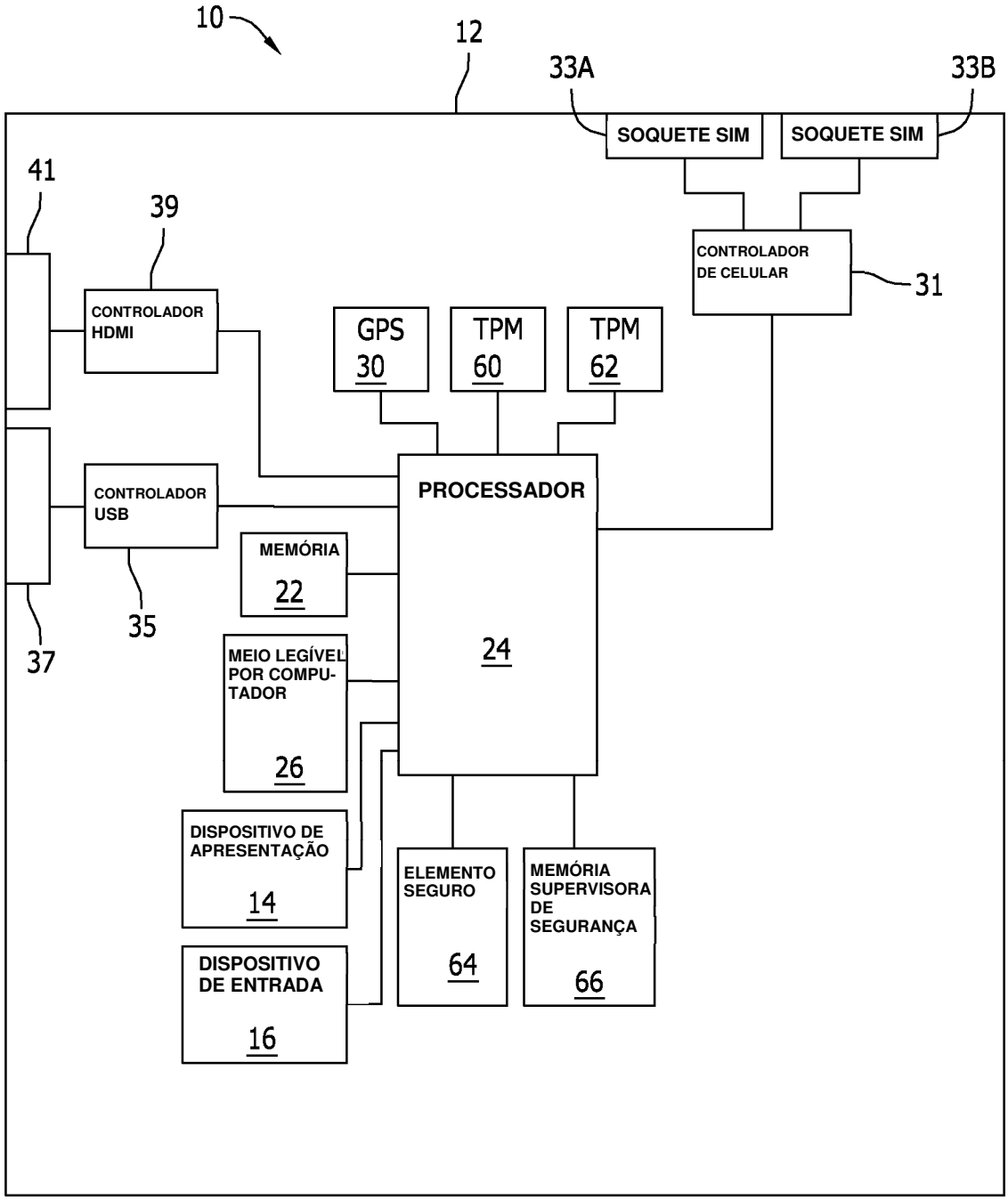
10
12
33A
33B
SOQUETE SIM
SOQUETE SIM
41
39
CONTROLADOR DE CELULAR
31
CONTROLADOR HDMI
GPS 30
TPM 60
TPM 62
CONTROLADOR USB
PROCESSADOR
24
MEMÓRIA 22
35
37
MEIO LEGÍVEL POR COMPUTADOR 26
DISPOSITIVO DE APRESENTAÇÃO 14
ELEMENTO SEGURO 64
MEMÓRIA SUPERVISORA DE SEGURANÇA 66
DISPOSITIVO DE ENTRADA 16

FIG. 3

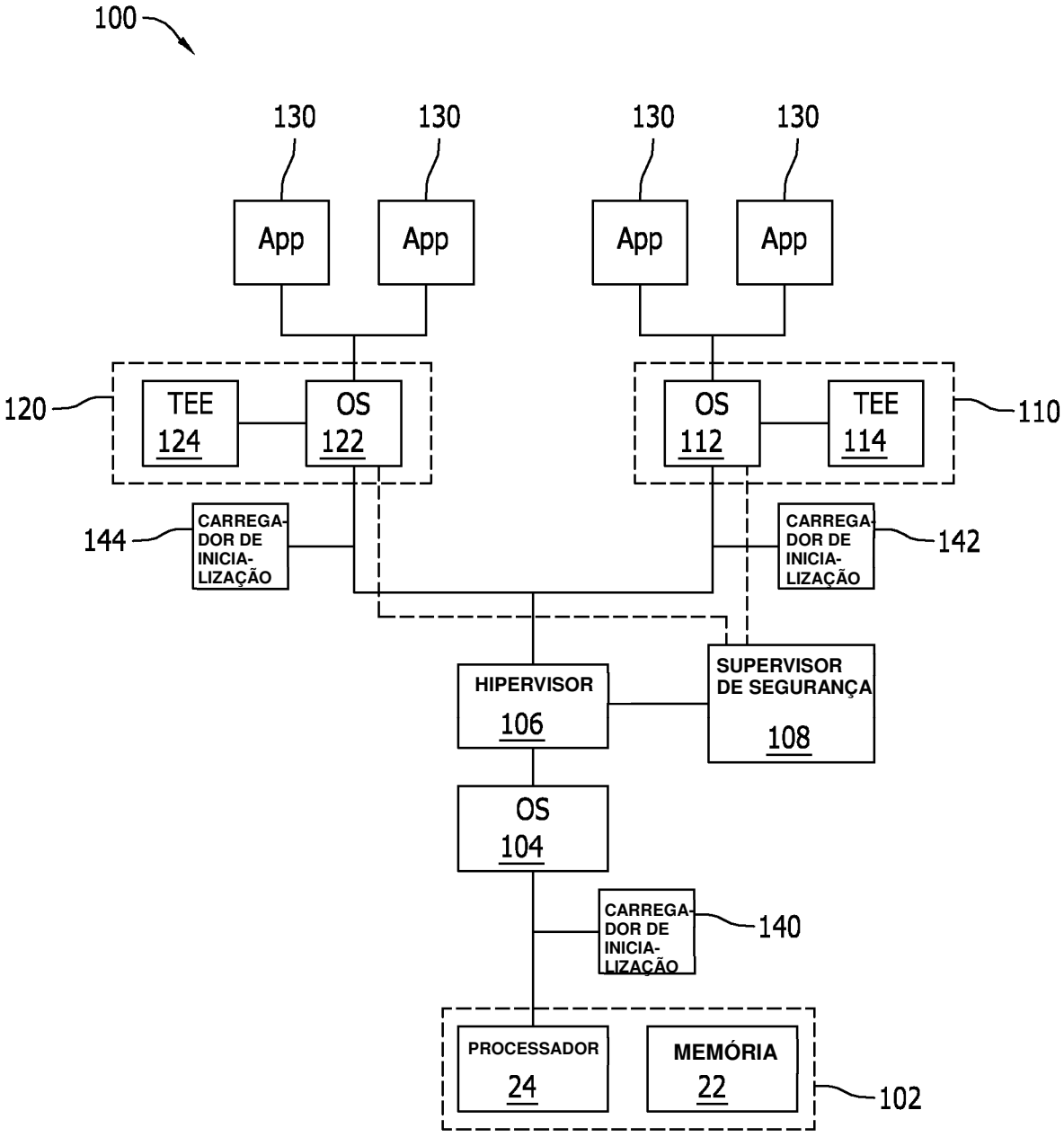
100
130
130
130
130
App
App
App
App
120
TEE
124
OS
122
OS
112
TEE
114
110
144
CARREGA-DOR DE INICIA-LIZAÇÃO
CARREGA-DOR DE INICIA-LIZAÇÃO
142
HIPERVISOR
106
SUPERVISOR DE SEGURANÇA
108
OS
104
CARREGA-DOR DE INICIA-LIZAÇÃO
140
PROCESSADOR
24
MEMÓRIA
22
102

FIG. 4

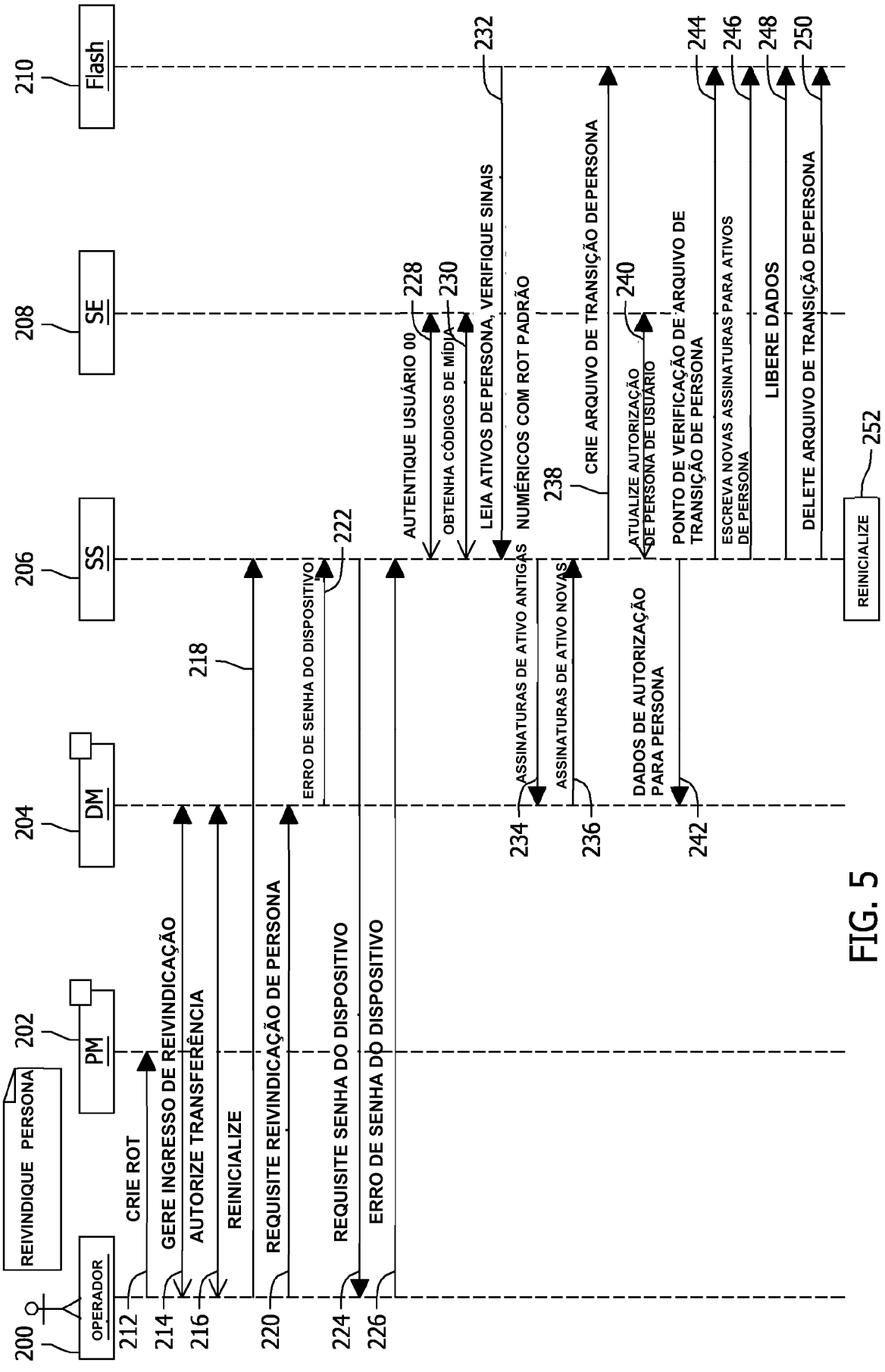
200
OPERADOR
REIVINDIQUE PERSONA
202
PM
204
DM
206
SS
208
SE
210
Flash
212
CRIE ROT
214
GERE INGRESSO DE REIVINDICAÇÃO
216
AUTORIZE TRANSFERÊNCIA
218
REINICIALIZE
220
REQUISITE REIVINDICAÇÃO DE PERSONA
222
ERRO DE SENHA DO DISPOSITIVO
224
REQUISITE SENHA DO DISPOSITIVO
226
ERRO DE SENHA DO DISPOSITIVO
228
AUTENTIQUE USUÁRIO 00
230
OBTENHA CÓDIGOS DE MÍDIA
232
LEIA ATIVOS DE PERSONA, VERIFIQUE SINAIS NUMÉRICOS COM ROT PADRÃO
234
ASSINATURAS DE ATIVO ANTIGAS
236
ASSINATURAS DE ATIVO NOVAS
238
CRIE ARQUIVO DE TRANSIÇÃO DEPERSONA
240
ATUALIZE AUTORIZAÇÃO DE PERSONA DE USUÁRIO
242
DADOS DE AUTORIZAÇÃO PARA PERSONA
244
PONTO DE VERIFICAÇÃO DE ARQUIVO DE TRANSIÇÃO DE PERSONA
246
ESCREVA NOVAS ASSINATURAS PARA ATIVOS DE PERSONA
248
LIBERE DADOS
250
DELETE ARQUIVO DE TRANSIÇÃO DEPERSONA
252
REINICIALIZE

FIG. 5

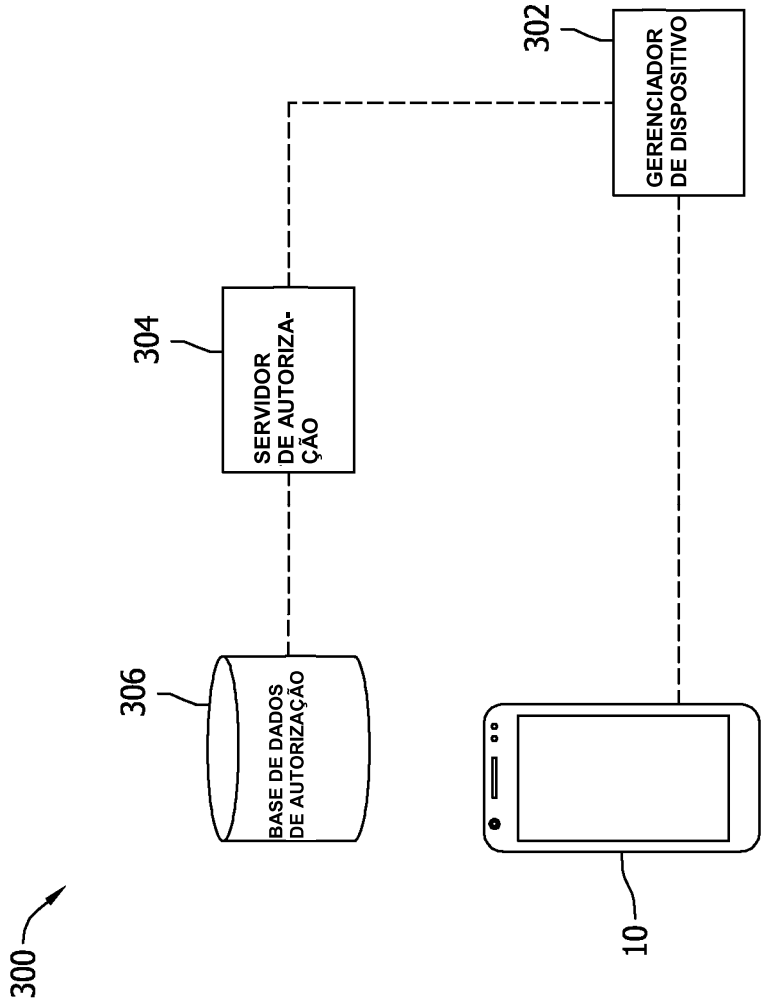
300
306
BASE DE DADOS DE AUTORIZAÇÃO
304
SERVIDOR DE AUTORIZA-ÇÃO
302
GERENCIADOR DE DISPOSITIVO
10

FIG. 6

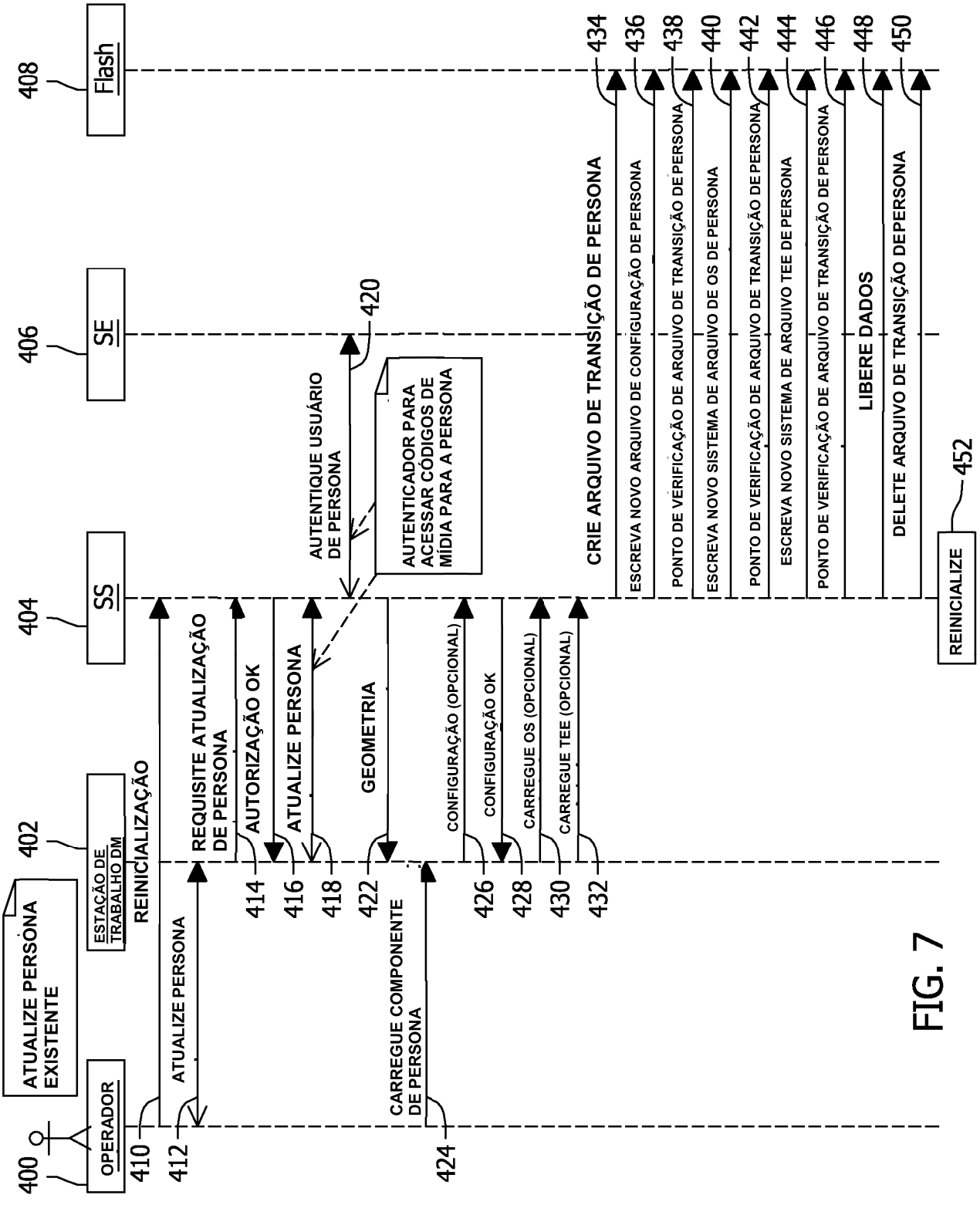
400
OPERADOR
ATUALIZE PERSONA EXISTENTE
402
ESTAÇÃO DE TRABALHO DM
404
SS
406
SE
408
Flash
410
REINICIALIZAÇÃO
412
ATUALIZE PERSONA
REQUISITE ATUALIZAÇÃO DE PERSONA
414
AUTORIZAÇÃO OK
416
ATUALIZE PERSONA
418
AUTENTIQUE USUÁRIO DE PERSONA
420
AUTENTICADOR PARA ACESSAR CÓDIGOS DE MÍDIA PARA A PERSONA
422
GEOMETRIA
424
CARREGUE COMPONENTE DE PERSONA
426
CONFIGURAÇÃO (OPCIONAL)
428
CONFIGURAÇÃO OK
430
CARREGUE OS (OPCIONAL)
432
CARREGUE TEE (OPCIONAL)
434
CRIE ARQUIVO DE TRANSIÇÃO DE PERSONA
436
ESCREVA NOVO ARQUIVO DE CONFIGURAÇÃO DE PERSONA
438
PONTO DE VERIFICAÇÃO DE ARQUIVO DE TRANSIÇÃO DE PERSONA
440
ESCREVA NOVO SISTEMA DE ARQUIVO DE OS DE PERSONA
442
PONTO DE VERIFICAÇÃO DE ARQUIVO DE TRANSIÇÃO DE PERSONA
444
ESCREVA NOVO SISTEMA DE ARQUIVO TEE DE PERSONA
446
PONTO DE VERIFICAÇÃO DE ARQUIVO DE TRANSIÇÃO DE PERSONA
448
LIBERE DADOS
450
DELETE ARQUIVO DE TRANSIÇÃO DEPERSONA
452
REINICIALIZE

FIG. 7

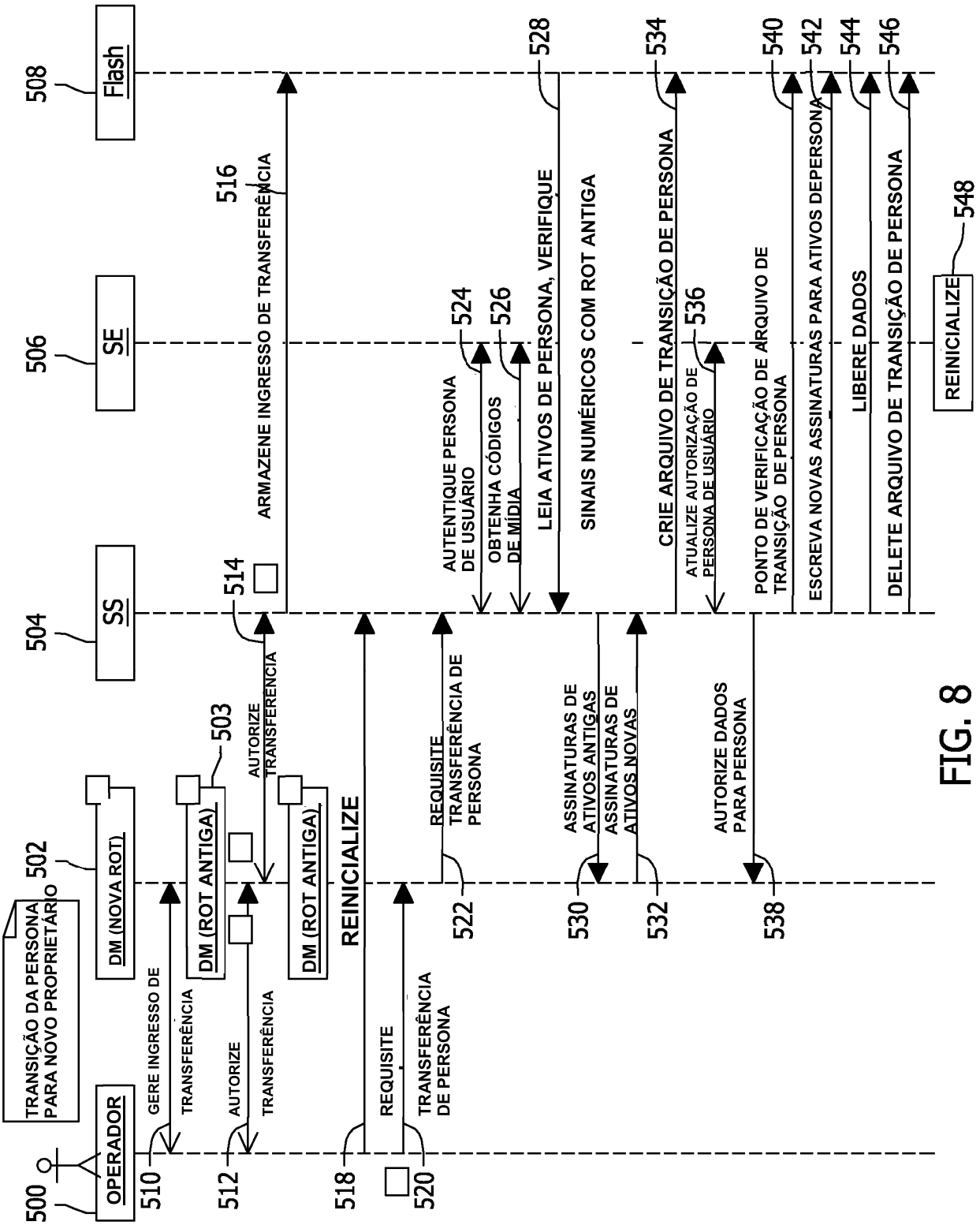
500
OPERADOR
TRANSIÇÃO DA PERSONA PARA NOVO PROPRIETÁRIO
502
DM (NOVA ROT)
503
DM (ROT ANTIGA)
DM (ROT ANTIGA)
504
SS
506
SE
508
Flash
510
GERE INGRESSO DE TRANSFERÊNCIA
512
AUTORIZE TRANSFERÊNCIA
514
AUTORIZE TRANSFERÊNCIA
516
ARMAZENE INGRESSO DE TRANSFERÊNCIA
518
REINICIALIZE
REQUISITE
520
TRANSFERÊNCIA DE PERSONA
REQUISITE TRANSFERÊNCIA DE PERSONA
522
524
AUTENTIQUE PERSONA DE USUÁRIO
526
OBTENHA CÓDIGOS DE MÍDIA
528
LEIA ATIVOS DE PERSONA, VERIFIQUE SINAIS NUMÉRICOS COM ROT ANTIGA
530
ASSINATURAS DE ATIVOS ANTIGAS
532
ASSINATURAS DE ATIVOS NOVAS
534
CRIE ARQUIVO DE TRANSIÇÃO DE PERSONA
536
ATUALIZE AUTORIZAÇÃO DE PERSONA DE USUÁRIO
538
AUTORIZE DADOS PARA PERSONA
540
PONTO DE VERIFICAÇÃO DE ARQUIVO DE TRANSIÇÃO DE PERSONA
542
ESCREVA NOVAS ASSINATURAS PARA ATIVOS DEPERSONA
544
LIBERE DADOS
546
DELETE ARQUIVO DE TRANSIÇÃO DE PERSONA
548
REINICIALIZE

FIG. 8

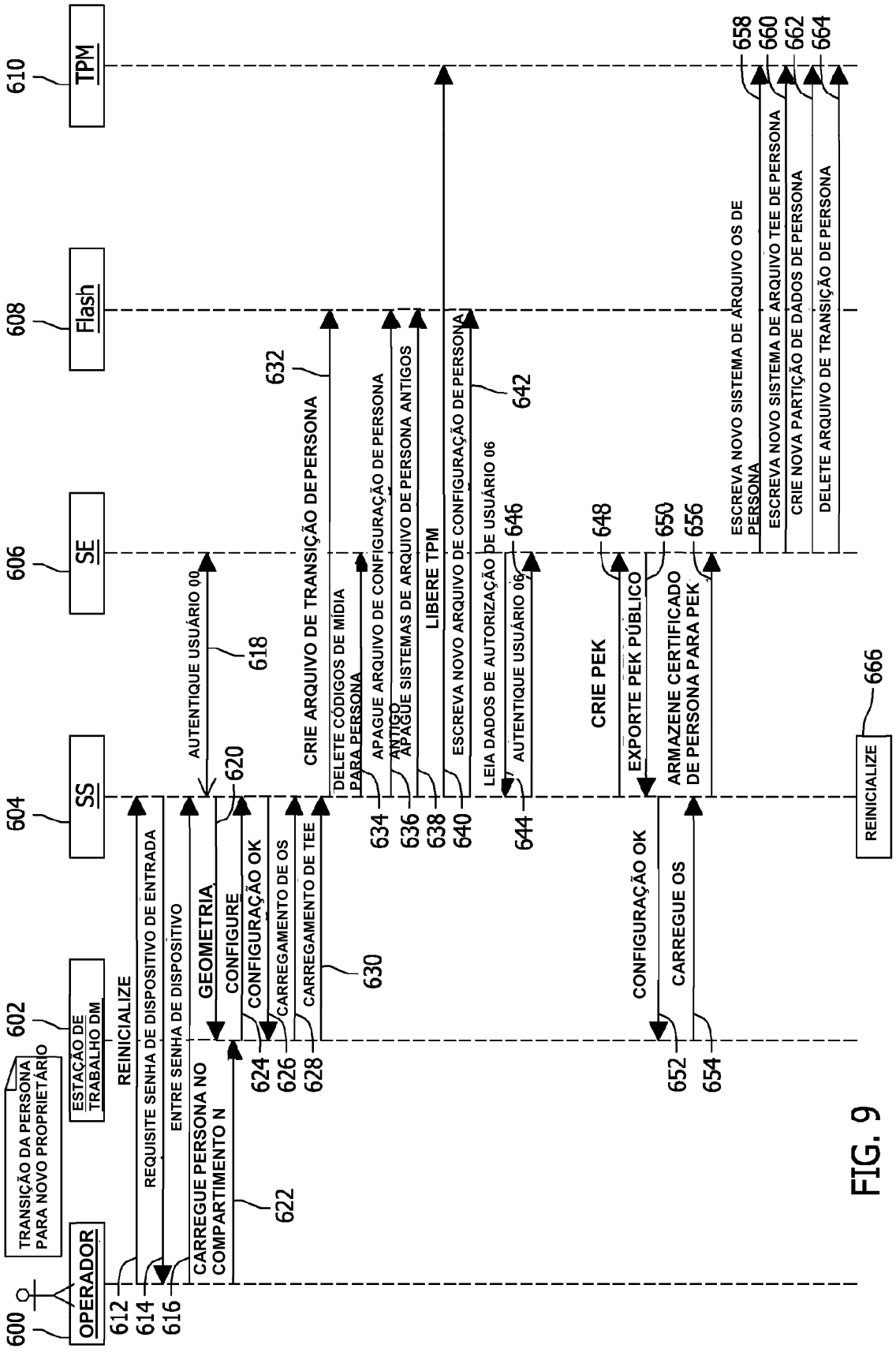
600
OPERADOR
602
ESTAÇÃO DE TRABALHO DM
TRANSIÇÃO DA PERSONA PARA NOVO PROPRIETÁRIO
604
SS
606
SE
608
Flash
610
TPM
612
REINICIALIZE
614
REQUISITE SENHA DE DISPOSITIVO DE ENTRADA
616
ENTRE SENHA DE DISPOSITIVO
CARREGUE PERSONA NO COMPARTIMENTO N
622
GEOMETRIA
CONFIGURE
620
CONFIGURAÇÃO OK
624
CARREGAMENTO DE OS
626
CARREGAMENTO DE TEE
628
630
AUTENTIQUE USUÁRIO 00
618
CRIE ARQUIVO DE TRANSIÇÃO DE PERSONA
632
DELETE CÓDIGOS DE MÍDIA PARA PERSONA
634
APAGUE ARQUIVO DE CONFIGURAÇÃO DE PERSONA ANTIGO
636
APAGUE SISTEMAS DE ARQUIVO DE PERSONA ANTIGOS
638
LIBERE TPM
640
ESCREVA NOVO ARQUIVO DE CONFIGURAÇÃO DE PERSONA
642
LEIA DADOS DE AUTORIZAÇÃO DE USUÁRIO 06
644
AUTENTIQUE USUÁRIO 06
646
CRIE PEK
648
EXPORTE PEK PÚBLICO
650
ARMAZENE CERTIFICADO DE PERSONA PARA PEK
656
CONFIGURAÇÃO OK
652
CARREGUE OS
654
ESCREVA NOVO SISTEMA DE ARQUIVO OS DE PERSONA
658
ESCREVA NOVO SISTEMA DE ARQUIVO TEE DE PERSONA
660
CRIE NOVA PARTIÇÃO DE DADOS DE PERSONA
662
DELETE ARQUIVO DE TRANSIÇÃO DE PERSONA
664
REINICIALIZE
666

FIG. 9