República Federativa do Brasil

Ministério do Desenvolvimento, Indústria, Comércio e Serviços

Instituto Nacional da Propriedade Industrial

(11) BR 112017014632-0 B1

(22) Data do Depósito: 27/01/2016

(45) Data de Concessão: 26/12/2023

(54) Título: MÉTODO IMPLEMENTADO POR COMPUTADOR, SISTEMA DE COMPUTADOR, E, MÍDIA LEGÍVEL DE COMPUTADOR

(51) Int.Cl.: H04L 9/08; H04L 9/30.

(30) Prioridade Unionista: 27/01/2015 US 62/108,468.

(73) Titular(es): VISA INTERNATIONAL SERVICE ASSOCIATION.

(72) Inventor(es): ERIC LE SAINT; SOUMENDRA BHATTACHARYA.

(86) Pedido PCT: PCT US2016015218 de 27/01/2016

(87) Publicação PCT: WO 2016/123264 de 04/08/2016

(85) Data do Início da Fase Nacional: 06/07/2017

(57) Resumo: MÉTODO IMPLEMENTADO POR COMPUTADOR, E, SISTEMA DE COMPUTADOR. As modalidades podem fornecer métodos para provisionamento de forma segura dos dados de credencial sensíveis, tais como uma chave de uso limitado (LUK) em um dispositivo do usuário. Em algumas modalidades, os dados de credencial podem ser criptografados usando uma chave de proteção de armazenamento separada e descriptografada somente no momento de uma transação para gerar um criptograma para a transação. Assim, a proteção end-to-end pode ser fornecida durante o trânsito e o armazenamento dos dados de credencial, limitar a exposição dos dados de credencial somente quando os dados de credencial forem necessários, reduzindo, assim, o risco de comprometimento dos dados de credencial.

MÉTODO IMPLEMENTADO POR COMPUTADOR, SISTEMA DE COMPUTADOR, E, MÍDIA LEGÍVEL DE COMPUTADOR

[001] O presente pedido é não-provisório e reivindica o benefício do Pedido Provisório U.S. nº 62/108.468, depositado em 27 de janeiro de 2015 (Número do dossier do advogado: 079900-0929835), incorporado neste documento por referência, em sua totalidade, para todos os propósitos. O presente recurso está relacionado ao Pedido de nº U.S. 14/841.589, depositado em 31 de agosto de 2015 (Número do dossier do advogado: 079900-0945228), que é incorporada por referência, para todos os efeitos em sua totalidade.

FUNDAMENTOS

[002] Conforme os dispositivos de usuário como celulares habilitados para NFC e cartões sem contato continuam a aumentar em popularidade, manter a segurança do pagamento e outras transações continua a ser uma preocupação. Por exemplo, a fim de realizar uma transação de pagamento, é normalmente necessário autenticar o dispositivo do usuário. Um método para autenticar um dispositivo do usuário é através do uso de um criptograma gerado pelo dispositivo. O criptograma é tipicamente gerado usando dados confidenciais de credencial, provisionados de um servidor. Se um invasor ganhar acesso aos dados confidenciais de credencial, ele potencialmente poderá forjar o criptograma. Assim, a segurança dos dados de credencial é essencial para a realização de transações seguras. No entanto, é um desafio fornecer uma proteção adequada dos dados de credencial durante a transmissão e armazenamento visto que invasores podem espionar as mensagens de provisionamento ou violar os dispositivos de usuário.

[003] As modalidades da presente invenção abordam esses problemas e outros problemas individual e coletivamente.

BREVE SUMÁRIO

[004] As modalidades referem-se aos sistemas e métodos para

provisionamento de forma segura de dados de credencial. As técnicas descritas neste documento podem fornecer proteção ponta-a-ponta (end-to-end) de dados de credencial sensíveis durante e após o processo de provisionamento, de modo a minimizar o risco de exposição dos dados de credencial.

[005] De acordo com algumas modalidades, é fornecido um método implementado por computador. Uma chave pública de cliente ou de usuário única pode ser determinada por um dispositivo de usuário. O dispositivo do usuário pode enviar uma mensagem de solicitação de provisionamento que inclui a chave pública efêmera para um computador servidor de provisionamento. Uma mensagem de resposta de provisionamento criptografada pode ser recebida através do dispositivo de usuário a partir do computador servidor de provisionamento, a mensagem de resposta de provisionamento criptografada compreendendo os dados de credencial criptografados. O dispositivo de usuário pode determinar um segredo compartilhado de resposta usando uma chave pública de servidor estática. O dispositivo de usuário pode determinar uma chave de sessão de resposta do segredo compartilhado de resposta, a chave de sessão de resposta utilizável para descriptografar a mensagem de resposta de provisionamento criptografada. O dispositivo de usuário pode descriptografar a mensagem de resposta de provisionamento criptografada usando a chave de sessão de resposta para determinar os dados de credencial criptografados. Um dispositivo de usuário pode ser determinado a partir de uma chave de proteção de armazenamento do segredo compartilhado de resposta, a chave de proteção de armazenamento sendo diferente da chave de sessão de resposta e utilizável para descriptografar os dados de credencial criptografados. A chave de proteção de armazenamento pode ser criptografada usando uma chave de criptografia de chave para gerar uma chave de proteção de armazenamento criptografada. A chave de proteção de armazenamento criptografada pode ser

armazenada. Os dados de credencial criptografados podem ser armazenados.

[006] Os dados de credencial podem incluir uma chave de uso limitado (LUK) ou dados de derivação de chave para uma chave de uso único (SUK). Os dados de credencial criptografados podem ser armazenados em um servidor de armazenamento conectado remotamente ao dispositivo de usuário e a chave de proteção de armazenamento criptografado pode ser armazenada no dispositivo de usuário.

[007] Em resposta a uma indicação para gerar um criptograma usado para autenticar uma mensagem de solicitação de autorização, os dados de credencial criptografados podem ser recuperados. A chave de proteção de armazenamento criptografada pode ser recuperada. A chave de proteção de armazenamento criptografada pode ser descriptografada usando a chave de criptografia de chave para obter a chave de proteção de armazenamento. Os dados de credencial criptografados podem ser descriptografados usando a chave de proteção de armazenamento para obter dados de credencial. E o criptograma pode ser gerado usando os dados de credencial. Em algumas modalidades, decifrar os dados de credencial criptografados que usam a chave da proteção de armazenamento compreendem derivar uma chave de criptografia de credencial usando a chave de proteção de armazenamento e os dados de derivação de chave para a chave de criptografia credencial, os dados de derivação de chaves compreendem dados específicos ao dispositivo de usuário e decifrar os dados de credencial criptografados usando a chave de criptografia de credencial. Em algumas modalidades, o criptograma é gerado usando uma chave de criptograma derivada dos dados de credencial.

[008] O dispositivo de usuário pode gerar um segredo compartilhado de solicitação usando uma chave privada de usuário correspondendo à chave pública de usuário avulsa e a chave pública de servidor estática. Os dados de solicitação podem ser criptografados usando o segredo compartilhado de solicitação para obter os dados de solicitação criptografados, em que a

mensagem de solicitação de provisionamento inclui os dados de solicitação criptografados.

[009] A mensagem de resposta de provisionamento pode incluir uma chave pública de servidor estática cega e o segredo compartilhado de resposta pode ser determinado usando a chave pública de servidor estática cega.

[0010] A determinação da chave pública de usuário avulsa pode compreender gerar um par de chaves de usuário efêmeras que compreendem uma chave privada de usuário efêmera e uma chave pública de usuário efêmera, onde a chave pública de usuário efêmero é usada como a chave pública de usuário avulsa. Em alternativa, a determinação da chave pública de usuário avulsa pode compreender cegar uma chave pública de usuário estática.

[0011] De acordo com algumas modalidades, é fornecido um método implementado por computador. Um computador servidor pode receber uma mensagem de solicitação de provisionamento a partir de um dispositivo de usuário incluindo uma chave pública de usuário avulsa. O segredo compartilhado de resposta pode ser gerado usando uma chave privada de servidor estática e chave pública de usuário avulsa. Os dados de credencial a ser incluídos em uma mensagem de resposta de provisionamento podem ser identificados. A chave de sessão de resposta pode ser determinada a partir do segredo compartilhado de resposta, a chave de sessão de resposta utilizável para criptografar a mensagem de resposta de provisionamento. Uma chave de proteção de armazenamento pode ser determinada a partir do segredo compartilhado de resposta, a chave de proteção de armazenamento sendo diferente da chave de sessão de resposta e utilizável para criptografar os dados de credencial. Os dados de credencial podem ser criptografados usando a chave de proteção de armazenamento para gerar os dados de credencial criptografados. A mensagem de resposta de provisionamento pode ser criptografa usando a chave de sessão de resposta para gerar a mensagem de

resposta de provisionamento criptografada, em que a mensagem de resposta de provisionamento inclui os dados de credencial criptografados. O computador servidor pode enviar uma mensagem de resposta de provisionamento criptografada ao dispositivo de usuário.

[0012] Os dados de credencial podem compreender uma LUK e dados de derivação de chave de criptograma utilizáveis para derivar uma chave de criptograma que é usada para gerar um criptograma.

[0013] A criptografia dos dados de credencial pode compreender a determinação de uma chave de criptografia de credencial usando a chave de proteção de armazenamento e dados de derivação de chaves, onde os dados de derivação de chave são específicos para o dispositivo de usuário. A mensagem de resposta de provisionamento pode incluir uma chave pública de servidor estática cega correspondente à chave privada de servidor estática.

[0014] De acordo com algumas modalidades, é fornecido um método implementado por computador. Uma chave pública de usuário avulsa pode ser determinada por um dispositivo de usuário. A chave pública de proteção de armazenamento pode ser determinada. Uma mensagem de solicitação de provisionamento pode ser enviada para um computador servidor de provisionamento, que inclui a chave pública de usuário avulsa e chave pública de proteção de armazenamento. Uma mensagem de resposta de provisionamento criptografada pode ser recebida a partir do computador servidor de provisionamento, a mensagem de resposta de provisionamento criptografada compreendendo dados de credencial criptografados, em que os dados de credencial criptografados são criptografados usando a chave pública de proteção de armazenamento. Um segredo compartilhado de resposta pode ser determinado usando uma chave pública de servidor estática. A chave de sessão de resposta pode ser determinada a partir do segredo compartilhado de resposta, a chave de sessão de resposta utilizável para descriptografar a mensagem de resposta de provisionamento criptografada. A mensagem de

resposta de provisionamento criptografada pode ser descriptografada usando a chave de sessão de resposta para determinar os dados de credencial criptografados. Os dados de credencial criptografados podem ser armazenados.

[0015] A chave pública de proteção de armazenamento e a chave pública de usuário avulsa podem corresponder a uma mesma chave privada de usuário. Alternativamente, a chave pública de proteção de armazenamento e a chave pública de usuário avulsa correspondem às chaves privadas de usuário diferentes.

[0016] Em resposta a uma indicação para gerar um criptograma usado para autenticar uma mensagem de solicitação de autorização, os dados de credencial criptografados podem ser recuperados. Os dados de credencial criptografados podem ser descriptografados usando uma chave privada de proteção de armazenamento correspondente à chave pública de proteção de armazenamento para obter os dados de credencial. O criptograma pode ser gerado usando os dados de credencial.

[0017] Outras modalidades são direcionadas aos sistemas, dispositivos de consumidor portáteis e mídia legível de computador associados aos métodos descritos aqui.

[0018] Uma melhor compreensão da natureza e as vantagens das modalidades da presente invenção podem ser adquiridas com referência à seguinte descrição detalhada e os desenhos que acompanham.

BREVE DESCRIÇÃO DAS FIGURAS

[0019] A FIG.1 mostra um sistema de pagamento de exemplo, de acordo com algumas modalidades.

[0020] A FIG.2 mostra um exemplo de um dispositivo de usuário, de acordo com algumas modalidades.

[0021] A FIG.3 mostra um computador servidor de exemplo, de acordo com algumas modalidades.

[0022] A FIG. 4 mostra uma vista em bloco em elevação de um processo de provisionamento de credencial segura, de acordo com algumas modalidades.

[0023] A FIG. 5 mostra um processo de exemplo para provisionar de forma segura os dados de credencial de um computador servidor, de acordo com algumas modalidades.

[0024] A FIG. 6 mostra outro processo de exemplo para provisionar de forma segura os dados de credencial de um computador servidor, de acordo com algumas modalidades.

[0025] A FIG. 7 mostra um exemplo de processo para usar os dados de credencial para realizar transações, de acordo com algumas modalidades.

[0026] A FIG. 8 mostra outro processo de exemplo para usar os dados de credencial para conduzir as transações, de acordo com algumas modalidades.

[0027] A FIG. 9 mostra um processo de exemplo para provisionamento com segurança de credencial a um dispositivo de usuário, de acordo com algumas modalidades.

[0028] A FIG. 10 mostra outro processo de exemplo para provisionamento com segurança de dados de credencial a um dispositivo do usuário, de acordo com algumas modalidades.

[0029] A FIG. 11 mostra um diagrama de fluxo de dados para provisionamento e usando os dados de credencial, de acordo com as modalidades.

[0030] A FIG. 12 mostra um primeiro exemplo de mensagem de solicitação de provisionamento e uma mensagem de resposta de provisionamento correspondente, de acordo com algumas modalidades.

[0031] A FIG. 13 mostra um segundo exemplo de uma mensagem de solicitação de provisionamento e uma mensagem de resposta de provisionamento correspondente, de acordo com algumas modalidades.

[0032] A FIG. 14 mostra um diagrama de bloco de nível elevado de um sistema de computador que pode ser usado para implementar qualquer uma das entidades ou componentes descritos acima.

TERMOS

[0033] Antes de discutir as modalidades da invenção, a descrição de alguns termos pode ser útil no entendimento de modalidades da invenção.

[0034] O termo "computador servidor" podem incluir um computador ou agrupamento de dispositivos de computação. Por exemplo, o computador servidor pode ser um mainframe grande, um agrupamento de minicomputadores ou um grupo de servidores que funciona como uma unidade. Em um exemplo, o computador servidor pode ser um servidor de banco de dados acoplado a um servidor da Web. O computador servidor pode ser acoplado a um banco de dados e pode incluir qualquer hardware, software, outra lógica ou combinação dos anteriores para atender as solicitações de um ou mais computadores de cliente (por exemplo, dispositivos de usuário). O computador servidor pode incluir um ou mais aparelhos computacionais e pode usar qualquer de uma variedade de estruturas, disposições e compilações de computação para atender as solicitações de um ou mais computadores de cliente.

[0035] O termo "par de chaves de público/privado" pode incluir um par de chaves criptográficas vinculadas gerada por uma entidade. A chave pública pode ser usada para funções públicas tais como criptografar uma mensagem para enviar para a entidade ou para verificar uma assinatura digital que supostamente foi feita pela entidade. A chave privada, por outro lado, pode ser utilizada para eventos privados como descriptografar uma mensagem recebida ou aplicar uma assinatura digital. A chave pública será geralmente ser autorizada por um elemento conhecido como Autoridade de Certificação (CA) que armazena a chave pública em um banco de dados e a distribui a qualquer outra entidade que o solicite. A chave privada será mantida

normalmente em um meio de armazenamento de segurança e será geralmente somente conhecido para a entidade. No entanto, os sistemas criptográficos descritos aqui podem caracterizar os mecanismos de recuperação de chave para recuperar as chaves perdidas e evitando a perda de dados. As chaves públicas e privadas podem estar em qualquer formato adequado, incluindo aquelas baseadas em RSA ou criptografia de curva elíptica (ECC).

[0036] A "assinatura digital" pode referir-se ao resultado da aplicação de um algoritmo com base em um par de chaves pública/privada, que permite que uma parte assinante se manifeste e uma parte verificadora verifique a autenticidade e a integridade de um documento. A parte assinante age por meio da chave privada e a parte verificadora age por meio da chave pública. Esse processo certifica-se a autenticidade do remetente, a integridade do documento assinado e o chamado princípio de não-repúdio, que não permite a renegar o que foi assinado. Um certificado ou outros dados que inclui uma assinatura digital por uma parte assinante é referido como sendo "assinado" pela parte assinante.

[0037] O "certificado" ou "certificado digital" pode incluir um documento eletrônico ou arquivo de dados que usa uma assinatura digital para vincular uma chave pública aos dados associados a uma identidade. O certificado pode incluir um ou mais campos de dados, tais como o nome civil da identidade, um número de série do certificado, uma data de válido-a-partir-de e válido-até para o certificado, as permissões relacionadas a certificados, etc. Um certificado pode conter uma data "válido-a-parti-de" que indica a primeira data em que o certificado é válido, e uma data de "válido-até" que indica a última data em que o certificado é válido. Um certificado também pode conter um hash dos dados no certificado que inclui os campos de dados. A menos que indicado do contrário, cada certificado é assinado por uma autoridade de certificação.

[0038] Uma "autoridade de certificação" (CA) pode incluir um ou

mais computadores de servidor operativamente acoplados para emitir certificados para as entidades. A CA pode fornecer sua identidade usando um certificado de CA, que inclui a chave pública da CA. O certificado da CA pode ser assinado pela chave privada de outra CA ou pode ser assinado pela mesma chave privada da CA. Esse último é conhecido como um certificado auto assinado. A CA pode manter um banco de dados de todos os certificados emitidos pela CA e também pode manter uma lista de certificados revogados.

[0039] Em um processo típico, a autoridade de certificação recebe um certificado não assinado de uma entidade cuja identidade é conhecida. O certificado não assinado inclui uma chave pública, um ou mais campos de dados e uma hash dos dados no certificado. A CA assina o certificado com uma chave privada correspondente à chave pública incluída no certificado CA. A CA pode então armazenar o certificado assinado em um banco de dados e emitir o certificado assinado à entidade.

[0040] O "nonce criptográfico" pode incluir qualquer número, sequência, sequência de bits ou outro valor de dados destinados a ser utilizados em associação com uma sessão de comunicação única. Em alguns casos, um nonce criptográfico pode ser aleatoriamente ou pseudo-aleatoriamente gerado. Por exemplo, o nonce criptográfico pode ser um número aleatório. Normalmente, um nonce criptográfico é de comprimento suficiente a tornar insignificante a probabilidade de gerar independentemente várias vezes o mesmo valor de nonce.

[0041] A "chave cega", tal como uma "chave pública cega" pode incluir uma chave que foi ofuscada ou alterada do valor original pela combinação com outro elemento de dados, como um nonce criptográfico. Por exemplo, na criptografia de curva elíptica, uma chave pública pode ser multiplicada pelo nonce para gerar uma "chave pública cega". Da mesma forma, uma chave privada pode ser multiplicada pelo nonce para gerar uma "chave privada cega".

[0042] A "chave avulsa" refere-se a uma chave que é fornecida para uma única vez. Uma chave avulsa pode incluir uma chave de um par de chave efêmera, como descrito abaixo. Em algumas modalidades, as chaves avulsas podem incluir chaves cegas que são geradas usando a mesma chave estática (por exemplo, uma chave pública estática), mas ocultada usando nonce criptográfico diferente, o fator de identificação ou outros fatores de ocultamento.

[0043] Um "par de chaves efêmeras" pode incluir uma chave pública (isto é, uma "chave pública efêmera") e uma chave privada (isto é, uma "chave privada efêmera") geradas para uso com uma única transação ou outra sessão de comunicação. O par de chaves efêmeras pode ser de qualquer formato adequado, tal como ECC ou RSA. Normalmente, um par de chaves efêmeras pode ser excluído, uma vez que a sessão de comunicação ou transação terminou.

[0044] O "par de chaves estáticas" pode incluir uma chave pública (isto é, uma "chave pública estática") e uma chave privada (isto é, uma "chave privada estática") mantidas durante um período de tempo. Normalmente, embora não necessariamente, uma chave privada estática pode ser armazenada com segurança, tal como em um módulo de segurança de hardware (HSM) ou elemento de segurança (SE). Tipicamente, embora não necessariamente, uma chave pública estática pode ser vinculada a uma identidade através do uso de um certificado digital. O par de chaves estáticas pode ser de qualquer formato adequado, tal como ECC ou RSA.

[0045] Um "segredo compartilhado" pode incluir qualquer valor de dados ou outras informações conhecidas apenas a partes autorizadas em uma comunicação segura. Um segredo compartilhado pode ser gerado de forma adequada, a partir de quaisquer dados adequados. Por exemplo, um algoritmo com base em Diffie-Hellman, tal como Curva Elíptica de Diffie-Hellman (ECDH) pode ser usado para gerar um segredo compartilhado de uma chave

privada e uma chave pública. Em alguns casos, um segredo compartilhado pode ser usado para gerar uma chave de sessão.

[0046] O termo "dados de identificação" pode incluir quaisquer dados ou informações associadas a um usuário ou dispositivo. Exemplos de dados de identificação podem incluir um nome de um usuário associado ao dispositivo, uma organização associada ao dispositivo, as informações de pagamento tais como Número da Conta Principal (PAN) ou token associado ao dispositivo, uma data de expiração do PAN ou token, um certificado associado ao dispositivo, um IMEI ou número de série de dispositivo, etc.

[0047] O termo "dados de autenticação" pode incluir quaisquer dados ou informações adequadas para autenticar um usuário ou dispositivo. Exemplos de dados de autenticação podem incluir uma senha ou frase-chave, uma chave de criptografia (por exemplo, uma chave privada), um certificado, dados biométricos associados a um usuário (por exemplo, impressão digital, voz, imagem facial, verificação de retina/íris) e similares.

[0048] Um "fator de identificação" pode incluir quaisquer dados ou informações determinados a partir de dados de identificação e/ou dados de autenticação. Tipicamente, embora não necessariamente, o fator de identificação pode ser gerado por meio de hash de uma combinação de dados de identificação e dados de autenticação.

[0049] Uma "chave de encriptação" podem incluir qualquer valor de dados ou outras informações adequadas para codificar de forma criptografada os dados. Uma "chave de descriptografia" pode incluir qualquer valor de dados ou outras informações adequadas para descriptografar os dados criptografados. Em alguns casos, a mesma chave usada para criptografar os dados pode ser operável para descriptografar os dados. Essa chave pode ser conhecida como uma chave de criptografia simétrica.

[0050] Uma "chave de sessão" pode incluir qualquer chave usada para criptografar ou descriptografar os dados a serem comunicadas de forma

segura. Em alguns casos, uma chave de sessão pode ser gerada a partir um segredo compartilhado conhecido ambos para uma entidade de envio e uma entidade receptora. Por exemplo, a chave de sessão pode ser derivada usando uma função de derivação de chave e o segredo compartilhado. Uma chave de sessão pode ser usada para proteger os dados incluídos em uma mensagem de solicitação ou resposta. Em tais casos, uma chave de sessão também pode ser referida como uma chave de proteção de mensagem.

[0051] "Credenciais" ou "dados de credencial" pode incluir quaisquer dados que são provisionados de um servidor a um dispositivo de usuário (por exemplo, dispositivo móvel) que permita que o dispositivo de usuário realize transações (por exemplo, operações de pagamento). Os exemplos de dados de credencial podem incluir tokens, PAN ou outras informações de conta, uma ou mais chaves (por exemplo, LUKs usadas para gerar criptogramas, chaves públicas estáticas cegas ou não cegas, etc.), parâmetros de derivação de chave (por exemplo, para derivar uma SUK que é usada gerar um criptograma, uma chave secreta compartilhada, uma chave de criptografia, etc.), parâmetros de derivação de chave, as informações de cadeia de certificados, parâmetros de transação e todos os outros dados apropriados.

[0052] Uma "chave de proteção de armazenamento" ou "chave de proteção de credencial" pode incluir uma chave de criptografia que é usada para proteger os dados de credencial ou quaisquer outros dados confidenciais. Por exemplo, a chave de proteção de armazenamento pode ser usada diretamente para criptografar ou descriptografar os dados de credencial. Uma chave de proteção de armazenamento também pode ser usada indiretamente para criptografar ou descriptografar os dados de credencial. Por exemplo, a chave de proteção de armazenamento pode ser usada para derivar outra chave de criptografia que é usada para criptografar ou descriptografar os dados de credencial. Em algumas modalidades, a chave de proteção de armazenamento pode incluir um par de chave pública/privada. A chave pública pode ser usada

para criptografar os dados de credencial, enquanto que a chave privada pode ser usada para descriptografar os dados de credencial.

[0053] A "chave de uso limitado" (LUK) pode incluir qualquer chave de criptografia ou outros dados que possam ser usados um número limitado de vezes. Uma LUK pode ser usado para qualquer propósito adequado. Por exemplo, em algumas modalidades, um LUK pode ser usado para gerar um criptograma para uma transação.

[0054] A "chave de uso único" (SUK) é uma LUK que pode ser usada apenas uma vez. Por exemplo, uma SUK pode ser usado para criptografar ou descriptografar dados relacionados a uma única transação. Em algumas modalidades, uma SUK pode ser derivada de uma LUK.

[0055] Um "criptograma" pode incluir qualquer elemento de dados ou outras informações usadas para autenticar uma entidade como um dispositivo ou um usuário. Por exemplo, um criptograma pode incluir dados estáticos (isto é, pré-determinados), dados dinâmicos ou uma combinação dos dois que são criptografados usando uma chave de encriptação (por exemplo, um LUK). Um criptograma pode ser usado em qualquer contexto apropriado. Por exemplo, um "criptograma de registro" pode incluir um criptograma que é usado para confirmar o registro de uma entidade. Um "criptograma de transação" pode incluir um criptograma que é usado para autenticar uma entidade que realiza uma transação.

DESCRIÇÃO DETALHADA

[0056] As modalidades podem fornecer métodos para provisionamento de forma segura dos dados de credencial sensíveis, tais como uma chave de uso limitado (LUK) em um dispositivo do usuário. Em algumas modalidades, os dados de credencial podem ser criptografados usando uma chave de proteção de armazenamento separada e descriptografada somente no momento de uma transação para gerar um criptograma para a transação. Assim, a proteção end-to-end pode ser

fornecida durante o trânsito e o armazenamento dos dados de credencial, limitar a exposição dos dados de credencial somente quando os dados de credencial forem necessários, reduzindo, assim, o risco de comprometimento dos dados de credencial.

[0057] Por exemplo, em uma modalidade, um dispositivo de usuário pode determinar uma chave pública de usuário avulsa e enviar uma mensagem de solicitação de provisionamento incluindo a chave pública de usuário avulsa para um computador servidor de provisionamento. O computador servidor de provisionamento pode identificar os dados de credencial (por exemplo, LUK) a serem incluídos em uma mensagem de resposta de provisionamento. O computador servidor pode gerar um segredo compartilhado de resposta a chave pública de usuário avulsa e uma chave privada de servidor estática. O segredo compartilhado de resposta pode ser usado determinar uma chave de sessão de resposta e uma chave da proteção de armazenamento. A chave de proteção de armazenamento pode ser usada para criptografar os dados de credencial para gerar os dados de credencial criptografados. Os dados de credencial criptografados podem ser incluídos na mensagem de resposta de provisionamento. A mensagem de resposta de provisionamento pode ser criptografada usando a chave de sessão de resposta e enviada ao dispositivo de usuário.

[0058] O dispositivo de usuário pode derivar um segredo compartilhado de resposta usando uma chave pública de servidor estática e uma chave privada de usuário correspondendo à chave pública de usuário. O dispositivo de usuário pode determinar uma chave de sessão de resposta do segredo compartilhado de resposta e descriptografar a mensagem de resposta de provisionamento criptografa usando a chave de sessão de resposta para determinar os dados de credencial criptografados. O dispositivo de usuário também pode determinar a chave de proteção de armazenamento do segredo compartilhado de resposta. Os dados de credencial criptografados podem ser

armazenados como é, sem ser descriptografado, no dispositivo de usuário ou um provedor de armazenamento externo. A chave de proteção de armazenamento também pode opcionalmente ser cifrada antes de ser armazenada.

[0059] No momento de uma transação, os dados de credencial criptografados podem ser obtidos e descriptografados usando a chave de proteção de armazenamento. Os dados de credencial descriptografados podem ser usados gerar um criptograma que possa ser usado para conduzir uma transação.

[0060] Consequentemente, a proteção end-to-end pode ser fornecida para os dados de credencial sensíveis. Os dados de credencial se mantêm criptografados durante a transmissão, de modo que mesmo que um invasor intercepte a mensagem de solicitação de provisionamento, o mesmo não será capaz de decifrar os dados de credencial sem o acesso à chave de proteção de armazenamento. Além disso, os dados de credencial permanecem criptografados em repouso, de modo que no evento improvável que o dispositivo de armazenamento (por exemplo, dispositivo de usuário) seja comprometido, os dados de credencial são protegidos dos invasores. Uma vez que os dados de credencial são armazenados em um formato criptografado, um invasor não poderia fazer uso dos dados de credencial, a menos que o invasor também tivesse posse da chave de proteção de armazenamento. Além disso, algumas modalidades podem armazenar a chave de proteção de armazenamento e os dados de credencial criptografados em locais diferentes. Por exemplo, a chave de proteção de armazenamento pode ser armazenada em um elemento de segurança. Tais modalidades podem, ainda, atenuar o risco de um compromisso.

[0061] Além disso, algumas modalidades podem provisionar os dados de credencial criptografados em um dispositivo de usuário anteriormente não autenticado usando apenas duas mensagens: uma mensagem de solicitação de

provisionamento de um dispositivo de usuário e uma mensagem de resposta de provisionamento ao dispositivo de usuário. Assim, as modalidades podem fornecer os benefícios acima quando reduzirem o tempo e processar necessário para provisão do dispositivo de usuário. Os exemplos acima destacam somente algumas das vantagens fornecidas pelas modalidades da invenção.

I. Sistemas

[0062] As modalidades são utilizáveis com vários sistemas de autorização, por exemplo, sistemas de pagamentos, sistema de acesso de documentos, sistema de acesso de construção e similares. Embora os exemplos dos sistemas de pagamento sejam descritos, as modalidades serão igualmente aplicáveis a outros sistemas de autorização.

A. Sistema de Pagamento

[0063] A FIG.1 mostra um sistema de pagamento de exemplo 100, de acordo com algumas modalidades. O sistema é composto por um usuário (não mostrado) que pode operar um dispositivo do usuário 101. O usuário poderá usar o dispositivo do usuário 101 para realizar transações de pagamento em comunicação com um dispositivo de acesso 102. Como usado aqui, um "dispositivo do usuário" pode incluir um computador do tipo desktop, computador do tipo laptop, celular, tablet, cartão de crédito, cartão de débito ou qualquer dispositivo de computação apropriado. Como usado aqui, um "dispositivo de acesso" pode incluir qualquer dispositivo de computação, tais como um terminal de ponto de venda (POS) ou servidor da web, adequado para se comunicar com um dispositivo do usuário. Em algumas modalidades, o dispositivo de acesso 102 pode se comunicar diretamente com o dispositivo do usuário 101. Em outras modalidades, o dispositivo de acesso 102 pode comunicar-se ao dispositivo do usuário 101 através de um dispositivo de interface, como um relógio inteligente, óculos inteligentes ou qualquer outro dispositivo adequado. O dispositivo de acesso 102 pode ser conectado ao

computador do vendedor 103, que pode ser conectado ao computador do adquirente 104. O computador do adquirente 104 pode estar conectado ao computador do emissor 106 através da rede de processamento de pagamento 105. O dispositivo do usuário 101 pode, opcionalmente, se comunicar com um dispositivo de armazenamento 107 que pode ser conectado de forma operável para o dispositivo do usuário 101. O dispositivo de armazenamento 107 pode incluir ou ser incluído em qualquer servidor de armazenamento de dados local ou remoto adequado, sistema ou serviço seja fornecido por um provedor de armazenamento. O provedor de armazenamento pode não ser a mesma entidade que fornece os dispositivos 101-106. Por exemplo, o dispositivo de armazenamento 107 pode ser parte de um serviço de armazenamento baseado em nuvem fornecido por um provedor de armazenamento em nuvem externo. Qualquer um ou todos os dispositivos 101-107 podem ser implementados usando um ou mais dispositivos de computação, tais como computadores de servidor.

[0064] Como usado aqui, um "emissor" normalmente pode se referir a uma entidade empresarial (por exemplo, um banco) que mantém contas financeiras para um usuário e muitas vezes emite ou provisiona um dispositivo do usuário 101, como um dispositivo móvel, ou cartão de débito ou crédito para o usuário. Um "vendedor" normalmente é uma entidade que se envolve em transações e pode vender bens ou serviços. Um "adquirente" é normalmente uma entidade empresarial (por exemplo, um banco comercial) que tem uma relação de negócios com um comerciante em particular ou outra entidade. Algumas entidades podem executar ambas as funções de emissor e adquirente. Algumas modalidades podem abranger tais entidades únicas emissoras-adquirentes. Cada uma das entidades pode compreender um ou mais aparelhos computadores (por exemplo, dispositivo de acesso 102, computador do vendedor 103, computador do adquirente 104, rede de processamento de pagamento 105 e computador do emissor 106) para permitir

comunicação ou para realizar uma ou mais das funções descritas no presente documento.

[0065] A rede de processamento de pagamento 105 pode incluir subsistemas de processamento de dados, redes e operações usadas para suportar e fornecer serviços de autoridade de certificado, serviços de autorização, serviços de arquivo de exceção, serviços de contabilização de transação e serviços compensação e liquidação. Uma rede de processamento de pagamento de exemplo pode incluir VisaNet™. As redes de processamento de pagamento como VisaNet™ são capazes de processar transações de cartão de crédito, transações de cartão de débito e outros tipos de transações comerciais. VisaNet™, em particular, inclui um sistema de VIP (Sistema de Pagamentos Integrado Visa (Visa Integrated Payments system) que processa solicitações de autorização e um sistema de Base II que executa serviços de compensação e liquidação.

[0066] A rede de processamento de pagamento 105 pode incluir um ou mais computadores de servidor. Um computador servidor é tipicamente um computador poderoso ou um agrupamento de computadores. Por exemplo, o computador servidor pode ser um mainframe grande, um agrupamento de minicomputadores ou um grupo de servidores que funciona como uma unidade. Em um exemplo, o computador servidor pode ser um servidor de banco de dados acoplado a um servidor da Web. A rede de processamento de pagamento 105 pode usar qualquer rede com fio ou sem fio adequada, incluindo a Internet.

[0067] Em algumas transações de pagamento, o usuário adquire um bem ou serviço em um comerciante usando um dispositivo do usuário 101. O dispositivo do usuário 101 pode interagir com um dispositivo de acesso 102 em um comerciante associado ao computador do vendedor 103. Por exemplo, o usuário pode tocar o dispositivo do usuário 101 contra um leitor NFC no dispositivo de acesso à 102. Como alternativa, o usuário pode indicar detalhes

de pagamento ao vendedor através de uma rede de computador, tal como em uma transação on-line ou comércio eletrônico.

[0068] Uma mensagem de solicitação de autorização para uma transação pode ser gerada pelo dispositivo de acesso 102 ou computador do vendedor 103 e, em seguida, encaminhada ao computador do adquirente 104. Após receber a mensagem de solicitação de autorização, o computador do adquirente 104 envia a mensagem de solicitação de autorização para a rede de processamento de pagamento 105. A rede de processamento de pagamento 105, em seguida, encaminha a mensagem de solicitação de autorização para o computador do emissor correspondente 106 associado a um emissor associado ao usuário ou dispositivo do usuário 101.

[0069] Uma "mensagem de solicitação de autorização" pode ser uma mensagem eletrônica que é enviada para uma rede de processamento de pagamento e/ou um emissor para solicitar a autorização para uma transação. Uma mensagem de solicitação de autorização de acordo com algumas modalidades pode cumprir a norma ISO 8583, que é um padrão para sistemas que trocam informações de transação eletrônica associadas a um pagamento feito por um usuário usando um dispositivo de pagamento ou conta de pagamento. A mensagem de solicitação de autorização pode incluir um identificador de conta de emissor pode ser associado a um dispositivo de pagamento ou a conta de pagamento. Uma mensagem de solicitação de autorização também pode incluir elementos de dados adicionais correspondentes às "informações de identificação" incluindo, a título de exemplo apenas: um código de serviço, um CVV (valor de verificação de cartão), um dCVV (valor de verificação de cartão dinâmico), uma data de validade, etc. Uma mensagem de solicitação de autorização também pode incluir "informações de transações", tal como qualquer informações associadas a uma transação atual, tais como quantidade de transação, identificador de vendedor, local do vendedor, valor de transação, etc., assim

como quaisquer outras informações que podem ser utilizadas para determinar se identificar e/ou autorizar uma transação. A mensagem de solicitação de autorização também pode incluir outras informações, tais como informações que identificam o dispositivo de acesso que gerou a mensagem de solicitação de autorização, as informações sobre a localização do dispositivo de acesso, etc.

[0070] Depois do computador do emissor 106 recebe a mensagem de solicitação de autorização, o computador do emissor 106 envia uma mensagem de resposta de autorização para a rede de processamento de pagamento 105 para indicar se a transação atual foi autorizada (ou não autorizada). A rede de processamento de pagamentos 105, em seguida, encaminha a mensagem de resposta de autorização de volta para o computador do adquirente 104. Em algumas modalidades, a rede de processamento de pagamento 105 pode recusar a transação, mesmo se o computador do emissor 106 autorizou a transação, por exemplo, dependendo um valor da pontuação de risco de fraude. O computador do adquirente 104, em seguida, envia a mensagem de resposta de volta ao computador do vendedor 103.

[0071] Uma "mensagem de resposta de autorização" pode ser uma resposta de mensagem eletrônica a uma mensagem de solicitação de autorização gerada por um computador do emissor 106 e/ou uma rede de processamento de pagamento 105. A mensagem de resposta de autorização pode incluir, a título de exemplo, um ou mais dos indicadores de status a seguir: Aprovação -- a transação foi aprovada; Recusa -- a transação não foi aprovada; ou Call Center - resposta pendendo de mais informações, vendedor deve ligar para o número de telefone de autorização gratuito. A mensagem de resposta de autorização também pode incluir um código de autorização, que pode ser um código que um emissor retorna em resposta a uma mensagem de solicitação de autorização em uma mensagem eletrônica (diretamente ou

através da rede de processamento de pagamento 105) para o computador do vendedor 103 que indica aprovação da transação. O código pode servir como prova de autorização. Tal como acima referido, em algumas modalidades, uma rede de processamento de pagamento 105 pode gerar ou encaminhar a mensagem de resposta de autorização para o vendedor, normalmente através do computador do adquirente 104.

[0072] Depois que o computador do vendedor 103 recebe a mensagem de resposta de autorização, o computador do vendedor 103 pode, então, fornecer a mensagem de resposta de autorização ao usuário. A mensagem de resposta pode ser exibida pelo dispositivo de acesso 102 ou pode ser impressa em um recibo físico. Alternativamente, se a transação for uma transação on-line, o vendedor pode fornecer uma página da web ou outra indicação da mensagem de resposta de autorização, tal como um recibo virtual. Os recibos podem incluir dados de transação para a transação.

[0073] No final do dia, um processo de compensação e liquidação normal pode ser realizado pela rede de processamento de pagamento 105. Um processo de compensação é um processo de troca de detalhes financeiros entre um adquirente e um emissor para facilitar a postagem para a conta de pagamento do cliente e reconciliação da posição de liquidação do usuário.

B. Dispositivo do Usuário

[0074] A FIG.2 mostra um exemplo de um dispositivo de usuário 200, de acordo com algumas modalidades. Por exemplo, o dispositivo do usuário 200 pode incluir ou ser incluído no dispositivo do usuário 101 descrito na FIG. 1. Os exemplos de dispositivos de usuário 200 podem incluir celulares, tablets, computadores do tipo desktop e laptop, dispositivos vestíveis (por exemplo, relógios inteligentes, faixas de fitness, pulseiras de tornozelo, anéis, brincos, etc.) ou quaisquer outros dispositivos de computação capazes de receber, armazenar e transmitir dados. O dispositivo do usuário 200 pode ser configurado para comunicar-se diretamente ou indiretamente com um

computador servidor 300 para implementar os métodos descritos neste documento. O dispositivo do usuário 200 pode incluir um processador 201 acoplado de forma comunicativa a uma interface de rede 202, uma memória 203, um meio legível por computador 210 e, opcionalmente, um elemento de segurança 204.

[0075] O processador 201 pode abranger um ou mais CPUs, cada um dos quais pode incluir pelo menos um núcleo de processador operável para executar os componentes do programa para a execução de solicitações geradas por usuário e/ou sistema. A CPU pode ser um microprocessador, tal como da AMD Athlon, Duron e/ou Opteron; IBM e/ou PowerPC da Motorola; Processador de Celular da IBM e da Sony; Intel Celeron, Itanium, Pentium, Xeon e/ou XScale; e/ou processador(es) similar(es). A CPU interage com memória através de sinal que passas através dos conduítes condutores para executar o código de programa de sinal armazenado de acordo com as técnicas de processamento de dados convencionais. Em alguns casos, o processador 201 pode incluir múltiplos CPUs acoplados em uma rede, tais como em um sistema de computação distribuído ou em cluster.

[0076] A interface de rede 202 pode ser configurada para permitir que o dispositivo 200 se comunique com outras entidades tais como dispositivos 101-107, outros dispositivos de computação de computação, etc. usando uma ou mais redes de comunicações. As interfaces de rede podem aceitar, se comunicar e/ou conectar a uma rede de comunicações. As interfaces de rede podem empregar protocolos de conexão, tais como, mas não se limitando a: conexão direta, Ethernet (grosso, fino, par trançado 10/100/1300 Base T e/ou similares), Token Ring, conexão sem fio tal como IEEE 802.11a-x e/ou similares. Uma rede de comunicações pode ser qualquer um e/ou a combinação dos seguintes: uma interconexão direta; a Internet; uma Rede de Área Local (LAN); uma Rede de Área Metropolitana (MAN); uma conexão personalizada segura; uma Rede de Área Ampla (WAN); uma rede sem fio

(por exemplo, empregando protocolos tais como, mas não se limitando a, um Wireless Application Protocol (WAP), I-mode e/ou similares); e/ou similares.

[0077] A memória 203 pode ser usada para armazenar dados e código. A memória 203 pode ser acoplada ao processador 201 interna ou externamente (por exemplo, armazenamento de dados com base em nuvem) e pode incluir qualquer combinação de memória volátil e/ou não-volátil, tais como RAM, DRAM, ROM, flash ou qualquer outro dispositivo de memória adequado.

[0078] O elemento de segurança 204 pode incluir um módulo resistente a adulteração capaz de hospedar de forma segura os aplicativos e/ou dados confidenciais. Tais aplicativos e/ou dados podem estar relacionados com as solicitações de pagamento, autenticação/autorização, gerenciamento de chave criptográfica e similares. Por exemplo, algumas ou todas as porções de credenciais, chaves criptográficas ou os principais materiais, criptogramas, compartilhou segredos, informações de conta e similares, podem ser configurados para o elemento de segurança 204 o dispositivo do usuário 200 para proteger contra acesso não autorizado. Em algumas modalidades, o elemento de segurança 204 poderá incluir ou ser incluído em qualquer combinação de módulos de segurança com base em software (tais como a emulação de cartão de host ou HCE) e/ou com base em hardware (tal como um módulo de segurança de hardware ou HSM, um cartão inteligente ou cartão chip).

[0079] O meio legível por computador 210 pode ser sob a forma de uma memória (por exemplo, flash, ROM, etc.) e pode incluir código executável pelo processador 201 para implementar os métodos descritos neste documento. O meio legível por computador 210 pode incluir um módulo de autenticação 211, um módulo de criptografia 212 e um módulo de aplicação 213. Em várias modalidades, esses módulos podem ser configurados para executar, individual ou coletivamente, alguns ou todos dos métodos 400,

1100, 1400, 1200, 1300, 1700, 11100 de FIGS. 4-5, 8, 11, 12, 15, e 18, respectivamente.

[0080] O módulo de autenticação 211 pode incluir qualquer programa, software ou outro código apropriado para autenticar o dispositivo de computação 200 a outro dispositivo de computação ou autenticar outro dispositivo de computação no dispositivo de computação 200. Por exemplo, o módulo de autenticação 211 pode ser configurado para gerar e enviar uma mensagem de solicitação de autenticação para outro dispositivo de computação e receber e processar uma mensagem de resposta de autenticação de outros dispositivos de computação. Da mesma forma, o módulo de autenticação 211 pode ser configurado para receber e processar uma mensagem de solicitação de autenticação de outro dispositivo de computação e gerar e enviar uma mensagem de resposta de autenticação para o outro dispositivo de computação.

[0081] O módulo de criptografia 212 pode incluir qualquer programa, software ou outro código apropriado para executar operações relacionadas a criptografia ou descriptografia. Por exemplo, o módulo de criptografia pode ser configurado para gerar um segredo compartilhado, como o uso de um protocolo de acordo de chave, tal como o Diffie-Hellman. O módulo de criptografia 212 pode ser ainda mais configurado para derivar uma chave de sessão ou chave de proteção de armazenamento de um segredo compartilhado, como o uso de uma função de derivação de chave (KDF). Em algumas modalidades, o módulo de criptografia 212 pode ser configurado para armazenar uma ou mais chaves estáticas, tal como uma chave privada de dispositivo de usuário estática ou uma chave privada de servidor estática. Em algumas modalidades, o módulo de criptografia 212 pode ser implementado usando qualquer combinação de software (como a emulação do cartão de host ou HCE) e hardware (como um módulo de hardware de segurança ou HSM).

[0082] O módulo de aplicação 213 pode incluir qualquer programa,

software ou outro código apropriado para executar um ou mais aplicativos. Por exemplo, o módulo de aplicação 213 pode incluir uma solicitação de pagamento operável para realizar uma transação de pagamento. Em algumas modalidades, a solicitação de pagamento pode ser configurada para permitir que um usuário selecione bens e serviços a serem comprados, obter credenciais seguras (por exemplo, uma chave de criptograma) de um emissor de uma conta de pagamento e/ou iniciar ou conduzir uma transação de pagamento (por exemplo, usando as credenciais de segurança).

[0083] Entende-se que os componentes descritos aqui são apenas para fins ilustrativos e não se destinam a serem um fator limitante. Em várias modalidades, mais ou menos componentes do que os listados aqui podem ser fornecidos. Por exemplo, em uma modalidade, o dispositivo do usuário 200 pode não incluir um elemento de segurança 204. Em tal modalidade, os dados confidenciais ou sensíveis (por exemplo, as chaves criptográficas) podem ser armazenados (por exemplo, em formato criptografado) em e/ou recuperados de um dispositivo de armazenamento 107 conectado de forma operável ao dispositivo do usuário 200. Em algumas modalidades, o dispositivo do usuário 200 não pode incluir um módulo de aplicação 213.

C. Computador servidor

[0084] A FIG.3 mostra um computador servidor de exemplo 300, de acordo com algumas modalidades. Por exemplo, o computador servidor 300 pode incluir ou ser incluído em qualquer dos dispositivos 102-106 descritos na FIG. 1. Exemplos de computadores de servidor 300 podem incluir celulares, tablets, computadores do tipo desktop e laptop, computadores de mainframe ou qualquer outro dispositivo de computação apropriado para receber, armazenar e transmitir dados. O computador servidor 300 pode ser configurado para comunicar-se diretamente ou indiretamente com um dispositivo do usuário 200 para implementar os métodos descritos neste documento. O computador servidor 300 pode incluir um processador 301

acoplado de forma comunicativa a uma interface de rede 302, uma memória 303, um meio legível computador 310 e, opcionalmente, um elemento de segurança 304.

[0085] O processador 301, a interface de rede 302, memória 303 pode ser semelhante ao processador 201, interface de rede 202 e memória 203 do dispositivo do usuário 200. O meio legível por computador 310 pode ser sob a forma de uma memória (por exemplo, flash, ROM, etc.) e pode incluir código executável pelo processador 301 para implementar os métodos descritos neste documento. O meio legível por computador 310 pode incluir um módulo de autenticação 311, um módulo de criptografia 312 e um módulo de aplicação 313. Em várias modalidades, esses módulos podem ser configurados para executar, individual ou coletivamente, alguns ou todos dos métodos 700, 1200, 1400, 1300, 1300, 1900, 11100 de FIGS. 6-7, 9, 11, 13, 15, 17, e 18, respectivamente.

[0086] O módulo de autenticação 311 pode incluir qualquer programa, software ou outro código apropriado para autenticar o dispositivo de computação 300 a outro dispositivo de computação ou autenticar outro dispositivo de computação no dispositivo de computação 300. Por exemplo, o módulo de autenticação 311 pode ser configurado para gerar e enviar uma mensagem de solicitação de autenticação para outro dispositivo de computação e receber e processar uma mensagem de resposta de autenticação de outros dispositivos de computação. Da mesma forma, o módulo de autenticação 311 pode ser configurado para receber e processar uma mensagem de solicitação de autenticação de outro dispositivo de computação e gerar e enviar uma mensagem de resposta de autenticação para o outro dispositivo de computação.

[0087] O módulo de criptografia 312 pode incluir qualquer programa, software ou outro código apropriado para executar operações relacionadas a criptografia ou descriptografia. Por exemplo, o módulo de criptografia pode

ser configurado para gerar um segredo compartilhado, como o uso de um protocolo de acordo de chave, tal como o Diffie-Hellman. O módulo de criptografia 312 pode ser ainda mais configurado para derivar uma chave de sessão ou chave de proteção de armazenamento de um segredo compartilhado, como o uso de uma função de derivação de chave (KDF). Em algumas modalidades, o módulo de criptografia 312 pode ser configurado para armazenar uma ou mais chaves estáticas, tal como uma chave privada de dispositivo de usuário estática ou uma chave privada de servidor estática. Em algumas modalidades, o módulo de criptografia 312 pode ser implementado usando qualquer combinação de software (como a emulação do cartão de host ou HCE) e hardware (como um módulo de hardware de segurança ou HSM).

[0088] O módulo de aplicação 313 pode incluir um serviço de aplicativo de pagamento operável para as solicitações de pagamento de serviço em um ou mais dispositivos de computação. Em algumas modalidades, o serviço de aplicativo de pagamento pode ser configurado para permitir que um usuário selecione bens e serviços que a serem comprados. O módulo de aplicação 313 também pode incluir serviços para se matricular ou registrar novamente os dispositivos de usuário e/ou conduzir transações com dispositivos de usuário.

[0089] Entende-se que os componentes descritos aqui são apenas para fins ilustrativos e não se destinam a serem um fator limitante. Em várias modalidades, mais ou menos componentes do que os listados aqui podem ser fornecidos. Por exemplo, em uma modalidade, o computador servidor 300 não pode incluir um elemento de segurança 304 e/ou um módulo de aplicação 313.

[0090] Enquanto o termo geral "computador servidor" é usada, em algumas modalidades, os computadores de servidor diferentes podem ser fornecidos para implementar diferentes características da invenção. Por exemplo, um servidor de provisionamento pode ser configurado para

estabelecer segredo(s) compartilhado(s) com um dispositivo do usuário e credenciais de provisionamento incluindo parâmetros de derivação de chave de token, parâmetros de atualização, parâmetros de derivação de criptograma, parâmetros de transação e quaisquer outros dados apropriados para um dispositivo do usuário. Um registro do servidor pode ser configurado para fornecer dados de registro para um dispositivo do usuário, receber um criptograma de registro do dispositivo do usuário e validar um criptograma de registro usando os dados de registro fornecidos pelo dispositivo do usuário. Um servidor de validação pode ser configurado para validar os criptogramas de transação fornecidos por um dispositivo do usuário usando segredo compartilhado de atualização é determinado com base em um segredo compartilhado anterior. Um servidor de renovação pode ser configurado para estabelecer que um novo segredo compartilhado pode ser estabelecido entre o usuário e o computador servidor. Além disso, o servidor de renovação pode ser configurado para provisão de novos parâmetros (por exemplo, novos parâmetros de derivação de chave, novos parâmetros de derivação de criptograma e/ou novos parâmetros de atualização) podem ser configurados para o dispositivo do usuário a ser usado para a geração dos criptogramas e/ou chaves de criptograma.

[0091] Em várias modalidades, o servidor de provisionamento, o servidor de registro e o servidor de validação podem ser implementados por computadores de servidor separados ou no mesmo computador servidor. Por exemplo, o servidor de validação pode ser implementado por um servidor de transação configurado para manipular as solicitações de pagamento separado do servidor de provisionamento e/ou servidor de registro. O servidor de provisionamento e o servidor de registro podem ser o mesmo servidor ou em servidores separados. O servidor de registro e o servidor de renovação podem ser os mesmos servidores ou separados. Quando implementados por computadores de servidor separados, o servidor de provisionamento, o

servidor de registro, o servidor de renovação e/ou o servidor de validação pode comunicar uns com os outros, a fim de acessar informações necessárias para descriptografar e/ou verificar os dados (por exemplo, as chaves privadas de servidor, segredos compartilhados, parâmetros de derivação de chave, parâmetros de derivação de criptograma, parâmetros de atualização, criptogramas, dados de solicitação, etc.).

II. MÉTODOS

[0092] As modalidades podem usar os sistemas e aparelhos descritos acima para provisionar de forma segura os dados confidenciais tais como as credenciais de um computador servidor a um dispositivo de usuário. As FIGS. 4-10 descrevem alguns exemplos de tais métodos. Em algumas modalidades, o dispositivo do usuário pode incluir o dispositivo do usuário 101 ou 200 de FIGS.1 e 2, respectivamente. O computador servidor pode incluir o dispositivo, 102, 103, 104, 105, 106 ou 300 de FIGS. 1 e 3, respectivamente. Em algumas modalidades, o computador servidor pode incluir um computador servidor de provisionamento.

A. Diagrama de Bloco de Nível Elevado

[0093] A FIG. 4 mostra uma vista em bloco em elevação de um processo de provisionamento de credencial segura 400, de acordo com algumas modalidades. O processo 400 pode ser usado aos dados confidenciais de provisão, tais como dados de credencial, a partir de um fornecedor confidencial 406 para um dispositivo móvel 402. O dispositivo móvel 402 pode incluir o dispositivo de usuário discutido nas FIGS. 1-2. O fornecedor confidencial 406 pode incluir um servidor de provisionamento de modo que um computador de usuário 300, um computador do vendedor 103, um computador do adquirente 104, um computador de rede de processamento de pagamento 105, um computador do emissor 106 e similares. O dispositivo móvel 402 pode, opcionalmente, comunicar com um provedor de armazenamento externo 408 para armazenar e/ou recuperar os dados tais

como dados de credencial. Em algumas modalidades, parte ou todas as funcionalidades do dispositivo móvel 402 discutidas abaixo podem ser executadas por um aplicativo móvel 404 instalada no dispositivo móvel 402.

[0094] Na etapa 1, o dispositivo móvel 402 gera um par de chave de usuário para proteger dados no trânsito entre o dispositivo móvel 402 e o fornecedor de dados confidenciais 406. O par de chaves pode ser de qualquer formato apropriado, tais como chaves baseadas em curva elíptica (EC) ou chaves baseadas em RSA. Preferivelmente, a chave pública e/ou a chave privada do par de chave de usuário são chaves avulsas. Isto é, a chave pública e/ou a chave privada do par de chaves de usuário é diferente para cada nova solicitação de provisionamento. Em uma modalidade, um par de chaves de usuário pode gerar um par de chaves efêmeras que compreende uma chave pública efêmera e uma chave privada efêmera. Um par de chaves efêmeras novas e diferentes podem ser geradas para cada nova solicitação de provisionamento. As chaves privadas/públicas efêmeras podem ser usadas diretamente como chaves avulsas. Alternativamente, as chaves pública/privadas efêmeras podem ser ainda cegas, ofuscadas ou modificadas como discutido abaixo, para formar as chaves avulsas. Em algumas outras modalidades, em vez de um par de chaves efêmeras, o par de chaves de usuário pode incluir um par de chaves estáticas que permanece estática (isto é, inalterado) para todas as solicitações de provisionamento ou semi-estática por um período pré-determinado de tempo ou um número predeterminado das solicitações de provisionamento. As chaves estática ou semi-estática podem ser cegadas, ofuscadas ou de outra maneira ser modificadas (por exemplo, usando um nonce criptográfico diferente, um número aleatório, dados específicos ou dados específicos de usuário, dados da transação, etc.) para cada pedido de provisionamento, de modo que as chaves cegas resultantes sejam chaves avulsas mesmo que as chaves de base subjacentes possam ser de estáticas ou semi-estáticas.

[0095] Na etapa 2, o dispositivo móvel 402 envia uma solicitação para o provedor de dados confidenciais 406 para os dados de credencial. O provedor de dados confidenciais 406 normalmente tem um par de chaves estáticas compreendendo uma chave pública estática e uma chave privada estática. A mensagem de solicitação pode ser protegida usando a chave privada de usuário (que pode ser estática ou efêmera, cega ou não-cega) e a chave pública de provedor de dados confidenciais. Por exemplo, a chave privada de usuário e a chave pública de provedor podem ser usadas para gerar uma chave de sessão de solicitação. A chave de sessão de solicitação pode ser usada para criptografar parte ou todas as partes da mensagem de solicitação. A mensagem de solicitação pode incluir a chave pública de usuário (que pode ser estática ou efêmera, cega ou não-cega).

[0096] Na etapa 3, o provedor de dados confidenciais 406 descriptografa a mensagem de solicitação. Em algumas modalidades, o provedor de dados confidenciais 406 pode descriptografar a mensagem de solicitação usando uma chave de sessão de pedido que é gerada usando a chave privada de provedor de dados confidenciais correspondente à chave pública de provedor de dados confidenciais e a chave pública de usuário do dispositivo móvel (que pode ser fornecida na mensagem de solicitação e que pode ou não ser cega).

[0097] Na etapa 4, o provedor de dados confidenciais 406 prepara uma resposta com os dados confidenciais, tais como dados de credencial. Como discutido, as credenciais ou os dados de credencial podem incluir quaisquer informações provisionadas do provedor de dados confidenciais 406 para o dispositivo móvel 402 que permite que o dispositivo móvel 402 realize as transações (por exemplo, transações de pagamento). Os exemplos de dados de credencial podem incluir PAN, token ou outras informações de conta, uma ou mais chaves criptográficas (por exemplo, LUKs usadas para gerar criptogramas, chaves públicas estáticas cegas ou não cegas, etc.), parâmetros

de derivação de chave (por exemplo, para derivar uma SUK que é usada gerar um criptograma, uma chave secreta compartilhada, uma chave de proteção de armazenamento, uma chave de criptografia, etc.), parâmetros de derivação de chave, as informações de cadeia de certificados, parâmetros de transação e todos os outros dados apropriados.

[0098] Para aumentar a segurança, os dados confidenciais podem ser protegidos usando uma chave de proteção de armazenamento que é diferente das chaves de sessão. A chave de proteção de armazenamento pode ser usada para criptografar diretamente alguns ou todos os dados confidenciais ou derivar uma chave de criptografia de credencial que é usada para criptografar os dados confidenciais. A chave de proteção de armazenamento pode ser uma chave de criptografia simétrica. Como alternativa, a chave de proteção de armazenamento pode ser uma chave assimétrica, como uma chave pública. Em tais casos, a chave privada correspondente à chave pública pode ser usada para descriptografar os dados confidenciais.

[0099] Na etapa 5, o provedor de dados confidenciais 406 envia uma resposta ao dispositivo móvel 402. A resposta pode incluir dados criptografados sensíveis. Algumas ou todas as partes da resposta podem ser protegidas usando uma chave de sessão de resposta para proteger os dados em trânsito. A chave de sessão de resposta pode ser gerada usando a chave pública de usuário e a chave privada de provedor confidencial. A resposta pode incluir a chave pública de provedor confidencial (que pode ser cegada) de modo a permitir que o dispositivo móvel 402 para descriptografar a resposta. Em alguns casos, a resposta pode não incluir a chave pública de provedor confidencial quando o dispositivo móvel 402 for capaz de determinar a chave pública de provedor confidencial (por exemplo, de um certificado).

[00100] Na etapa 6, o dispositivo móvel 402 descriptografa a resposta. Por exemplo, o dispositivo móvel 402 pode gerar um segredo compartilhado

de resposta usando a chave pública de provedor confidencial e a chave privada de usuário. Uma chave de sessão de resposta pode ser gerada a partir do segredo compartilhado de resposta e usada para descriptografar a resposta. Os dados confidenciais protegidos pela chave de proteção de armazenamento podem permanecer criptografados para evitar a exposição dos dados confidenciais. A chave de proteção de armazenamento (M_DEK) pode ser gerada pelo dispositivo móvel 402, por exemplo, usando o segredo compartilhado de resposta.

[00101] Na etapa 7, a chave de proteção de armazenamento é armazenada no dispositivo móvel 402. A chave de proteção de armazenamento pode ser armazenada com segurança no armazenamento. Por exemplo, a chave de proteção de armazenamento pode ser criptografada usando uma chave de criptografia de chave (KEK) do dispositivo móvel. Como alternativa, a chave de proteção de armazenamento pode ser armazenada em um módulo resistente a adulteração e seguro do dispositivo móvel ou protegido usando criptografia de caixa branca, ou quaisquer outras técnicas adequadas. Em algumas modalidades, a chave de proteção de armazenamento é usada como uma entrada para uma função de derivação de chave opcional, juntamente com alguns dados de derivação específicos ao dispositivo móvel (por exemplo, a impressão digital de dispositivo) para derivar uma chave de criptografia de credencial específica de dispositivo. A chave de criptografia de credencial específica de dispositivo pode ser armazenada em dispositivos móveis em vez de ou em adição à chave de proteção de armazenamento.

[00102] Similar a chave de proteção de armazenamento, os dados confidenciais criptografados que foram criptografados usando a chave de proteção de armazenamento (ou uma chave de criptografia de credencial derivada da chave de proteção de armazenamento) também podem ser armazenados no dispositivo móvel 402. Em algumas modalidades, os dados

confidenciais cifrados podem ser armazenados em um elemento seguro do dispositivo móvel (por exemplo, um módulo de segurança resistente a adulteração). Em outras modalidades, os dados criptografados sensíveis podem ser armazenados em um dispositivo móvel sem um elemento de segurança. Devido ao fato de que os dados confidenciais permanecem criptografados quando no armazenamento, o risco de exposição dos dados confidenciais é minimizado, mesmo quando o dispositivo de armazenamento está comprometido.

[00103] Em algumas modalidades, a chave de proteção de armazenamento e os dados criptografados sensíveis podem ser armazenados nos mesmos ou diferentes locais de armazenamento. Por exemplo, a chave de proteção de armazenamento (por exemplo, em um formato criptografado) e os dados confidenciais criptografados podem ser armazenados em um elemento sem segurança do dispositivo móvel (por exemplo, quando o dispositivo móvel não for um elemento de segurança). Em outro exemplo, a chave de proteção de armazenamento (por exemplo, em uma forma criptografada ou descriptografada) pode ser armazenada em um elemento de segurança do dispositivo móvel, enquanto que os dados criptografados sensíveis podem ser armazenados em um elemento de armazenamento regular (uma vez que os dados confidenciais já estão criptografados).

[00104] Na etapa 8, o dispositivo móvel 402 opcionalmente pode encaminhar os dados confidenciais criptografados sejam armazenadas por um provedor de armazenamento externo 408. O armazenamento de dados confidenciais criptografados no provedor de armazenamento externo pode ser útil para fins de cópia de segurança. Por exemplo, uma cópia dos dados criptografados sensíveis pode ser armazenada no dispositivo móvel e um outro dispositivo (por exemplo, um computador pessoal ou desktop). O armazenamento de dados criptografados sensíveis no provedor de armazenamento externo também pode ser usado para reduzir o risco de

exposição de dados confidenciais criptografados no dispositivo móvel. Por exemplo, o provedor de armazenamento externo pode fornecer um maior nível de segurança de dados (por exemplo, via proteção de hardware e/ou software de segurança) do que o dispositivo móvel. Uma cópia dos dados confidenciais criptografados pode ser armazenada apenas no provedor de armazenamento externo e não no dispositivo móvel, que é considerado menos seguro. Em alguns casos, a chave de proteção de armazenamento e os dados confidenciais criptografados podem ser armazenados em locais diferentes, de modo a minimizar o risco de exposição dos dados confidenciais. Um invasor não seria capaz de descriptografar os dados confidenciais criptografados sem a chave de proteção de armazenamento e vice-versa. Mesmo com a chave de proteção de armazenamento e os dados confidenciais criptografados, um invasor pode não ser capaz de decifrar os dados confidenciais criptografados. Por exemplo, em algumas modalidades, a chave de proteção de armazenamento não pode ser usada para criptografar diretamente os dados confidenciais criptografados. Em vez disso, a chave de proteção de armazenamento precisa ser combinada com informações adicionais desconhecidas para o atacante (por exemplo, dados específicos de dispositivo) para derivar uma chave de criptografia para descriptografar os dados confidenciais criptografados.

[00105] O provedor de armazenamento externo 408 pode ser operado por ou associados a um computador do vendedor 103, um computador do adquirente 104, uma rede de processamento de pagamento 105, um computador do emissor 106 ou quaisquer outras entidades apropriadas (por exemplo, um provedor de armazenamento baseados em nuvem). Em um exemplo, o provedor de armazenamento externo é ou está associado a mesma entidade (por exemplo, um usuário) que também possui ou opera o dispositivo móvel. Em algumas outras modalidades, o provedor de armazenamento externo 408 pode incluir um dispositivo de armazenamento 107 que é

conectado ao dispositivo móvel (por exemplo, um disco rígido externo). O provedor de armazenamento externo 408 pode ser conectado remotamente ao dispositivo móvel através de uma ou mais redes (por exemplo, redes com fio ou sem fios). Como alternativa, o provedor de armazenamento externo 408 pode ser conectado localmente ao dispositivo móvel sem o uso de uma rede.

[00106] Na etapa 9, o dispositivo móvel 402, opcionalmente, pode obter os dados confidenciais criptografados do provedor de armazenamento externo 408. Por exemplo, o dispositivo móvel 402 pode autenticar no provedor de armazenamento externo 408 (por exemplo, usando um nome de usuário e senha), e o provedor de armazenamento externo 408 pode retornar os dados confidenciais criptografados em resposta. O dispositivo móvel 402 pode, em seguida, descriptografar os dados confidenciais criptografados, de modo que os dados descriptografados sensíveis (por exemplo, dados de credencial) possam ser usados para realizar uma transação. Por exemplo, os dados confidenciais criptografados podem ser descriptografados usando a chave de proteção de armazenamento para obter o material criptográfico (por exemplo, uma LUK) para gerar um criptograma. O criptograma pode ser usado em uma solicitação de autenticação/autorização de uma transação. Alternativa ou adicionalmente, o dispositivo móvel 402 pode armazenar os dados confidenciais criptografados no armazenamento local seguro (por exemplo, elemento de segurança 204) ou, caso contrário, proteger os dados confidenciais criptografados no armazenamento do dispositivo móvel. Por exemplo, os dados descriptografados sensíveis podem ser re-codificados usando uma chave de criptografia secreta do dispositivo móvel (em vez de ou além da chave de proteção de armazenamento) antes de serem armazenados no dispositivo móvel.

[00107] Em várias modalidades, os dados confidenciais restos criptografados no momento, provisionamento, a partir do provedor de dados confidenciais 406 para o dispositivo móvel 402, durante a transmissão entre o

dispositivo móvel 402 e o provedor de armazenamento externo 408, assim como durante o armazenamento, o dispositivo móvel 402 e/ou o provedor de armazenamento externo 408. Assim, a proteção end-to-end dos dados confidenciais é fornecida até o uso real dos dados confidenciais ao tempo da transação, limitar a exposição dos dados confidenciais só quando os dados confidenciais forem necessários, reduzindo assim o risco de comprometimento dos dados confidenciais.

B. Dispositivo do usuário

[00108] A FIG. 5 mostra um processo de exemplo 500 para provisionar de forma segura os dados de credencial de um computador servidor, de acordo com algumas modalidades. Em tais modalidades, os dados de credencial podem ser protegidos por uma chave de proteção de armazenamento que é determinada com base em um segredo compartilhado. Os aspectos do processo 500 podem ser realizados por um dispositivo de usuário tal como um dispositivo de usuário 101 ou 200. Alternativamente ou adicionalmente, os aspectos do processo 500 podem ser realizados por outras entidades apropriadas. Alguns ou todos os aspectos do processo 500 (ou quaisquer outros processos descritos neste documento, ou variações e/ou suas combinações) podem ser executados sob o controle de um ou mais sistemas de controle/computador configurados com instruções executáveis e podem ser implementadas como código (por exemplo, instruções executáveis, um ou mais programas de computador ou um ou mais aplicativos) coletivamente em um ou mais processadores, por hardware ou combinações destes. O código pode ser armazenado em um meio de armazenamento legível por computador, por exemplo, sob a forma de um programa de computador que compreende uma pluralidade de instruções executáveis por um ou mais processadores. O meio de armazenamento legível por computador pode ser não-transitório. A ordem em que as operações são descritas não se destina a ser interpretada como uma limitação e qualquer número das operações descritas pode ser

combinado em qualquer ordem e/ou em paralelo para implementar os processos.

[00109] No bloco 502, uma chave pública de usuário avulsa é determinada. A chave pública de usuário avulsa é uma chave pública associado com o dispositivo de usuário e também pode ser referida como a chave pública de cliente avulsa. A chave pública de usuário avulsa pode ser uma parte de um par de chaves de usuário que inclui a chave pública e uma chave privada correspondente. O par de chaves pode ser de qualquer formato apropriado, tais como chaves baseadas em curva elíptica (EC) ou chaves baseadas em RSA. O par de chaves de usuário pode incluir um par de chaves efêmero que é gerado para cada solicitação de provisionamento. Como alternativa, o par de chaves de usuário pode incluir um par de chaves estáticas que é os mesmos para todas as solicitações de provisionamento, ou um par de chaves semi-estática que permanecem estáticas para um período predeterminado de tempo ou um número predeterminado de solicitações de provisionamento. Os valores das chaves estáticas ou semi-estáticas podem ser cegos, ofuscados ou alterados de forma diferente para cada solicitação de provisionamento, resultando em chaves avulsas. Por exemplo, a multiplicação de ponto pode ser realizada em uma chave pública/privada de usuário com algum outro elemento de dados (por exemplo, um número aleatório, um nonce criptográfico, fator de identificação, dados de transações, etc.) para modificar o valor da chave de usuário para cada solicitação de provisionamento. Em algumas modalidades, a chave privada do par de chaves de usuário pode permanecer estática enquanto a chave pública de alterações de par de chaves de usuário com cada solicitação de provisionamento. Em outros casos, as chaves públicas e privadas do par de usuário podem ser modificadas para cada solicitação de provisionamento.

[00110] Em algumas modalidades um fator de identificação é calculado usando os dados de identificação e dados de autenticação. Os dados

de identificação podem incluir quaisquer dados ou informações associadas a um usuário ou um dispositivo do usuário. Exemplos de dados de identificação podem incluir um nome de um usuário associado ao dispositivo do usuário, uma organização associada ao dispositivo do usuário, as informações de pagamento tais como Número da Conta Principal (PAN) ou token associado ao dispositivo do usuário, uma data de expiração associada a PAN ou token, um certificado associado ao dispositivo do usuário, um IMEI ou número de série de dispositivo do usuário, etc. Os dados de autenticação podem incluir quaisquer dados ou informações adequadas para autenticar um usuário ou dispositivo do usuário. Exemplos de dados de autenticação podem incluir uma senha ou frase-chave, uma chave secreta (por exemplo, uma chave privada), etc. Um fator de identificação pode incluir quaisquer dados ou informações determinados a partir de dados de identificação e/ou dados de autenticação. Por exemplo, em algumas modalidades, o fator de identificação pode ser gerado por uma combinação dos dados de identificação e a autenticação de hash.

[00111] O fator de identificação pode ser combinado com a chave pública de usuário (que pode ser efêmera, estática ou semi-estática) e a chave privada de usuário (que pode ser efêmera, estática ou semi-estática). Como resultado, uma chave pública efêmera combinada ou cega e uma chave privada efêmera combinada ou cega podem ser determinadas. Uma chave combinada ou cega pode incluir uma chave que foi ofuscada ou alterada do valor original pela combinação com outro valor ou elemento de dados, conforme discutido acima. Em algumas modalidades, o ocultamento das chaves de usuário pode ser opcional (por exemplo, quando forem usadas chaves efêmeras).

[00112] O segredo compartilhado de solicitação pode ser gerado usando a chave privada de usuário (que pode ou não ser cega ou combinada com outros elementos de dados) e uma chave pública de servidor estática. O

primeiro segredo compartilhado de solicitação pode ser usado para proteger (por exemplo, criptografar ou descriptografar) a mensagem de solicitação de provisionamento, como discutido abaixo. A chave pública de servidor estática pode incluir uma chave pública estática, mantida pelo computador servidor, tal como em um elemento de segurança. Em algumas modalidades, a chave pública de servidor estática pode ser determinada a partir de um certificado digital do computador servidor, que pode ter sido obtido anteriormente pelo dispositivo de usuário e que pode ser assinado por uma autoridade de certificação confiável.

[00113] O segredo compartilhado de solicitação pode ser gerado a partir da chave privada de usuário (que pode ou não ser combinada uma chave cega ou combinada) e a chave pública de servidor estática usando qualquer método adequado. Por exemplo, nas modalidades usando criptografia de curva elíptica, o segredo compartilhado pode ser determinado usando o protocolo Diffie-Hellman de curva elíptica (ECDH).

[00114] Uma chave de sessão de solicitação pode ser gerada usando o segredo compartilhado de solicitação e outros dados suplementares adequados tais como dados de derivação de chaves, se houver. A chave de sessão de solicitação também pode ser referida como uma chave de proteção de mensagem uma vez que é utilizada para proteger uma mensagem entre o dispositivo de usuário e o computador servidor. Exemplos de tais dados suplementares podem incluir um identificador de computador servidor e/ou uma chave pública de usuário avulsa.

[00115] A chave de sessão de solicitação pode ser de qualquer formato apropriado (por exemplo, AES, DES, Blowfish, etc.), de qualquer comprimento adequado e gerado usando qualquer função de derivação de chave apropriado (KDF). Por exemplo, em uma modalidade, a chave de sessão de solicitação pode ser gerada usando o algoritmo de Função de Derivação de Chave com Base em Senha 2 (Password-Based KeyDerivation

Function (PBKDF2)). Em algumas modalidades, outros dados de dispositivo de usuário, tal como um identificador de dispositivo de usuário, podem ser usados como entradas adicionais para a função de derivação de chave.

[00116] No bloco 504, uma mensagem de solicitação de provisionamento é enviada para um computador servidor de provisionamento. Em algumas modalidades, a mensagem de solicitação de provisionamento pode passar através de um ou mais intermediários (por exemplo, rede não confiável) antes de chegar ao computador servidor. A mensagem de solicitação pode incluir a chave pública de usuário avulsa (cega ou não cega). A mensagem de solicitação também pode incluir dados de identificação, um identificador de dispositivo de usuário, dados de autenticação, juntamente com quaisquer outros dados adequados destinados ao computador servidor. Por exemplo, os dados de solicitação também podem incluir informações de configuração de cliente e/ou diretivas para o serviço. Em alguns exemplos, tais informações podem ser fornecidas pelos dispositivos de usuário que não incluem, a priori, meios para autenticação forte. Parte ou todos os dados de pedido (dados contidos na mensagem de solicitação) podem ser protegidos (por exemplo, criptografados) usando a chave de sessão de solicitação para formar uma mensagem de solicitação criptografada. Uma mensagem de solicitação de provisionamento de exemplo é mostrada na FIG. 12. Em um exemplo, os dados de identificação e os dados de autenticação são criptografados e armazenados em uma porção de texto codificado da mensagem de solicitação. A chave pública de usuário avulsa pode ser armazenada em uma porção de texto não codificado da mensagem de solicitação. Em outro exemplo, a chave pública de usuário avulsa também pode ser criptografada e armazenada na porção de texto codificado. Em alguns casos, a mensagem de solicitação de provisionamento pode incluir a chave pública de usuário e não inclui os dados de solicitação criptografados.

[00117] No bloco 506, uma mensagem de resposta de provisionamento

é recebida do computador servidor de provisionamento. A mensagem de resposta de provisionamento pode incluir a chave pública do computador servidor cega e dados de resposta criptografados. Normalmente, a chave pública de servidor estática cega pode ser uma forma cega da chave pública de servidor estática usada para gerar o segredo compartilhado de solicitação. A vantagem de fornecer uma chave pública de servidor estática cega é que a chave pública de computador servidor estática é ofuscada e a identidade do computador servidor protegida contraespionagem. Em que a chave pública de servidor estática não é cega, um nonce criptográfico pode ser fornecido como parte dos dados de resposta e usado para calcular criptogramas. Por exemplo, o nonce criptográfico do servidor (entropia) pode ser usado ou armazenado para derivação adicional ou um segundo nonce criptográfico pode ser fornecido como parte dos parâmetros de derivação. É essencial que a entropia do servidor seja usada no cálculo dos criptogramas (por exemplo, criptogramas de transação de pagamento). Uma mensagem de resposta de provisionamento de exemplo é mostrada na FIG. 12.

[00118] No bloco 508, um segredo compartilhado de resposta é determinado usando a chave pública de servidor estática. O segredo compartilhado de resposta pode ser usado para proteger (por exemplo, criptografar e/ou descriptografar) a mensagem de resposta. Além disso, em algumas modalidades, o segredo compartilhado de resposta pode ser usado para derivar a chave de proteção de armazenamento usada para proteger dados confidenciais (por exemplo, dados de credencial) incluídos na resposta. O segredo compartilhado de resposta pode ser determinado usando a chave privada de usuário (que pode ser efêmera, estática ou semi-estática) e a chave pública de servidor estática. Em algumas modalidades, uma chave pública de servidor estática cega pode ser recebida a partir do computador servidor, por exemplo, como parte da mensagem de resposta de provisionamento ou de um canal separado. Em algumas outras modalidades, os dados de ocultação (por

exemplo, um nonce criptográfico, um número aleatório) podem ser fornecidos para o dispositivo de usuário (por exemplo, como parte da mensagem de resposta de provisionamento) em vez da chave pública de servidor estática cega. Em tais casos, a chave pública de servidor estática cega pode ser derivada pelo dispositivo de usuário usando a chave pública de servidor estática e os dados de ocultação fornecidos. Por exemplo, uma chave cega pode ser derivada usando um nonce criptográfico que pode ser fornecido como parte da mensagem de resposta de provisionamento. O nonce criptográfico pode ser um número aleatório ou pseudoaleatório. O nonce criptográfico também pode ser usado para verificar um certificado do computador servidor, conforme discutido em outro lugar.

[00119] Em algumas modalidades, o segredo compartilhado de resposta pode ser gerado a partir da chave privada de usuário e a chave pública de servidor estática cega usando qualquer método adequado, como ECDH. Em outras modalidades, o segredo compartilhado de resposta pode ser determinado sem uma chave cega. Em tais modalidades, a mensagem de resposta de provisionamento (por exemplo, as credenciais) pode incluir dados de ocultamento (por exemplo, nonce criptográfico) que podem ser usados para derivar uma chave de criptograma.

[00120] Normalmente, o segredo compartilhado de solicitação é diferente do segredo compartilhado de resposta. Por exemplo, a chave pública de servidor estático pode ser ocultada diferentemente quando usada para gerar o segredo compartilhado de solicitação e o segredo compartilhado de resposta. Em tais modalidades, o segredo compartilhado de solicitação é substancialmente o mesmo que o segredo compartilhado de solicitação.

[00121] No bloco 510, uma chave de sessão de resposta é determinada usando o segredo compartilhado de resposta e outros dados complementares adequados tais como dados de derivação de chave, se houver. A chave de sessão de resposta também pode ser referida como uma chave de proteção de

mensagem uma vez que é utilizada para proteger uma mensagem entre o dispositivo de usuário e o computador servidor. Exemplos de tais dados suplementares podem incluir um identificador de computador servidor um identificador de dispositivo de usuário e/ou uma chave pública de usuário truncada. A segunda chave de sessão pode ser gerada usando qualquer KDF apropriado.

[00122] A chave de sessão de resposta pode ser de qualquer formato apropriado (por exemplo, AES, DES, Blowfish, etc.), de qualquer comprimento adequado e gerado usando qualquer função de derivação de chave apropriado (KDF). Por exemplo, em uma modalidade, a chave de sessão de resposta pode ser gerada usando o algoritmo de Função de Derivação de Chave com Base em Senha 2 (Password-Based KeyDerivation Function (PBKDF2)). Em algumas modalidades, outros dados específicos de dispositivo de usuário, tal como um identificador de dispositivo de usuário ou outras informações de impressão digital de dedo de dispositivo, podem ser usados como entradas adicionais para a função de derivação de chave.

[00123] No bloco 512, a mensagem de resposta de provisionamento é descriptografada usando a chave de sessão de resposta para obter os dados de resposta. Os dados de resposta podem incluir dados de credencial criptografados, um nonce criptográfico, uma cadeia de certificado do computador servidor, dados de derivação de chave, descritores de conjunto de codificação e quaisquer outros dados. Parte ou todos os dados de resposta podem ser criptografados utilizando a chave de sessão de resposta.

[00124] A autenticação do computador servidor pode ser executada através do dispositivo de usuário. A cadeia de certificado do computador servidor pode ser validada. A cadeia de certificados do computador servidor pode ser validada usando qualquer método adequado online ou offline. Por exemplo, para cada um dentre os um ou mais certificados na cadeia, a assinatura digital do certificado pode ser validada usando uma chave pública

confiável conhecida (por exemplo, a chave pública da autoridade de certificado ou uma chave pública da entidade devidamente autorizada pela CA). Por exemplo, em algumas modalidades, um algoritmo de assinatura digital, tais como o algoritmo de assinatura digital de curva elíptica (ECDSA) pode ser usado para validar um certificado. Em algumas modalidades, um certificado do computador servidor pode ser verificado usando um nonce criptográfico que é fornecido como parte da mensagem de resposta de provisionamento (por exemplo, como parte das credenciais).

[00125] A chave pública de computador servidor estática cega pode ser verificada usando o certificado do computador servidor e o nonce criptográfico. Verificando a chave pública do computador servidor estática cega pode incluir garantir que a chave pública do computador servidor estática cega corresponda a um valor esperado. Por exemplo, em alguns casos, uma segunda chave pública de computador servidor estática cega pode ser gerada usando a chave pública de computador servidor estática incluída no certificado do computador servidor e um nonce criptográfico extraído dos dados de resposta. A segunda chave pública de computador servidor estática cega, então, poderá ser comparada à chave pública de computador servidor estática cega recebida na para garantir que as chaves correspondam. Alternativamente, em alguns casos, a chave pública de computador servidor estática cega recebida pode ser verificada comparando a mesma a uma chave pública de computador servidor estática cega armazenada. Se as chaves corresponderem, o computador servidor pode ser autenticado. Caso contrário, a autenticação pode falhar. Em algumas modalidades, a chave pública estática cega pode ser fornecida em ambos o texto sem codificação e no texto codificado da mensagem de resposta, de modo a permitir a verificação e impedir adulteração.

[00126] Deve ser notado que esse método de autenticação (isto é, verificando uma chave pública estática cega) pode fornecer a vantagem de

que a chave pública do computador servidor estática, que pode ser considerada confidencial (uma vez que pode revelar a identidade do computador servidor), não necessita ser transmitida em texto claro. Assim, a autenticação do computador servidor pode ser executada ao mesmo tempo que protege a identidade do computador servidor de um intruso que capta a mensagem de solicitação de provisionamento.

[00127] Os dados de resposta também podem incluir dados de credenciais criptografados, que podem permanecer criptografados sem ser descriptografados até que os dados de credencial sejam realmente necessários para realizar uma transação. Os dados de credencial podem incluir quaisquer dados que são provisionados de um servidor a um dispositivo de usuário (por exemplo, dispositivo móvel) que permita que o dispositivo de usuário realize transações (por exemplo, operações de pagamento). Os exemplos de dados de credencial podem incluir tokens, PAN ou outras informações de conta, uma ou mais chaves (por exemplo, LUKs usadas para gerar criptogramas, chaves públicas estáticas cegas ou não cegas, etc.), parâmetros de derivação de chave (por exemplo, para derivar uma SUK que é usada gerar um criptograma, uma chave secreta compartilhada, uma chave de criptografia, etc.), parâmetros de derivação de chave, as informações de cadeia de certificados, parâmetros de transação e todos os outros dados apropriados.

[00128] Os dados de credencial podem incluir parâmetros de derivação de chave que podem ou não incluir uma chave de uso limitado (LUK). Os parâmetros de derivação de chave (que podem ou não incluir o LUK) podem ser usados para gerar um ou vários criptogramas para conduzir as transações. Por exemplo, o LUK pode ser usado para derivar um criptograma diretamente ou usado para derivar uma chave de criptograma que é usada para gerar um criptograma.

[00129] Os dados de credencial podem incluir parâmetros de derivação de criptograma podem ser usados para derivar criptogramas. Os dados de

credencial também podem incluir parâmetros de atualização que podem ser usados pelo dispositivo do usuário para gerar um segredo compartilhado atualizado com base em um segredo compartilhado anterior. Em algumas modalidades, os parâmetros de derivação de chave podem ser substancialmente o mesmo que os parâmetros de atualização. Em algumas outras modalidades, os parâmetros de derivação de chave podem ser diferentes do que os parâmetros de atualização. Os parâmetros de derivação de chave e/ou os parâmetros de atualização podem ser exclusivos por dispositivo do usuário ou por grupo dos dispositivos de usuário a fim de evitar ataques em massa offline.

[00130] Os parâmetros de derivação de chave, os parâmetros de derivação de criptograma e/ou os parâmetros de atualização podem incluir um LUK, uma especificação de quais parâmetros de transação de uma determinada transação usar, o código para realizar a derivação (ou um identificador de qual é o procedimento de derivação para usar) e/ou outras informações relacionadas a esses parâmetros. Em algumas modalidades, os parâmetros de derivação de chave, os parâmetros de derivação de criptograma e/ou os parâmetros de atualização podem incluir parâmetros "falsos" ou inválido para propósitos de ofuscação. O código pode ser o código de método de derivação personalizado em que é exclusivo para um dispositivo ou grupo de dispositivos e pode ser atribuído de forma aleatória. O código pode ser assinado pelo servidor ou outro fornecedor, de modo que o dispositivo do usuário possa autenticar o código. Em algumas modalidades, o código é ofuscado antes de ser assinado, tornando, assim, difícil para um invasor compreender, ignorar e/ou reverter o código.

[00131] No bloco 514, uma chave de proteção de armazenamento é determinada usando o segredo compartilhado de resposta. A chave de proteção de armazenamento pode ser útil para descriptografar dados de credencial criptografados. Por exemplo, a chave de proteção de

armazenamento pode ser usada, através do computador servidor, para criptografar diretamente os dados de credencial para gerar os dados de credencial criptografados. Como outro exemplo, a chave de proteção de armazenamento pode ser usada, em combinação com os dados específicos para o dispositivo de usuário ou usuário (por exemplo, informações de impressão digital de dispositivo ou informações de identificação de usuário), para derivar uma chave de criptografia de credencial foi usada para criptografar os dados de credencial.

[00132] Vários métodos podem ser usados para gerar a chave de proteção de armazenamento. Em uma modalidade, o segredo compartilhado de resposta pode ser usado para derivar uma sequência de bits aleatórios ou pseudoaleatórios. A sequência de bits pode ser dividida, de acordo com um algoritmo predeterminado, em duas porções. A primeira porção da sequência de bits pode ser usada como ou usada para gerar a chave de sessão de resposta; enquanto que a segunda parte da sequência de bits pode ser usada como ou usada para gerar a chave de proteção de armazenamento.

[00133] Em outra modalidade, o segredo compartilhado de resposta pode ser usado com funções de derivação de chave ou algoritmos de geração de chave diferentes para gerar a chave de sessão de resposta e a chave de proteção de armazenamento, respectivamente.

[00134] Em algumas modalidades alternativas, a chave de proteção de armazenamento pode não ser gerada a partir do segredo compartilhado de resposta. Conforme discutido em conexão com a FIG. 13, em vez de uma chave secreta compartilhada, a chave de proteção de armazenamento pode ser uma chave pública do dispositivo de usuário e corresponde a uma chave privada de armazenamento. A chave privada de armazenamento pode ser igual ou diferente da chave privada de usuário discutida no bloco 502, que é usada como uma chave pública de usuário avulsa e fornecida ao computador servidor (por exemplo, na mensagem de solicitação de provisionamento) com

a finalidade de gerar segredos compartilhados (por exemplo, segredo compartilhado de solicitação e o segredo compartilhado de resposta).

[00135] A chave pública de proteção de armazenamento pode ser fornecida ao computador servidor (por exemplo, na mensagem de solicitação de provisionamento) para proteger os dados de credencial. O computador servidor pode criptografar os dados de credencial com a chave de proteção de armazenamento e fornecer os dados criptografados de credencial ao dispositivo de usuário. Em tal uma modalidade, o dispositivo de usuário pode armazenar os dados de credencial criptografados até que os dados de credencial sejam necessários para realizar uma transação (por exemplo, para gerar um criptograma de transação). Ao tempo de transação, o dispositivo de usuário pode descriptografar os dados de credencial criptografados usando a chave privada de proteção de armazenamento correspondente à chave pública de proteção de armazenamento. A chave privada de proteção de armazenamento pode ser protegida pelo dispositivo de usuário (por exemplo, através de criptografia, criptografia de caixa branca ou módulo de hardware de segurança).

[00136] No bloco 516, a chave de proteção de armazenamento, opcionalmente, pode ser criptografada usando uma chave de criptografia de chave (KEK). A KEK pode incluir qualquer chave de criptografia apropriada do dispositivo de usuário. Em alguns casos, a KEK pode ser estática ou alternante ao longo do tempo. Por exemplo, a chave de proteção de armazenamento pode ser criptografada periodicamente com KEKs rotativas para aumentar a segurança. Em algumas modalidades, em vez de ou adicionalmente sendo criptografada com uma chave de criptografia, a chave de proteção de armazenamento pode ser protegida usando quaisquer outros métodos adequados incluindo módulo de hardware resistente a adulteração (por exemplo, chip inteligente), criptografia de caixa branca e similares. Em modalidades onde a chave de proteção de armazenamento é uma chave

pública, a chave privada de proteção de armazenamento correspondente (utilizável para descriptografar os dados de credencial criptografados) pode ser criptografada ou protegida de outra forma (por exemplo, usando criptografia de módulo de hardware de segurança ou de caixa-branca).

[00137] No bloco 518, os dados de credencial criptografados são armazenados. Os dados de credencial criptografados podem ser armazenados no dispositivo de usuário, por exemplo, em um módulo de segurança ou sem segurança. Alternativamente ou adicionalmente, os dados de credencial criptografados podem ser armazenados em um armazenamento de dados local ou remoto, tais como fornecido por um provedor de armazenamento externo discutido na FIG. 4. Em alguns casos, uma ou mais cópias dos dados de credencial criptografados podem ser armazenadas por um ou mais armazenamentos externos, por exemplo, para fornecer redundância. No entanto, os dados de credencial criptografados não podem ser descriptografados sem a chave de proteção de armazenamento que é protegida por criptografia ou outros métodos de proteção de dados adequados, reduzindo assim o risco de comprometimento dos dados de credencial.

[00138] No bloco 520, a chave de proteção criptografada é armazenada. A chave de armazenamento criptografada pode ser armazenada no dispositivo de usuário, por exemplo, em um módulo de segurança ou sem segurança. Alternativamente ou adicionalmente, a chave de armazenamento criptografada pode ser armazenada em um armazenamento de dados local ou remoto, tais como fornecido por um provedor de armazenamento externo discutido na FIG. 4. Em modalidades onde a chave de proteção de armazenamento é uma chave pública de usuário, a chave privada de proteção de armazenamento correspondente (utilizável para descriptografar os dados de credencial criptografados) pode ser criptografada ou protegida de outra forma (por exemplo, usando criptografia de módulo de hardware de segurança ou de caixa-branca). Em algumas modalidades, a chave de proteção criptografada e

os dados de credencial criptografados podem ser armazenados em locais diferentes, para reduzir o risco de comprometimento de ambos. Por exemplo, a chave de proteção criptografada pode ser armazenada no dispositivo de usuário e os dados de credencial criptografados podem ser armazenados em um provedor de armazenamento externo que é conectado remotamente ao dispositivo de usuário; ou vice-versa.

[00139] A FIG. 6 mostra outro processo de exemplo 600 para provisionar de forma segura os dados de credencial de um computador servidor, de acordo com algumas modalidades. Em tais modalidades, os dados de credencial podem ser protegidos por uma chave pública de armazenamento de proteção fornecida pelo dispositivo de usuário. Os aspectos do processo 600 podem ser realizados por um dispositivo de usuário tal como um dispositivo de usuário 101 ou 200. Alternativamente ou adicionalmente, os aspectos do processo 600 podem ser realizados por outras entidades apropriadas.

[00140] No bloco 602, uma chave pública de usuário avulsa é determinada. A chave pública de usuário avulsa pode ser semelhante à chave pública de usuário avulsa que é gerada no bloco 502 da FIG. 5 discutida acima.

[00141] No bloco 604, uma chave pública de proteção de armazenamento é determinada. A chave pública de proteção de armazenamento pode ser uma chave pública de um par de chaves de proteção de armazenamento pública/privada gerado e/ou mantido pelo dispositivo de usuário. A chave privada de proteção de armazenamento pode ser usada para descriptografar os dados confidenciais criptografados (por exemplo, dados de credencial). O par de chaves de proteção de armazenamento pode ser um par de chaves diferentes do que o par de chaves pública/particular de usuário usado no bloco 602 usado para gerar os segredos compartilhados (por exemplo, o segredo compartilhado de solicitação e o segredo compartilhado

de resposta). Alternativamente, o par de chaves de proteção de armazenamento e o par de chaves de usuário pode compartilhar a mesma chave privada. Por exemplo, a mesma chave privada de usuário pode ser usada para gerar duas chaves públicas, uma chave pública de proteção de armazenamento com a finalidade de proteger os dados de credencial e uma chave pública de usuário discutida no bloco 602 usada com a finalidade de proteger as mensagens em trânsito.

[00142] No bloco 606, uma mensagem de solicitação de provisionamento é enviada para um computador servidor de provisionamento. A mensagem de solicitação pode incluir a chave pública de usuário avulsa (cega ou não) e a chave pública de proteção de armazenamento. A mensagem de solicitação também pode incluir outros dados descritos na FIG. 5, como os dados de identificação, um identificador de dispositivo de usuário, dados de autenticação, juntamente com quaisquer outros dados adequados destinados ao computador servidor. Em algumas modalidades, um segredo compartilhado de solicitação e uma chave de sessão de solicitação podem ser determinados de maneira semelhante, como descrito na FIG. 5. A chave de sessão de solicitação pode ser usada para proteger a mensagem de solicitação de provisionamento. Uma mensagem de solicitação de provisionamento de exemplo é mostrada na FIG. 13.

[00143] No bloco 608, uma mensagem de resposta de provisionamento é recebida do computador servidor de provisionamento. A mensagem de resposta de provisionamento pode incluir os dados de credencial que foram criptografados usando a chave pública de proteção de armazenamento que foi enviada no bloco 606 acima. A mensagem de resposta de provisionamento também pode incluir uma chave pública de servidor estática cega e outros dados de resposta criptografados como descritos no bloco 506 da FIG. 5. Uma mensagem de solicitação de provisionamento de exemplo é mostrada na FIG. 13.

[00144] No bloco 610, um segredo compartilhado de resposta é determinado usando a chave pública de servidor estática. O segredo compartilhado de resposta pode ser determinado de forma semelhante, conforme descrito no bloco 508 da FIG. 5.

[00145] No bloco 612, uma chave de sessão de resposta é determinada usando o segredo compartilhado de resposta e outros dados complementares adequados tais como dados de derivação de chave, se houver. A chave de sessão de resposta pode ser determinada de forma semelhante, conforme descrito no bloco 510 da FIG. 5.

[00146] No bloco 614, a mensagem de resposta de provisionamento é descriptografada usando a chave de sessão de resposta para obter os dados de resposta. A mensagem de resposta de provisionamento pode ser descriptografada de uma maneira similar conforme descrito no bloco 512 da FIG. 5. Os dados de resposta podem incluir dados de credencial criptografados. Os dados de credencial criptografados podem ter foram criptografados usando a chave pública de proteção de armazenamento que foi fornecida no bloco 606 acima. As etapas de autenticação adicionais podem ser realizadas pelo dispositivo de usuário com base em dados de resposta, conforme descrito na FIG. 5.

[00147] No bloco 616, os dados de credencial criptografados são armazenados em uma maneira similar como descrito no bloco 518 da FIG. 5.

[00148] A chave privada de proteção de armazenamento que é usada para descriptografar os dados de credencial criptografados e/ou a chave pública de proteção de armazenamento pode ser armazenada de uma maneira similar como descrito em blocos 518 e 520 de FIG. 5. Por exemplo, a chave de pública/privada de proteção de armazenamento pode ser ainda criptografada usando uma chave de criptografia de chave antes de ser armazenada. A chave pública/privada de proteção de armazenamento pode ser armazenada em um módulo de segurança (por exemplo, cartão de chip

inteligente). A chave de pública/privada de proteção de armazenamento pode ser armazenada localmente no dispositivo de usuário ou em um provedor de armazenamento remoto. Em algumas modalidades, a chave pública/privada de proteção de armazenamento e os dados de credencial criptografados podem ser armazenados em locais diferentes, para reduzir o risco de comprometimento dos dados de credencial.

[00149] A FIG. 7 mostra um exemplo de processo 700 para usar os dados de credencial para realizar transações, de acordo com algumas modalidades. Em algumas modalidades, o processo 700 pode ser usado por um dispositivo de usuário para utilizar os dados de credencial criptografados obtidos usando o processo de provisionamento 500 descrito na FIG. 5. Os aspectos do processo 700 podem ser realizados por um dispositivo de usuário tal como um dispositivo de usuário 101 ou 200. Alternativamente ou adicionalmente, os aspectos do processo 700 podem ser realizados por outras entidades apropriadas.

[00150] No bloco 702, os dados de credencial criptografados são recuperados. Os dados de credencial criptografados podem ser obtidos de um dispositivo de usuário que recebeu a mensagem de resposta de provisionamento ou um armazenamento externo operativamente conectado ao dispositivo de usuário, como discutido acima. Por exemplo, os dados de credencial criptografados podem ser obtidos de um módulo de segurança como um cartão de chip inteligente. Os dados de credencial criptografados podem ser obtidos em resposta a uma indicação de que os dados de credencial sejam necessários para realizar uma transação. Por exemplo, a indicação pode indicar que uma mensagem de solicitação de autenticação ou autorização deve ser gerada. Especificamente, a indicação pode indicar que um criptograma usado para autenticar uma mensagem de solicitação de autorização precisa ser gerado usando os dados de credencial. A indicação pode ser recebida de um aplicativo móvel (por exemplo, aplicativo de pagamento) executando em um

dispositivo de usuário indica que uma operação de pagamento deve ser iniciada. A indicação pode ser recebida de um usuário interagir com o aplicativo móvel (por exemplo, através de uma tela de toque, teclado, mouse, voz, gesto ou outros métodos de entrada de usuário apropriados). A indicação pode ser recebida a partir de um computador do vendedor ou outra transação processamento de entidades (por exemplo, um computador do adquirente, um computador de rede de processamento de pagamento, um computador do emissor, etc.) em comunicação com um dispositivo de usuário.

[00151] No bloco 704, a chave de proteção de armazenamento é obtida. A chave de proteção de armazenamento pode ser obtida de um dispositivo de usuário que recebeu a mensagem de resposta de provisionamento ou um armazenamento externo operativamente conectado ao dispositivo de usuário, como discutido acima. Por exemplo, a chave de proteção de armazenamento pode ser obtida de um módulo de segurança como um cartão de chip inteligente. Se a chave de proteção de armazenamento for criptografada (por exemplo, usando uma KEK) antes de serem armazenadas, a chave de proteção de armazenamento pode ser descriptografada.

[00152] No bloco 706, os dados de credencial criptografados são descriptografados usando a chave de proteção de armazenamento para obter os dados de credencial. Em algumas modalidades, em que a chave de proteção de armazenamento foi usada para criptografar os dados de credencial, a chave de proteção de armazenamento pode ser usada para descriptografar diretamente os dados de credencial criptografados. Em algumas outras modalidades, a chave de proteção de armazenamento pode ser usada para derivar um chave de criptografia de dados (ou chave de criptografia de credencial) usando alguns dados específicos para o dispositivo de usuário (por exemplo, informações de impressão digital de dispositivo tais como identificador de dispositivo, configurações de hardware ou software, etc.). A

chave de criptografia de dados pode ser usada para descriptografar os dados de credencial criptografados.

[00153] No bloco 708, os dados de credencial são usados para realizar as transações. Por exemplo, os dados de credencial podem incluir um parâmetros de LUK ou derivação para derivar uma SUK. LUK ou SUK podem ser usadas para gerar uma chave de criptograma usando o segredo compartilhado atualizado e parâmetros de derivação de chave. Os parâmetros de derivação de chave podem incluir dados de derivação de chaves e/ou algoritmos de derivação de chave indicados nas mensagens de resposta anteriores a partir do computador servidor (por exemplo, a mensagem de resposta de provisionamento ou a mensagem de resposta de autenticação). Por exemplo, a LUK ou a SUK e/ou o segredo compartilhado podem ser fornecidos como entrada em uma função de derivação de chave, juntamente com certos dados de derivação de chave para produzir a chave de criptograma. Como outro exemplo, a LUK ou a SUK pode ser usada como a chave de criptograma. Em tais modalidades, a chave de criptograma pode ser uma chave de uso único que só é válida para uma única transação. Em outras modalidades, a chave de criptograma pode ser usada repetidamente por mais de uma transação.

[00154] Em algumas modalidades, o criptograma ainda é gerado usando dados de transações com base em parâmetros de derivação de criptograma que podem ser enviados como parte da resposta de provisionamento. Em algumas modalidades, o criptograma também pode incluir dados de transação (por exemplo, quantidade de transação, data de transação, etc.) e detalhes de conta de usuário (por exemplo, um token de pagamento, data de expiração de conta, etc.) que são criptografados usando a chave de criptograma.

[00155] O criptograma gerado pode ser usado para conduzir uma transação (ou outra comunicação segura). Geralmente, um criptograma de

transação autentica uma transação. Por exemplo, em algumas modalidades, o dispositivo de usuário pode fornecer um token de pagamento ou PAN e criptograma de transação para um dispositivo de acesso ou computador do vendedor, que pode gerar uma autorização ou mensagem de solicitação de autorização para a transação. A autenticação ou mensagem de solicitação de autorização pode incluir o criptograma de transação. O criptograma de transação pode ser verificado por uma entidade que recebe a autenticação ou mensagem de solicitação de autorização (por exemplo, um computador de rede de processamento de pagamento 105, um computador do emissor 106, um servidor de validação) a fim de determinar se deve aprovar ou negar a transação.

[00156] Em algumas modalidades, logo após o uso dos dados de credencial para realizar uma transação, os dados de credencial podem ser re-criptografados com uma chave de criptografia apropriada que pode ou não ser a chave de proteção de armazenamento. Por exemplo, os dados de credencial podem ser criptografados com uma chave secreta ou privada do dispositivo de usuário. A segurança de dados pode ser melhorada por atualizar a chave de criptografia (por exemplo, periodicamente) e, portanto, criptografar novamente os dados de credencial com a chave de criptografia atualizada.

[00157] A FIG. 8 mostra outro processo de exemplo 800 para usar os dados de credencial para conduzir as transações, de acordo com algumas modalidades. Em algumas modalidades, o processo 800 pode ser usado por um dispositivo de usuário para utilizar os dados de credencial criptografados obtidos usando o processo de provisionamento 600 descrito na FIG. 6. Os aspectos do processo 800 podem ser realizados por um dispositivo de usuário tal como um dispositivo de usuário 101 ou 200. Alternativamente ou adicionalmente, os aspectos do processo 800 podem ser realizados por outras entidades apropriadas.

[00158] No bloco 802, os dados de credencial criptografados são

recuperados. Os dados de credencial criptografados podem ser recuperados de maneira semelhante, conforme descrito no bloco 702 da FIG. 7.

[00159] No bloco 804, a chave privada de proteção de armazenamento é obtida. A chave privada de proteção de armazenamento pode corresponder à chave pública de proteção de armazenamento que foi usada para criptografar os dados de credencial. Em algumas modalidades, a chave pública de proteção de armazenamento pode ser obtida primeiro e usada para recuperar a chave privada de proteção de armazenamento correspondente. Em alguns casos, a chave privada de proteção de armazenamento pode ser criptografada durante o armazenamento (por exemplo, usando uma KEK) e, portanto, precisa ser decifrada antes de ser usada para descriptografar os dados de credencial criptografados. A chave privada de proteção de armazenamento pode ser obtida a partir do dispositivo de usuário ou um provedor de armazenamento externo.

[00160] No bloco 806, os dados de credencial criptografados são descriptografados usando a chave privada de proteção de armazenamento para obter os dados de credencial. Em algumas modalidades, em que a chave pública de proteção de armazenamento foi usada para criptografar diretamente os dados de credencial, a chave pública de proteção de armazenamento pode ser usada para descriptografar diretamente os dados de credencial criptografados. Em algumas outras modalidades, a chave pública de proteção de armazenamento pode ser usada para derivar uma chave de criptografia de dados (ou chave de criptografia de credencial) usando alguns dados específicos para o dispositivo de usuário (por exemplo, informações de impressão digital de dispositivo tais como identificador de dispositivo, configurações de hardware ou software, etc.). A chave de criptografia de dados foi usada para criptografar os dados de credencial. Em tais modalidades, a chave privada de proteção de armazenamento pode ser utilizada para, em conjunto com os dados específicos de usuário/dispositivo

derivar uma chave de descriptografia de dados, que é usada para descriptografar os dados de credencial criptografados.

[00161] No bloco 808, os dados de credencial são usados para realizar transações de forma semelhante, conforme descrito no bloco 708 da FIG. 7.

[00162] C. Computador servidor

[00163] A FIG. 9 mostra outro processo de exemplo 900 para provisionamento com segurança de dados de credencial a um dispositivo de usuário, de acordo com algumas modalidades. Em tais modalidades, os dados de credencial podem ser protegidos por uma chave de proteção de armazenamento que é determinada com base em um segredo compartilhado. Os aspectos do processo 900 podem ser realizados por um computador servidor como um dispositivo de servidor ou computador 102, 103, 104, 105, 106 ou 300. Por exemplo, o processo 900 pode ser executado por um servidor de provisionamento. Alternativamente ou adicionalmente, os aspectos do processo 900 podem ser realizados por outras entidades apropriadas.

[00164] Normalmente, antes do método 900, o computador servidor mantém um par de chaves de servidor estáticas. O par de chaves de servidor estáticas pode incluir uma chave pública (isto é, uma "chave pública de servidor estática") e uma chave privada (isto é, uma "chave privada de servidor estática"). O computador servidor também pode incluir um certificado de "computador servidor" incluindo a chave pública de servidor estática. O certificado do computador servidor pode ser assinado por uma autoridade de certificação, tais como rede de processamento de pagamento 105 ou computador do emissor 106.

[00165] No bloco 902, uma mensagem de solicitação de provisionamento é recebida de um dispositivo de usuário. A mensagem de solicitação de fornecimento inclui uma chave pública de usuário avulsa como discutidos no bloco 502 da FIG. 5. Uma mensagem de solicitação de provisionamento de exemplo é mostrada na FIG. 12. Em uma modalidade, a

chave pública de usuário avulsa pode ser gerada pelo dispositivo de usuário usando uma chave pública efêmera ou uma chave pública estática ou semi-estático com dados de mascaramento como um fator de identificação. Em outro exemplo, a chave pública avulsa pode ser apenas a chave pública efêmera, sem qualquer uso de dados de ocultação. Em alguns casos, a mensagem de solicitação de provisionamento pode incluir a chave pública de usuário avulsa, mas não inclui os dados de solicitação criptografados. Em tais implementações, certas etapas abaixo podem não ser necessárias, como será compreendido por um versado na técnica.

[00166] Para descriptografar os dados de solicitação criptografados, um segredo compartilhado de solicitação pode ser gerado usando a chave pública de usuário avulsa recebida acima e uma chave privada de servidor estática. O segredo compartilhado de solicitação pode ser gerado usando qualquer método adequado, como ECDH.

[00167] Uma chave de sessão de solicitação pode ser gerada usando o segredo compartilhado de solicitação e dados suplementares tais como dados de derivação de chaves, se necessário. Normalmente, os mesmos dados suplementares usados para gerar a chave de sessão de solicitação no dispositivo de usuário podem ser usados aqui.

[00168] Os dados de solicitação criptografados podem ser descriptografados usando a chave de sessão de solicitação para obter os dados de solicitação. Os dados de solicitação incluem os dados de identificação, um identificador de dispositivo de usuário, dados de autenticação, juntamente com quaisquer outros dados adequados destinados ao computador servidor. Por exemplo, os dados de solicitação também podem incluir informações de configuração de cliente e/ou diretivas para o serviço. Em alguns casos, os dados de solicitação também incluem a chave pública de usuário avulsa. O identificador de dispositivo do usuário pode incluir quaisquer dados adequados para identificar o dispositivo do usuário. Os dados de identificação

podem incluir quaisquer dados ou informações associadas a um usuário ou dispositivo do usuário. Exemplos de dados de identificação podem incluir um nome de um usuário associado ao dispositivo do usuário, uma organização associada ao dispositivo do usuário, as informações de pagamento tais como Número da Conta Principal (PAN) ou token associado ao dispositivo do usuário, uma data de expiração associada a PAN ou token, um certificado associado ao dispositivo do usuário, um IMEI ou número de série de dispositivo do usuário, etc.

[00169] O dispositivo de usuário pode ser autenticado ou verificado usando os dados de solicitação. Os dados de identificação podem ser verificados usando o identificador de dispositivo de usuário. Por exemplo, em algumas modalidades, o identificador de dispositivo do usuário pode ser usado para recuperar os dados de identificação correspondentes de um banco de dados de dispositivo. Os dados de identificação descriptografados podem, então, ser verificados por comparação aos dados de identificação recebidos. Em algumas modalidades, os dados de identificação incluem o identificador de dispositivo de usuário.

[00170] Os dados de autenticação associados ao identificador de dispositivo de usuário e/ou os dados de identificação podem ser obtidos. Os dados de autenticação podem incluir quaisquer dados ou informações adequadas para autenticar um usuário ou dispositivo do usuário. Exemplos de dados de autenticação podem incluir uma senha ou frase-chave, uma chave secreta (por exemplo, uma chave privada), etc. Em algumas modalidades, os dados de autenticação podem ser obtidos de um banco de dados de dispositivo.

[00171] O fator de identificação pode ser gerado usando os dados de autenticação recuperados e os dados de identificação. Um fator de identificação pode incluir quaisquer dados ou informações determinados a partir de dados de identificação e/ou dados de autenticação. Por exemplo, em

algumas modalidades, o fator de identificação pode ser gerado por uma combinação dos dados de identificação e a autenticação de hash.

[00172] A chave pública de usuário avulsa pode ser verificada para garantir que a chave pública de usuário avulsa corresponda a um valor esperado. Por exemplo, em alguns casos, uma chave pública avulsa cega pode ser gerada usando uma chave pública avulsa extraída dos dados de solicitação descriptografada e o fator de identificação determinado acima. A chave pública avulsa cega pode, então, ser comparada à chave pública avulsa recebida como parte da mensagem de solicitação (por exemplo, em uma porção de texto não codificado da mensagem de solicitação) para garantir que as teclas correspondam. Se as chaves corresponderem, o dispositivo do usuário pode ser autenticado. Caso contrário, a autenticação pode falhar.

[00173] Deve ser observado que este método de autenticação (isto é, verificando uma chave efêmera combinada) fornece a vantagem de que os dados de autenticação, que podem ser sensíveis, não necessitam ser transmitidos em texto simples, mesmo em forma criptografada. Assim, mesmo se a chave privada de servidor estática estiver comprometida mais tarde (embora improvável), os dados de autenticação de texto simples não são expostos. Além disso, uma vez que a cegueira de uma chave seja geralmente irreversível, um invasor não pode derivar o fator de identificação e muito menos os dados de autenticação usados para gerar o fator de identificação, mesmo com o conhecimento de ambas a chave pública de usuário cega e a chave pública de usuário não cega (por exemplo, chave pública efêmera).

[00174] No bloco 904, um segredo compartilhado de resposta pode ser gerado usando a chave privada de servidor estática e chave pública de usuário avulsa. Em algumas modalidades, a chave pública de servidor estática e/ou a chave privada de servidor estática podem ser cegas usando um nonce criptográfico (por exemplo, um valor de dados aleatórios ou pseudoaleatórios) e/ou o fator de identificação. O segredo compartilhado de resposta pode ser

gerado usando uma chave privada de servidor estática cega e chave pública de usuário avulsa. Em uma modalidade alternativa, a chave privada de servidor estática não é cega. Em vez disso, a chave pública de usuário avulsa é cega. O segredo compartilhado de resposta pode ser gerado usando qualquer método adequado, como ECDH.

[00175] No bloco 906, os dados de credencial a serem incluídos na mensagem de resposta provisória são identificados. Os dados de credencial podem incluir quaisquer dados especificamente provisionados para o dado dispositivo de usuário (por exemplo, dispositivo móvel) ou um dado grupo de dispositivos, de modo a habilitar o dispositivo de usuário para realizar transações (por exemplo, transações de pagamento). Os exemplos de dados de credencial podem incluir tokens, PAN ou outras informações de conta, uma ou mais chaves (por exemplo, LUKs usadas para gerar criptogramas, chaves públicas estáticas cegas ou não cegas, etc.), parâmetros de derivação de chave (por exemplo, para derivar uma SUK que é usada gerar um criptograma, uma chave secreta compartilhada, uma chave de criptografia, etc.), parâmetros de derivação de chave, as informações de cadeia de certificados, parâmetros de transação e todos os outros dados apropriados.

[00176] A mensagem de resposta de provisionamento também pode incluir outras informações, tais como a cadeia de certificado do computador servidor, uma chave pública de servidor estática, um nonce criptográfico e similares. A cadeia de certificado do computador servidor pode ser validada pelo dispositivo de usuário para verificar a identidade do computador servidor, conforme discutido na FIG. 5. A chave pública de servidor estática pode ou não ser cega. A chave pública de servidor estática pode ser usada pelo dispositivo de usuário para gerar o segredo compartilhado de resposta.

[00177] No bloco 908, uma chave de sessão de resposta pode ser determinada usando o segredo compartilhado de resposta e dados de derivação de chave, se necessário. Os dados de derivação de chaves podem

incluir dados específicos para o dispositivo de usuário ou usuário (por exemplo, identificador de dispositivo, identificador de usuário, etc.). Em uma modalidade, a chave de sessão de resposta pode ser determinada de forma semelhante, conforme descrito no bloco 510 da FIG. 5.

[00178] No bloco 910, uma chave de proteção de armazenamento pode ser determinada a partir do segredo compartilhado de resposta. A chave de proteção de armazenamento pode ser diferente da chave de sessão de resposta e utilizável para criptografar os dados de credenciais. Em uma modalidade, a chave de proteção de armazenamento pode ser determinada de forma semelhante, conforme descrito no bloco 514 da FIG. 5. Por exemplo, em uma modalidade alternativa, a chave de proteção de armazenamento pode ser uma chave pública fornecida pelo dispositivo de usuário (por exemplo, como parte da mensagem de solicitação de provisionamento mostrada na FIG. 13) e não gerada a partir do segredo compartilhado de resposta.

[00179] No bloco 912, os dados de credencial podem ser criptografados usando a chave de proteção de armazenamento para gerar os dados de credencial criptografados. Em uma modalidade, a chave de proteção de armazenamento pode ser usada diretamente para criptografar os dados de credencial. Em outra modalidade, a chave de proteção de armazenamento pode ser usada com dados específicos para o usuário ou dispositivo de usuário para o qual os dados de credencial são provisionados para derivar uma chave de criptografia de credencial, que é usada, então, para criptografar os dados de credencial. Em algumas modalidades, os dados de credencial e/ou proteção de armazenamento podem ser eliminados logo após a criação dos dados de credencial criptografados.

[00180] No bloco 914, alguns ou todos os dados da mensagem de resposta de provisionamento podem ser criptografados usando a chave de sessão de resposta. Por exemplo, o nonce criptográfico, a cadeia de certificado do computador servidor, os dados de derivação de chaves, os descritores de

conjunto de codificação e outros dados apropriados podem ser cifrados usando a chave de sessão de resposta. Os dados de credencial criptografados podem ou não ser criptografados usando a chave de sessão de resposta. Uma mensagem de resposta de provisionamento de exemplo é mostrada na FIG. 12.

[00181] No bloco 916, uma mensagem de resposta de provisionamento criptografada é enviada ao dispositivo de usuário. A mensagem de resposta de provisionamento pode passar através de um ou mais intermediários (por exemplo, rede não confiável) antes de chegar ao dispositivo do usuário. O dispositivo de usuário pode processar a mensagem de provisionamento criptografada de acordo com o processo de 700 da FIG. 7. Uma mensagem de resposta de provisionamento de exemplo é mostrada na FIG. 12.

[00182] A FIG. 10 mostra outro processo de exemplo 1000 para provisionamento com segurança de dados de credencial a um dispositivo do usuário, de acordo com algumas modalidades. Em tais modalidades, os dados de credencial podem ser protegidos por uma chave pública de armazenamento de proteção fornecida pelo dispositivo de usuário. Os aspectos do processo 1000 podem ser realizados por um computador servidor como um dispositivo de servidor ou computador 102, 103, 104, 105, 106 ou 300. Por exemplo, o processo 1000 pode ser executado por um servidor de provisionamento. Alternativamente ou adicionalmente, os aspectos do processo 1000 podem ser realizados por outras entidades apropriadas.

[00183] Normalmente, antes do método 1000, o computador servidor mantém um par de chaves de servidor estáticas. O par de chaves de servidor estáticas pode incluir uma chave pública (isto é, uma "chave pública de servidor estática") e uma chave privada (isto é, uma "chave privada de servidor estática"). O computador servidor também pode incluir um certificado de "computador servidor" incluindo a chave pública de servidor estática. O certificado do computador servidor pode ser assinado por uma

autoridade de certificação, tais como rede de processamento de pagamento 105 ou computador do emissor 106.

[00184] No bloco 1002, uma mensagem de solicitação de provisionamento é recebida de um dispositivo de usuário. A mensagem de solicitação de provisionamento inclui uma chave pública de usuário avulsa e uma chave pública de proteção de armazenamento tal como discutido na FIG. 6. Uma mensagem de solicitação de provisionamento de exemplo é mostrada na FIG. 13.

[00185] Como discutido na FIG. 9, um segredo compartilhado de solicitação e uma chave de sessão de solicitação podem ser gerados e a chave de sessão de solicitação pode ser usada para descriptografar a mensagem de solicitação de provisionamento para obter os dados de solicitação. Os dados de solicitação podem incluir a chave pública de proteção de armazenamento e a chave pública de usuário avulsa. O dispositivo de usuário pode ser autenticado ou verificado usando os dados de solicitação.

[00186] No bloco 1004, um segredo compartilhado de resposta pode ser gerado usando a chave privada de servidor estática e chave pública de usuário avulsa, conforme discutido no bloco 904 da FIG. 9.

[00187] No bloco 1006, os dados de credencial a serem incluídos na mensagem de resposta provisória são identificados, conforme discutido no bloco 906 da FIG. 9.

[00188] A mensagem de resposta de provisionamento também pode incluir outras informações, tais como a cadeia de certificado do computador servidor, uma chave pública de servidor estática, um nonce criptográfico e similares. A cadeia de certificado do computador servidor pode ser validada pelo dispositivo de usuário para verificar a identidade do computador servidor, conforme discutido na FIG. 6. A chave pública de servidor estática pode ou não ser cega. A chave pública de servidor estática pode ser usada pelo dispositivo de usuário para gerar o segredo compartilhado de resposta.

[00189] No bloco 1008, uma chave de sessão de resposta pode ser determinada usando o segredo compartilhado de resposta e dados de derivação de chave, se necessário, conforme discutido no bloco 908 da FIG. 9.

[00190] No bloco 1010, os dados de credencial podem ser criptografados usando a chave pública de proteção de armazenamento recebeu no bloco 1002 acima. Em uma modalidade, a chave pública de proteção de armazenamento pode ser usada diretamente para criptografar os dados de credencial. Em outra modalidade, a chave pública de proteção de armazenamento pode ser usada com dados específicos para o usuário ou dispositivo de usuário para o qual os dados de credencial são provisionados para derivar uma chave de criptografia de credencial, que é usada, então, para criptografar os dados de credencial.

[00191] No bloco 1012, alguns ou todos os dados da mensagem de resposta de provisionamento podem ser criptografados usando a chave de sessão de resposta, conforme discutido no bloco 914 da FIG. 9.

[00192] No bloco 1014, uma mensagem de resposta de provisionamento criptografada é enviada ao dispositivo de usuário, conforme discutido no bloco 916 da FIG. 9. Uma mensagem de solicitação de provisionamento de exemplo é mostrada na FIG. 13.

D. Fluxo de Dados de Exemplo

[00193] A FIG. 11 mostra um diagrama de fluxo de dados 1100 para provisionamento e usando os dados de credencial, de acordo com as modalidades. Conforme ilustrado, uma chave de proteção de armazenamento (SK_2) pode ser gerada no tempo de provisionamento a partir de um protocolo de acordo de chave, como Diffie-Hellman. Em algumas modalidades, o acordo de chave usado para gerar a chave de proteção de armazenamento pode ser o mesmo acordo de chave usado para gerar as chaves de sessão discutidas neste documento. Por exemplo, a chave de

proteção de armazenamento pode ser derivada de um segredo compartilhado também é usado para gerar uma chave de sessão. Em alternativas modalidades, a chave de proteção de armazenamento pode ser gerada usando um acordo de chave diferente que o acordo de chave usado para gerar as chaves de sessão. A chave de proteção de armazenamento pode ser usada para proteger os dados de credencial, como os dados de credencial (por exemplo, LUK), enquanto que as chaves de sessão podem ser usadas para proteger as mensagens em trânsito. Assim, a chave de proteção de armazenamento pode ser usada em conjunto com as chaves de sessão, como discutido neste documento, para fornecer proteção end-to-end dos dados confidenciais.

[00194] Em algumas modalidades, a chave de proteção de armazenamento pode ter aproximadamente o mesmo ciclo de vida (por exemplo, data de início efetivo e/ou tempo de expiração) que os dados confidenciais (por exemplo, uma LUK) que são protegidos usando a chave de proteção de armazenamento. Assim, quando novos dados de credencial (por exemplo, LUK) foram gerados por um computador servidor, uma nova chave de proteção de armazenamento também é gerada para proteger os dados de credencial. Em algumas modalidades, os dados de credencial (por exemplo, LUK) e/ou a chave de proteção de armazenamento pode ser associada com o indicador de ciclo de vida (por exemplo, um contador) que indica quando/se os dados de credencial e/ou a chave de proteção de armazenamento expiraria. Após o vencimento, os dados de credencial e/ou chave de proteção de armazenamento podem ser excluídos de um dispositivo de usuário. Em algumas outras modalidades, a chave de proteção de armazenamento pode ter um ciclo de vida mais longo ou mais curto do que os dados confidenciais.

[00195] Antes da primeira utilização dos dados de credencial, a chave de proteção de armazenamento (SK_2) pode ser codificada (por exemplo, de acordo com AES) usando uma chave de criptografia de chave (KEK) e armazenadas em um armazenamento de segurança. O armazenamento de

segurança pode ser fornecido por um dispositivo de usuário e/ou um provedor de armazenamento externo acessível pelo dispositivo de usuário.

[00196] Os dados de credencial criptografados (Enc_LUK) são provisionados a um dispositivo de usuário em uma mensagem de resposta de provisionamento no tempo de provisionamento. Posteriormente e antes da primeira utilização dos dados de credencial, podem ser armazenados os dados de credencial, na forma criptografada (Enc_LUK), no dispositivo de usuário e/ou em um armazenamento externo. Os dados confidenciais criptografados podem ser obtidos e descriptografados somente quando necessário (por exemplo, no tempo de transação), minimizando, assim, a exposição dos e limitar o risco de comprometimento dos dados confidenciais.

[00197] No tempo de transação, os dados de credencial criptografados (Enc_LUK) podem ser obtidos e descriptografados (AES^{-1}) para obter os dados de credencial (LUK). Em algumas modalidades, a chave de proteção de armazenamento (SK_2) é usada diretamente como uma chave de descriptografia para descriptografar os dados confidenciais criptografados. Em algumas outras modalidades, a chave de proteção de armazenamento (SK_2) pode ser usada para descriptografar indiretamente os dados de credencial criptografados, como discutido abaixo.

[00198] Como ilustrado na FIG. 11, a chave de proteção de armazenamento (SK_2) pode ser usada como entrada em uma função de derivação de chave opcional (KDF), juntamente com os dados de derivação de chaves (Dados da Derivação), para derivar uma chave de criptografia de dados (DEK). A DEK pode ser usada para descriptografar os dados de credencial criptografados (Enc_LUK) para obter os dados de credencial (por exemplo, LUK). Em algumas modalidades, os dados de derivação de chave não são fornecidos na mensagem de resposta de provisionamento, mas são conhecidos para o dispositivo de usuário e o computador servidor. Os dados de derivação de chaves podem ser exclusivos e/ou específicos ao dispositivo

de usuário como um identificador de dispositivo, uma impressão digital de dispositivo e similares. Uma impressão digital de dispositivo é informações coletadas sobre um dispositivo com a finalidade de identificar o dispositivo. Tal informação pode incluir várias informações de configuração de hardware e/ou software em quaisquer níveis apropriados tais como as configurações de navegador, configurações de TCP/IP, configurações sem fio, impressão digital de sistema operacional (OS), desvio de relógio de hardware e similares.

[00199] Os dados de credencial (LUK) podem ser usados para realizar uma ou mais transações. Por exemplo, os dados de credencial (LUK) podem ser usados para gerar os criptogramas de transação que podem ser usados para autenticar o dispositivo de usuário. Em algumas modalidades, a mensagem de resposta também pode indicar se deseja usar a função de derivação de chave opcional (KDF), como obter dados de derivação usados para a KDF ou outras diretivas sobre os aspectos de descriptografia dos dados de credencial criptografados.

E. Exemplo de Mensagens de Provisionamento

[00200] A FIG. 12 mostra um primeiro exemplo de mensagem de solicitação de provisionamento 1202 e uma mensagem de resposta de provisionamento correspondente 1210, de acordo com algumas modalidades. Por exemplo, a mensagem de solicitação de provisionamento 1202 pode ser enviada por um dispositivo de usuário (por exemplo, dispositivo de usuário 101) para um computador servidor de provisionamento (por exemplo, computador de rede de processamento de pagamento 105, computador de emissor 106, computador servidor 300); e a mensagem de resposta de provisionamento 1210 pode ser enviada a partir do computador servidor de provisionamento para o dispositivo de usuário durante um processo de provisionamento, como discutido na FIGS. 4-11.

[00201] Como mostrado na FIG. 12, em algumas modalidades, a

mensagem de solicitação de provisionamento 1202 podem incluir três porções de dados: uma porção de texto não codificado 1204, uma porção de texto codificado 1206 e um código de autenticação de mensagens (MAC) 1208 para a mensagem. A porção de texto não criptografado 1204 pode incluir uma única chave pública do dispositivo de usuário (que pode ou não ser cega). O MAC pode ser utilizado para a detecção de erros e/ou correção. A integridade da porção de texto não codificado 1204 e a porção de texto codificado 1206 é protegida pelo MAC 1208. O MAC 1222 pode ser gerado usando a mesma chave ou uma chave diferente do que a chave usada para gerar o texto codificado. Parte ou todas as porções dos dados de solicitação podem ser criptografadas (por exemplo, usando uma chave de sessão de solicitação derivada de um segredo compartilhado de solicição) para produzir a porção de texto codificado 1206. Os dados de solicitação que são criptografados podem incluir dados de identificação e quaisquer outros dados adequados.

[00202] A mensagem de resposta de provisionamento 1210 correspondente à mensagem de solicitação de provisionamento 1202 podem também incluir três porções de dados: uma porção de texto não codificado 1212, uma porção de texto codificado 1214 e um MAC 1216. A porção de texto não codificado 1212 pode incluir uma chave pública de servidor (que pode ser cega em algumas modalidades) e dados de credencial criptografados 1218. A chave pública de servidor pode ajudar o dispositivo de usuário a derivar a chave de sessão de resposta que pode ser usada para descriptografar a mensagem de resposta. Os dados de credencial criptografados 1218 podem ser criptografados usando uma chave de proteção de armazenamento separada que é diferente da chave de sessão de resposta (SK_s) usada para criptografar os dados de resposta de provisionamento. Os dados de credencial criptografados 1218 podem incluir uma porção de texto codificado 1220 e um MAC 1222. A porção de texto codificado 1220 pode incluir dados de credencial criptografados como uma LUK codificado, parâmetros de

derivação de chave codificados para derivar uma SUK, credenciais de pagamento como parâmetros de token e/ou token e similares. O MAC 1222 pode ser gerado para proteger a integridade da porção de texto codificada 1220 e a porção de texto não codificado 1212. O MAC 1222 pode ser gerado usando a mesma chave ou uma chave diferente do que a chave usada para gerar o texto codificado.

[00203] A porção de texto codificado 1214 da mensagem de resposta 1210 pode incluir outros dados de resposta que foram criptografados usando a chave de sessão de resposta, tais como um nonce criptográfico, uma cadeia de certificado do computador servidor, dados de derivação de chave, descritores de conjunto codificado e quaisquer outros dados de resposta adequados. Por exemplo, a porção de texto codificado 1214 pode incluir dados que indicam a função de derivação de chave (KDF) e/ou os dados de derivação que podem ser usados para derivar a chave de proteção de armazenamento ou chave de criptografia de credencial ou quaisquer outras chaves.

[00204] Embora a FIG. 12 mostre os dados de credencial criptografados 1218 como incluído na porção de texto não codificado 1212 da mensagem de resposta 1210, em algumas outras modalidades, pelo menos uma porção dos dados de credencial criptografados 1218 pode ser adicionalmente criptografada (por exemplo, usando a chave de sessão de resposta) e armazenada na porção de texto codificado 1214 da mensagem de resposta 1210.

[00205] A FIG. 13 mostra um segundo exemplo de uma mensagem de solicitação de provisionamento 1302 e uma mensagem de resposta de provisionamento correspondente 1310, de acordo com algumas modalidades. Por exemplo, a mensagem de solicitação de provisionamento 1302 pode ser enviada por um dispositivo de usuário (por exemplo, dispositivo de usuário 101) para um computador servidor de provisionamento (por exemplo, computador de rede de processamento de pagamento 105, computador de

emissor 106, computador servidor 300); e a mensagem de resposta de provisionamento 1310 pode ser enviada a partir do computador servidor de provisionamento para o dispositivo de usuário durante um processo de provisionamento, como discutido na FIGS. 4-11. Ao contrário da FIG. 12, a mensagem de solicitação 1302 na FIG. 12 incluem uma chave pública de proteção de armazenamento que é usada criptografar os dados de credencial (por exemplo, LUK) na mensagem de resposta 1310.

[00206] Como mostrado na FIG. 13, em algumas modalidades, a mensagem de solicitação de provisionamento 1302 podem incluir três porções de dados: uma porção de texto não codificado 1304, uma porção de texto codificado 1306 e um código de autenticação de mensagens (MAC) 1308 para a mensagem. A porção de texto não criptografado 1304 pode incluir uma única chave pública do dispositivo de usuário (que pode ou não ser cega). A chave pública avulsa pode ser semelhante ao descrito na mensagem de solicitação 1204 da FIG. 12. O MAC pode ser utilizado para a detecção de erros e/ou correção. A integridade da porção de texto não codificado 1304 e a porção de texto codificada 1306 é protegida pelo MAC 1308. O MAC 1308 pode ser gerado usando a mesma chave ou uma chave diferente do que a chave usada para gerar o texto codificado. Parte ou todas as porções dos dados de solicitação podem ser criptografadas (por exemplo, usando uma chave de sessão de solicitação derivada de um segredo compartilhado de solicitação) para produzir a porção de texto codificado 1306.

[00207] A porção de texto codificado 1308 da mensagem de solicitação 1302 pode incluir uma chave pública de proteção de armazenamento 1307 que pode ser usada para criptografar os dados de credencial (por exemplo, LUK) na mensagem de resposta 1310. A chave pública de proteção de armazenamento 1307 pode ser uma chave pública de um par de chaves de proteção de armazenamento pública/privada gerado e/ou mantido pelo dispositivo de usuário. A chave privada de proteção de armazenamento pode

ser usada para descriptografar os dados de credencial criptografados. O par de chaves de proteção de armazenamento pode ser um par de chaves diferentes do que o par de chaves pública/particular de usuário usado para gerar os segredos compartilhados (por exemplo, o segredo compartilhado de solicitação e o segredo compartilhado de resposta). Alternativamente, o par de chaves de proteção de armazenamento e o par de chaves de usuário pode compartilhar a mesma chave privada. Por exemplo, a mesma chave privada de usuário pode ser usada para gerar duas chaves públicas, uma com a finalidade de proteger os dados de credencia (chave pública de proteção de armazenamento) e outra com a finalidade de proteger as mensagens em trânsito.

[00208] As chaves pública e/ou privada de proteção de armazenamento podem ser chaves de uso limitado. Por exemplo, um novo par de chaves de proteção de armazenamento pode ser gerado para cada nova solicitação ou nova transação. Em outros casos, um novo par de chaves de proteção de armazenamento pode ser gerado por um período predeterminado de tempo ou para um número predeterminado de solicitações ou transações. Em algumas modalidades, o par de chaves pública/privada de armazenamento pode ter o mesmo ciclo de vida dos dados de credencial (por exemplo, LUK). Em outras modalidades, o par de chaves pública/privada de proteção de armazenamento pode ter um ciclo de vida mais curto ou mais longo do que os dados de credencial.

[00209] A mensagem de resposta de provisionamento 1310 pode também incluir três porções de dados: uma porção de texto não codificado 1312, uma porção de texto codificado 1314 e um MAC 1316. A porção de texto não codificado 1312 pode incluir uma chave pública de servidor (que pode ser cega em algumas modalidades). A chave pública de servidor pode ajudar o dispositivo de usuário a derivar a chave de sessão para descriptografar a mensagem de resposta. Alguns ou todos a dados podem ser

criptografados usando um segredo compartilhado de resposta (SK_s) para produzir a porção de texto codificado 1314. Por exemplo, a porção de texto codificado 1314 pode incluir dados de credencial criptografados 1318 que são criptografados usando a chave pública de proteção de armazenamento 1307 que é fornecida na mensagem de solicitação 1302. Os dados de credencial criptografados 1318 podem incluir uma porção de texto codificado 1320 e um MAC 1322 desta. A porção de texto codificado 1320 pode incluir dados de credencial criptografados como uma LUK codificado, parâmetros de derivação de chave codificados para derivar uma SUK, credenciais de pagamento como parâmetros de token e/ou token e similares. A integridade da porção de texto não codificado 1312 e a porção de texto codificada 1314 é protegida pelo MAC 1316. O MAC 1316 pode ser gerado usando a mesma chave ou uma chave diferente do que a chave usada para gerar o texto codificado. Em algumas modalidades, os dados de credencial criptografados podem ou não ser adicionalmente criptografados usando a chave de sessão de resposta.

[00210] A porção de texto codificado 1314 da mensagem de resposta 1310 pode incluir outros dados de resposta que foram criptografados usando a chave de sessão de resposta, tais como um nonce criptográfico, uma cadeia de certificado do computador servidor, dados de derivação de chave, descritores de conjunto codificado e quaisquer outros dados de resposta adequados.

[00211] Embora a FIG. 13 mostra os dados de credencial criptografados 1318 como incluídos na porção de texto codificado 1314 da mensagem de resposta de provisionamento 1310, em outras modalidades, pelo menos uma porção dos dados de credencial criptografados 1318 pode ser incluída na porção de texto não codificado 1312 da mensagem de resposta de provisionamento 1310.

III. Tipos de Transações

[00212] As técnicas descritas neste documento podem ser usadas para

configurar os dados de credencial para conduzir as transações. As transações podem incluir as transações de pagamento ou de não pagamento. Por exemplo, um dispositivo de usuário pode se comunicar com um computador servidor para acessar um ou mais recursos em uma ou mais operações sem pagamento.

[00213] Por exemplo, o dispositivo de usuário e o computador servidor podem se comunicar durante o processo de provisionamento para provisionar credenciais (por exemplo, uma LUK) ao dispositivo de usuário. A comunicação pode ser realizada da maneira similar conforme discutido acima nas FIGs. 4-10.

[00214] As credenciais provisionadas podem ser usadas em gerar criptogramas ou outros tokens de autenticação usados para autenticar o dispositivo de usuário em operações subsequentes. Os tokens de autenticação ou criptograma podem ser verificados por um computador servidor que pode ou não ser o mesmo que o servidor de provisionamento. Baseado nos resultados de autenticação, acesso aos recursos de servidor pode ser fornecido ou negado.

[00215] Em várias modalidades, um recurso pode incluir recursos de computação que são acessíveis através de um dispositivo de computação. Tais recursos de computação podem incluir objetos de dados, dispositivos de computação ou componentes de hardware/software destes (por exemplo, CPU, memória, aplicativos), serviços (por exemplo, serviços de web), sistemas de computador virtual, armazenamento ou gerenciamento de dados, conexões de rede e interfaces e similares. Por exemplo, um recurso pode incluir um ou mais dispositivos de computação (por exemplo, desktop, laptop, tablet, celular), arquivos ou outros dados armazenados no dispositivo de computação, memória ou dispositivo de armazenamento de dados associados aos dispositivos de computação, aplicativos instalados no dispositivos de computador, dispositivos periféricos associados aos dispositivos de

computação tais como dispositivos de entrada/saída (por exemplo, teclado, mouse, microfone, tela sensível ao toque, impressora), interfaces de rede, serviços fornecidos pelos dispositivos de computação e similares. Os recursos de computação podem incluir serviços baseados em nuvem ou online ou funcionalidades fornecidas pelos provedores de serviços. Os recursos de computação podem incluir um ou mais dispositivos de armazenamento, nós, sistemas ou uma porção dos mesmos tal como uma partição, um volume, um setor e similares. Os recursos de computação também podem incluir objetos de dados tais como credenciais (por exemplo, nome de usuário, senhas, chaves criptográficas, certificações digitais). Nesse caso, uma credencial mestra pode ser necessária para acessar essas credenciais. Um recurso pode incluir recursos tangíveis e/ou intangíveis. Os recursos tangíveis podem incluir dispositivos, edifícios e objetos físicos. Os recursos intangíveis podem incluir serviços e tempo, por exemplo.

IV. Aparelho de Computador

[00216] A FIG. 14 mostra um diagrama de bloco de nível elevado de um sistema de computador que pode ser usado para implementar qualquer uma das entidades ou componentes descritos acima. Os subsistemas mostrados na FIG. 14 são interligados através de um barramento de sistema 1475. Os subsistemas adicionais incluem uma impressora 1403, teclado 1406, disco fixo 1407 e monitor 1409, que é acoplado ao adaptador de vídeo 1404. Os periféricos e os dispositivos de entrada/saída (I/O), que se acasalam ao controlador I/O 1400, podem ser conectados ao sistema de computador através de qualquer número de meios conhecidos na técnica, como uma porta serial. Por exemplo, a porta serial 1405 ou a interface externa 1408 pode ser usada para conectar o aparelho de computador a uma rede de área ampla tal como a Internet, um dispositivo de entrada de mouse ou um digitalizador. A interligação através do barramento de sistema 1475 permite que o processador central 1402 se comunique com cada subsistema e controle a execução de

instruções da memória de sistema 1401 ou o disco fixo 1407, assim como a troca de informações entre os subsistemas. A memória de sistema 1401 e/ou o disco fixo pode incorporar um meio legível por computador.

[00217] A meio de armazenamento e meio legível por computador para conter código, ou porções de código, pode incluir qualquer meio apropriado conhecido ou usado na técnica, incluindo a mídia de armazenamento e meios de comunicação, tais como, mas não limitado a, meio volátil e não volátil, removível e irremovível, implementado em qualquer método ou tecnologia para armazenamento e/ou transmissão de informações, tais como instruções legíveis por computador, estruturas de dados, módulos de programa ou outros dados, incluindo RAM, ROM, EEPROM, memória flash ou outras tecnologias de memória, CD-ROM, disco versátil digital (DVD) ou outro armazenamento óptico, cassetes magnéticos, fita magnética, disco magnético de armazenamento ou outros dispositivos de armazenamento magnético, sinais de dados, transmissões de dados ou qualquer outro meio que possa ser usado para armazenar ou transmitir as informações desejadas e que possa ser acessado pelo computador. Com base na divulgação e nos ensinamentos apresentados neste documento, um indivíduo de conhecimento comum na técnica irá apreciar outras formas e/ou métodos para implementar as várias modalidades.

[00218] A descrição acima é ilustrativa e não restritiva. Muitas variações da invenção podem tornar-se aparente para aqueles qualificados na técnica mediante revisão da divulgação. O escopo da invenção pode, portanto, ser determinado não com referência a descrição acima, porém, em vez disso, pode ser determinado com referência as reivindicações pendentes ao longo de seu escopo completo ou equivalentes.

[00219] Deve ser entendido que qualquer uma das modalidades da presente invenção pode ser implementada sob a forma de lógica de controle utilizando hardware (por exemplo, um circuito integrado de aplicação

específica ou dispositivo de porta programável em campo) e/ou usando o software de computador com um processador programável geral de uma maneira integrada ou modular. Como usado aqui, um processador inclui um processador de único núcleo, processador de vários núcleos em um mesmo chip integrado ou várias unidades de processamento em uma única placa de circuito ou em rede. Com base na divulgação e nos ensinamentos fornecidos aqui, um indivíduo de conhecimento comum na técnica vai saber e observar outras maneiras e/ou métodos para implementar as modalidades da presente invenção usando hardware e uma combinação de hardware e software.

[00220] Qualquer um dos componentes de software ou funções descritas nesta aplicação pode ser implementado como código de software a ser executado por um processador usando qualquer linguagem de computador adequado, tais como, por exemplo, Java, C, C++, c#, Objective-C, Swift ou linguagem de script como Perl ou Python usando, por exemplo, técnicas convencionais ou orientadas a objeto. O código de software pode ser armazenado como uma série de instruções ou comandos em um meio legível por computador para armazenamento e/ou transmissão. Um meio legível por computador não transitório adequado pode incluir a memória de acesso aleatório (RAM), uma memória somente leitura (ROM), um meio magnético como um disco rígido ou um disquete ou um meio óptico como um disco compacto (CD) ou DVD (disco versátil digital), memória flash e similares. O meio legível por computador pode ser qualquer combinação de tais dispositivos de armazenamento ou transmissão.

[00221] Tais programas também podem ser codificados e transmitidos por meio de sinais adaptados para transmissão através de redes com fios, ópticas e/ou sem fio, de acordo com uma variedade de protocolos, incluindo a Internet. Como tal, um meio legível por computador, de acordo com uma modalidade da presente invenção pode ser criado usando um sinal de dados codificado com tais programas. O meio legível por computador codificado

com o código de programa pode ser embutido com um dispositivo compatível ou fornecido separadamente a partir de outros dispositivos (por exemplo, através de transferência pela Internet). Qualquer tal meio legível por computador pode residir em ou dentro de um único produto de computador (por exemplo, um disco rígido, um CD ou um sistema de computador inteiro) e pode estar presente ou dentro dos produtos de computador diferentes dentro de um sistema ou rede. Um sistema de computador pode incluir um monitor, impressora ou outro vídeo adequado para a prestação de qualquer dos resultados mencionados neste documento para um usuário.

[00222] Qualquer um dos métodos descritos neste documento pode ser totalmente ou parcialmente executado com um sistema de computador, incluindo um ou mais processadores, que podem ser configurados para executar as etapas. Assim, as modalidades podem ser direcionadas aos sistemas de computador configurados para executar as etapas de qualquer um dos métodos descritos neste documento, potencialmente com diferentes componentes realizando umas etapas respectivas ou um grupo de etapas respectivas. Embora apresentado como etapas numeradas, as etapas dos métodos neste documento podem ser executadas ao mesmo tempo ou em uma ordem diferente. Além disso, as porções dessas etapas podem ser usadas com partes de outras etapas de outros métodos. Além disso, todos ou partes de uma etapa podem ser opcionais. Além disso, qualquer uma das etapas, de qualquer um dos métodos pode ser executado com módulos, unidades, circuitos ou outros meios para executar essas etapas.

[00223] Os detalhes específicos das modalidades em particular podem ser combinados de forma adequada sem se afastar do espírito e o escopo das modalidades da invenção. No entanto, outras modalidades da invenção podem ser direcionadas para modalidades específicas relacionadas a cada aspecto individual ou combinações específicas desses aspectos individuais.

[00224] A descrição acima das modalidades de exemplo da invenção

foi apresentada para fins de ilustração e descrição. Não se destina a ser exaustiva ou limitar a invenção ao formulário descrito preciso e muitas variações e modificações são possíveis tendo em conta o ensinamento acima.

[00225] Uma recitação de "um", "uma" ou "a/o" destina-se a dizer "um ou mais", a menos que especificamente indicado do contrário. O uso de "ou" destina-se a dizer um "ou inclusivo" e não um "ou exclusivo" a menos que especificamente indicado do contrário.

[00226] Todas as patentes, pedidos de patente, publicações e descrições mencionadas neste documento são incorporados por referência, em sua totalidade para todos os efeitos. Nenhum é admitido à técnica anterior.

REIVINDICAÇÕES

1. Método implementado por computador, caracterizado pelo fato de que compreende:

determinar, através de um dispositivo de usuário, uma chave pública de usuário avulsa;

enviar, através do dispositivo de usuário para um computador servidor de provisionamento, uma mensagem de solicitação de provisionamento que inclui a chave pública de usuário avulsa;

receber, através do dispositivo de usuário, uma mensagem de resposta de provisionamento criptografada do computador servidor de provisionamento, a mensagem de resposta de provisionamento criptografada compreendendo os dados de credencial criptografados;

determinar, através do dispositivo de usuário, um segredo compartilhado de resposta usando uma chave pública de servidor estática e uma chave privada do usuário correspondente à chave pública de usuário avulsa;

determinar, através do dispositivo de usuário, uma chave de sessão de resposta do segredo compartilhado de resposta, a chave de sessão de resposta utilizável para descriptografar a mensagem de resposta de provisionamento criptografada;

descriptografar, através do dispositivo de usuário, a mensagem de resposta de provisionamento criptografada usando a chave de sessão de resposta para determinar os dados de credencial criptografados;

determinar, através do dispositivo de usuário, uma chave de proteção de armazenamento do segredo compartilhado de resposta, a chave de proteção de armazenamento sendo diferente da chave de sessão de resposta e utilizável para descriptografar os dados de credencial criptografados;

criptografar, através do dispositivo de usuário, a chave de proteção de armazenamento com uma chave de criptografia de chave para

gerar uma chave de proteção de armazenamento criptografada;

armazenar, através do dispositivo de usuário, a chave de proteção de armazenamento criptografada; e

armazenar, através do dispositivo de usuário, os dados de credencial criptografados.

2. Método implementado por computador, de acordo com a reivindicação 1, caracterizado pelo fato de que os dados de credencial criptografados incluem uma chave de uso limitado (LUK) ou dados de derivação de chaves para uma chave de uso único (SUK).

3. Método implementado por computador, de acordo com a reivindicação 1, caracterizado pelo fato de que os dados de credencial criptografados são armazenados em um servidor de armazenamento conectado remotamente ao dispositivo de usuário e a chave de proteção de armazenamento criptografada é armazenada no dispositivo de usuário.

4. Método implementado por computador, de acordo com a reivindicação 1, caracterizado pelo fato de que compreende ainda:

em resposta a uma indicação para gerar um criptograma usado para autenticar uma mensagem de solicitação de autorização, recuperar os dados de credencial criptografados;

recuperar a chave de proteção de armazenamento criptografado;

descriptografar a chave de proteção de armazenamento criptografada usando a chave de criptografia de chave para obter a chave de proteção de armazenamento;

descriptografar os dados de credencial criptografados usando a chave de proteção de armazenamento para obter dados de credencial; e

gerar o criptograma usando os dados de credencial.

5. Método implementado por computador, de acordo com a reivindicação 4, caracterizado pelo fato de que descriptografar os dados de

credencial criptografados usando a chave de proteção de armazenamento compreende:

derivar uma chave de criptografia de credencial usando a chave de proteção de armazenamento e dados de derivação de chave para a chave de criptografia de credencial, os dados de derivação de chave compreendem os dados específicos ao dispositivo de usuário; e

descriptografar os dados de credencial criptografados usando a chave de criptografia de credencial.

6. Método implementado por computador, de acordo com a reivindicação 4, caracterizado pelo fato de que o criptograma é gerado usando a chave de criptograma derivada dos dados de credencial.

7. Método implementado por computador, de acordo com a reivindicação 1, caracterizado pelo fato de que compreende ainda:

gerar, através do dispositivo de usuário, um segredo compartilhado de solicitação usando a chave pública de servidor estática e a chave privada de usuário correspondendo à chave pública de usuário avulsa; e

criptografar, através do dispositivo do usuário os dados de solicitação que usam o segredo compartilhado de solicitação para obter os dados de solicitação criptografados, em que a mensagem de solicitação de provisionamento inclui os dados de solicitação criptografados.

8. Método implementado por computador, de acordo com a reivindicação 1, caracterizado pelo fato de que a mensagem de resposta de provisionamento inclui uma chave pública de servidor estática cega e o segredo compartilhado de resposta é determinado usando a chave pública de servidor estática cega.

9. Método implementado por computador, de acordo com a reivindicação 1, caracterizado pelo fato de que determinar a chave pública de usuário avulsa compreende gerar um par de chaves de usuário efêmeras que compreendem uma chave privada de usuário efêmera e uma chave pública de

usuário efêmera, onde a chave pública de usuário efêmero é usada como a chave pública de usuário avulsa.

10. Método implementado por computador, de acordo com a reivindicação 1, caracterizado pelo fato de que determinar a chave pública de usuário avulsa compreende ocultar uma chave pública de usuário estática.

11. Método implementado por computador, caracterizado pelo fato de que compreende:

receber, através de um computador servidor de um dispositivo de usuário, uma mensagem de solicitação de provisionamento incluindo uma chave pública de usuário avulsa;

gerar, através do computador servidor, um segredo compartilhado de resposta usando uma chave privada de servidor estática e uma chave pública de usuário avulsa;

identificar, através do computador servidor, os dados de credencial a serem incluídos em uma mensagem de resposta de provisionamento;

determinar, através do computador servidor, uma chave de sessão de resposta do segredo compartilhado de resposta, a chave de sessão de resposta utilizável para criptografar a mensagem de resposta de provisionamento;

determinar, através do computador servidor, uma chave de proteção de armazenamento do segredo compartilhado de resposta, a chave de proteção de armazenamento sendo diferente da chave de sessão de resposta e utilizável para criptografar os dados de credencial criptografados;

criptografar, através do computador servidor, os dados de credencial usando a chave de proteção de armazenamento para gerar dados de credencial criptografados;

criptografar, através do computador servidor, a mensagem de resposta de provisionamento usando a chave de sessão de resposta para gerar

a mensagem de resposta de provisionamento criptografada, em que a mensagem de resposta de provisionamento inclui os dados de credencial criptografados; e

enviar, através do computador servidor para o dispositivo de usuário, a mensagem de resposta de provisionamento criptografada.

12. Método implementado por computador, de acordo com a reivindicação 11, caracterizado pelo fato de que os dados de credencial compreendem uma LUK e dados de derivação de chave de criptograma utilizáveis para derivar uma chave de criptograma que é usada para gerar um criptograma.

13. Método implementado por computador, de acordo com a reivindicação 11, caracterizado pelo fato de que criptografar os dados de credencial compreende a determinação de uma chave de criptografia de credencial usando a chave de proteção de armazenamento e dados de derivação de chaves, onde os dados de derivação de chave são específicos para o dispositivo de usuário.

14. Método implementado por computador, de acordo com a reivindicação 11, caracterizado pelo fato de que a mensagem de resposta de provisionamento inclui uma chave pública de servidor estática cego correspondendo à chave privada de servidor estática.

15. Método implementado por computador, caracterizado pelo fato de que compreende:

determinar, através de um dispositivo de usuário, uma chave pública de usuário avulsa;

determinar, através de um dispositivo de usuário, uma chave pública de proteção de armazenamento;

enviar, através do dispositivo de usuário para um computador servidor de provisionamento, uma mensagem de solicitação de provisionamento que inclui a chave pública de usuário avulsa e chave pública

de proteção de armazenamento;

receber, através do dispositivo de usuário, uma mensagem de resposta de provisionamento criptografada do computador servidor de provisionamento, a mensagem de resposta de provisionamento criptografada compreendendo dados de credencial criptografados, em que os dados de credencial criptografados são criptografados usando a chave pública de proteção de armazenamento;

determinar, através do dispositivo de usuário, um segredo compartilhado de resposta usando uma chave pública de servidor estática e uma chave privada do usuário correspondente à chave pública de usuário avulsa;

determinar, através do dispositivo de usuário, uma chave de sessão de resposta do segredo compartilhado de resposta, a chave de sessão de resposta utilizável para descriptografar a mensagem de resposta de provisionamento criptografada;

descriptografar, através do dispositivo de usuário, a mensagem de resposta de provisionamento criptografada usando a chave de sessão de resposta para determinar os dados de credencial criptografados; e

armazenar, através do dispositivo de usuário, os dados de credencial criptografados.

16. Método implementado por computador, de acordo com a reivindicação 15, caracterizado pelo fato de que a chave pública de proteção de armazenamento e a chave pública de usuário avulsa ambas correspondem a uma mesma chave privada de usuário.

17. Método implementado por computador, de acordo com a reivindicação 15, caracterizado pelo fato de que a chave pública de proteção de armazenamento e a chave pública de usuário avulsa correspondem às chaves privadas de usuário diferentes.

18. Método implementado por computador, de acordo com a

reivindicação 15, caracterizado pelo fato de que compreende ainda:

em resposta a uma indicação para gerar um criptograma usado para autenticar uma mensagem de solicitação de autorização, recuperar os dados de credencial criptografados;

descriptografar os dados de credencial criptografados usando uma chave privada de proteção de armazenamento correspondente à chave pública de proteção de armazenamento para obter os dados de credencial; e

gerar o criptograma usando os dados de credencial.

19. Mídia legível de computador, caracterizada pelo fato de que armazena em si uma pluralidade de instruções para controlar um processador para empregar o método conforme definido em qualquer uma das reivindicações 1 a 18.

20. Sistema de computador, caracterizado pelo fato de que compreende:

uma memória que armazena instruções executáveis por computador; e

um processador configurado para acessar a memória e executar as instruções executáveis por computador para empregar o método conforme definido em qualquer uma das reivindicações 1 a 18.

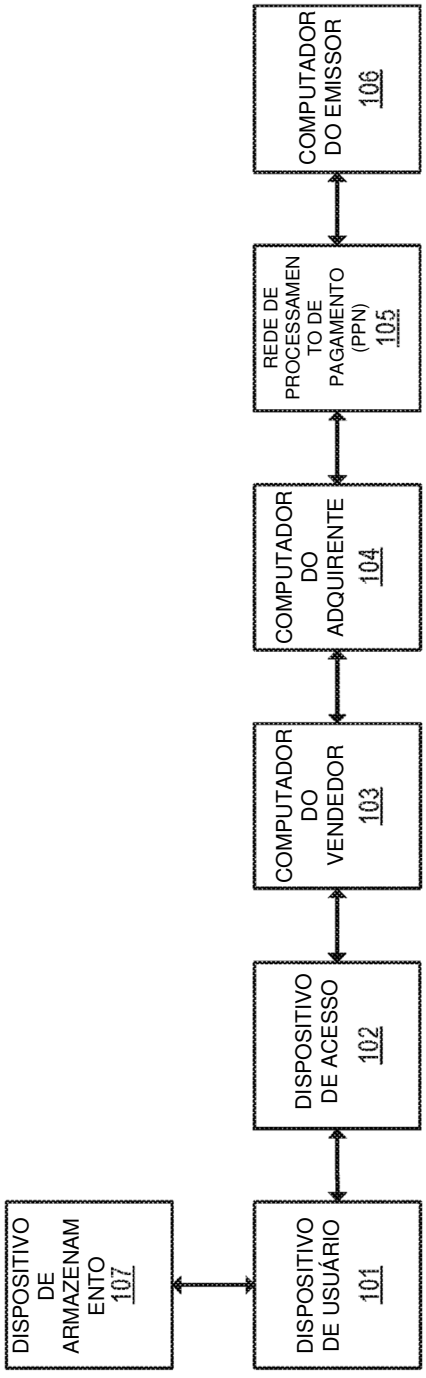
100
DISPOSITIVO DE USUÁRIO 101
DISPOSITIVO DE ARMAZENAMENTO 107
DISPOSITIVO DE ACESSO 102
COMPUTADOR DO VENDEDOR 103
COMPUTADOR DO ADQUIRENTE 104
REDE DE PROCESSAMENTO DE PAGAMENTO (PPN) 105
COMPUTADOR DO EMISSOR 106

FIG. 1

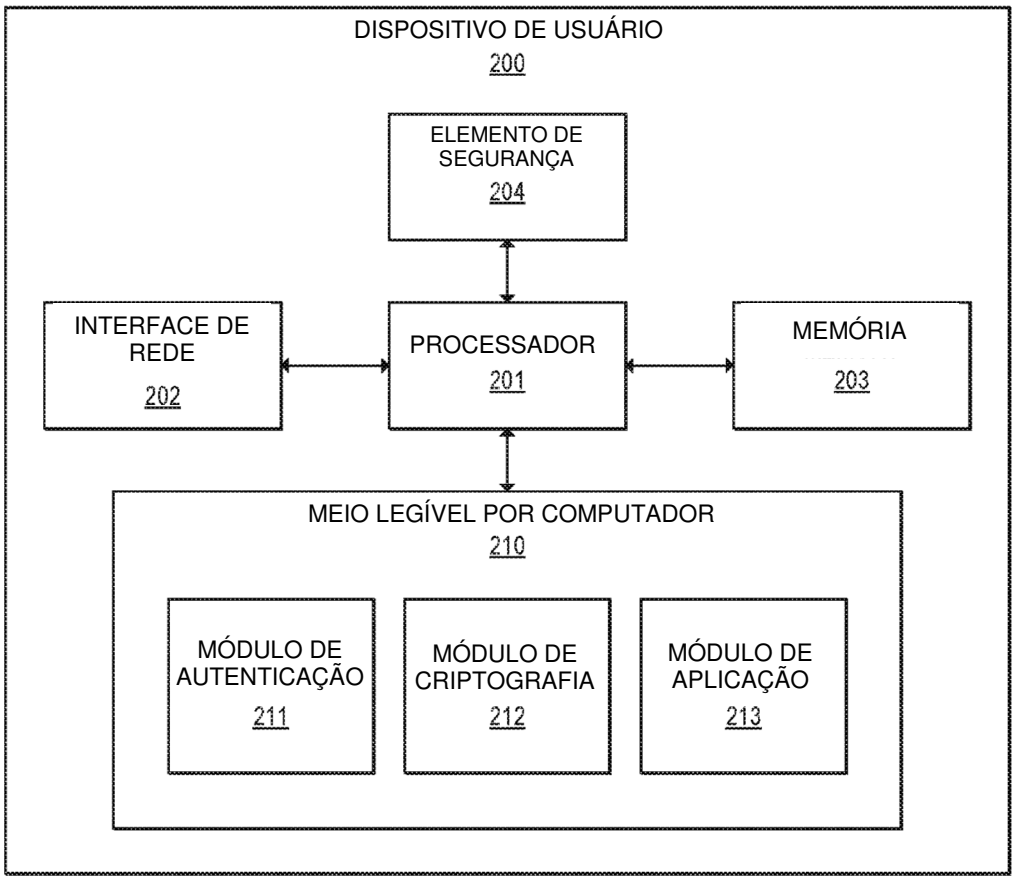
DISPOSITIVO DE USUÁRIO
200
ELEMENTO DE SEGURANÇA
204
INTERFACE DE REDE
202
PROCESSADOR
201
MEMÓRIA
203
MEIO LEGÍVEL POR COMPUTADOR
210
MÓDULO DE AUTENTICAÇÃO
211
MÓDULO DE CRIPTOGRAFIA
212
MÓDULO DE APLICAÇÃO
213

FIG. 2

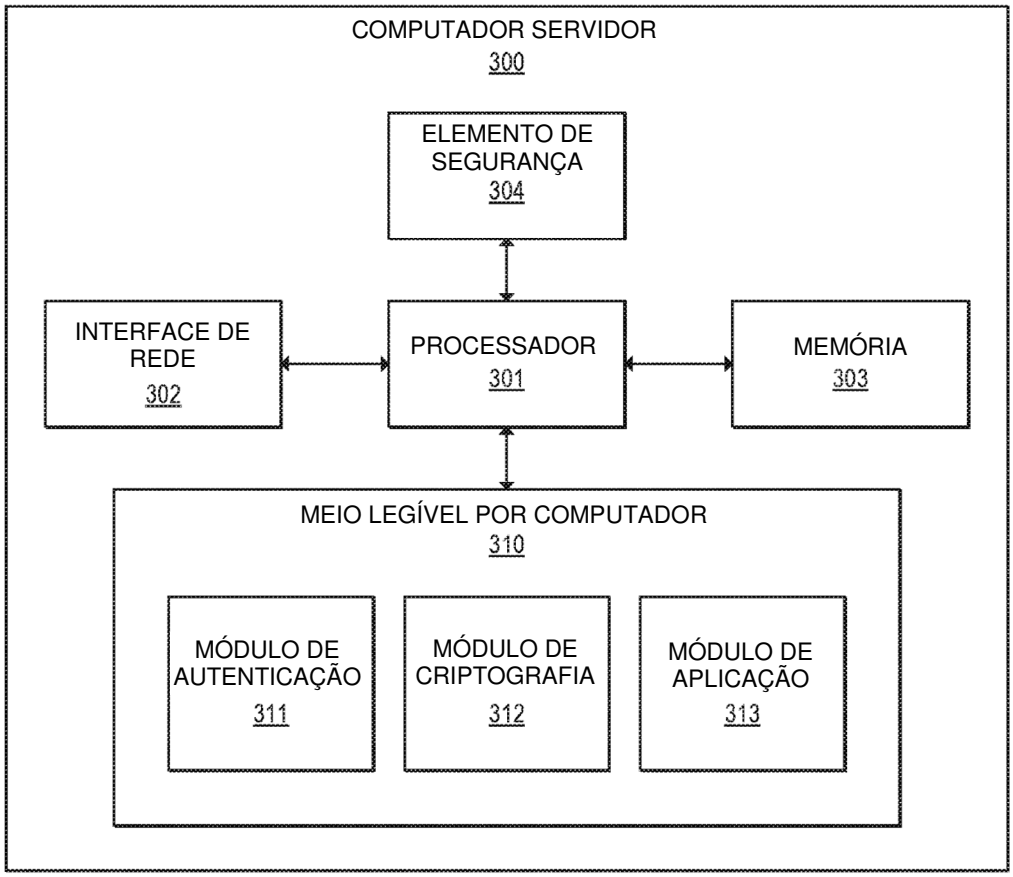
COMPUTADOR SERVIDOR
300
ELEMENTO DE SEGURANÇA
304
INTERFACE DE REDE
302
PROCESSADOR
301
MEMÓRIA
303
MEIO LEGÍVEL POR COMPUTADOR
310
MÓDULO DE AUTENTICAÇÃO
311
MÓDULO DE CRIPTOGRAFIA
312
MÓDULO DE APLICAÇÃO
313

FIG. 3

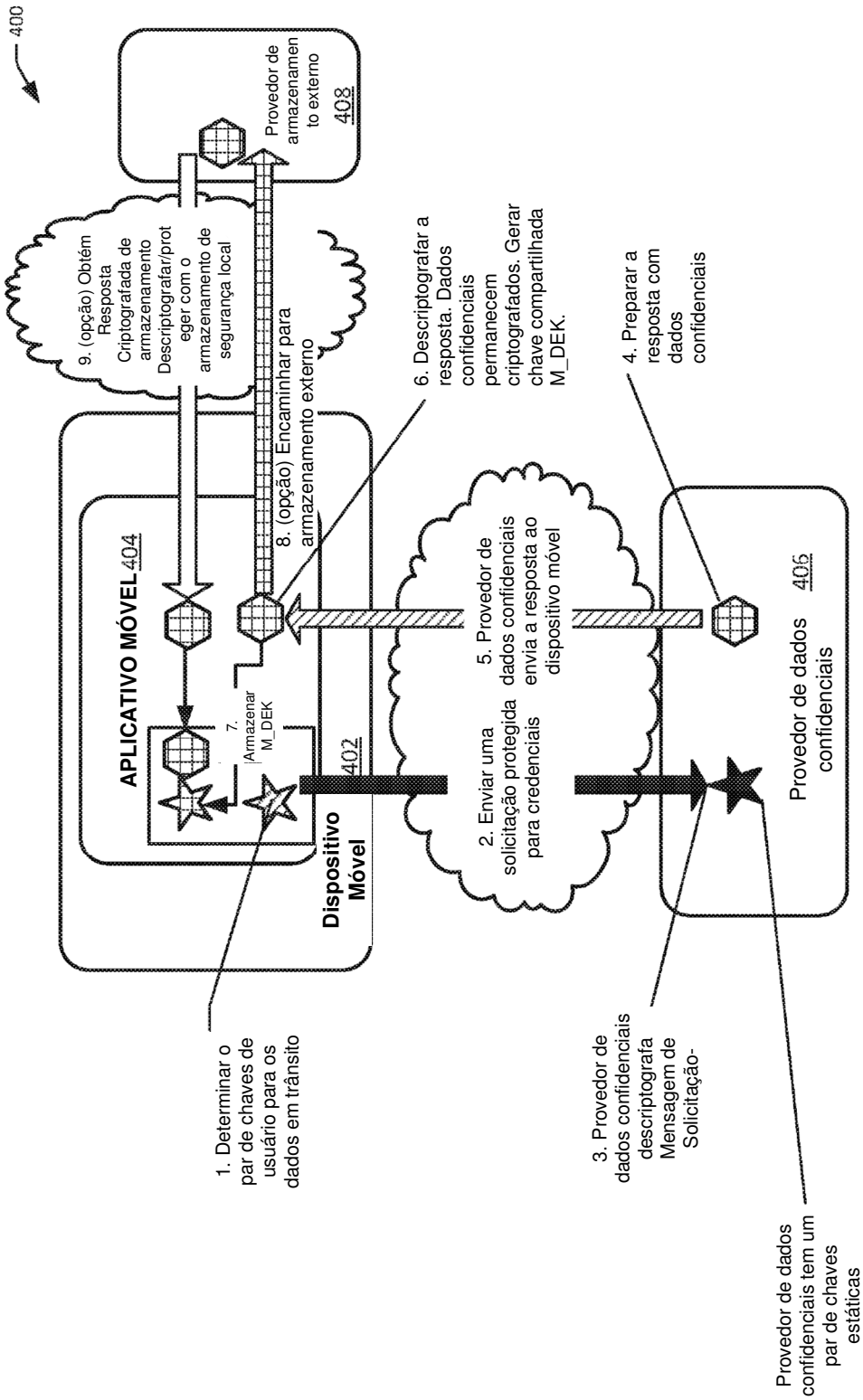
400
Provedor de armazenamento externo 408
9. (opção) Obtém Resposta Criptografada de armazenamento Descriptografar/proteger com o armazenamento de segurança local
8. (opção) Encaminhar para armazenamento externo
6. Descriptografar a resposta. Dados confidenciais permanecem criptografados. Gerar chave compartilhada M_DEK.
4. Preparar a resposta com dados confidenciais
APLICATIVO MÓVEL 404
7. Armazenar M_DEK
Dispositivo Móvel 402
5. Provedor de dados confidenciais envia a resposta ao dispositivo móvel
2. Enviar uma solicitação protegida para credenciais
Provedor de dados confidenciais 406
1. Determinar o par de chaves de usuário para os dados em trânsito
3. Provedor de dados confidenciais descriptografa Mensagem de Solicitação-
Provedor de dados confidenciais tem um par de chaves estáticas

FIG. 4

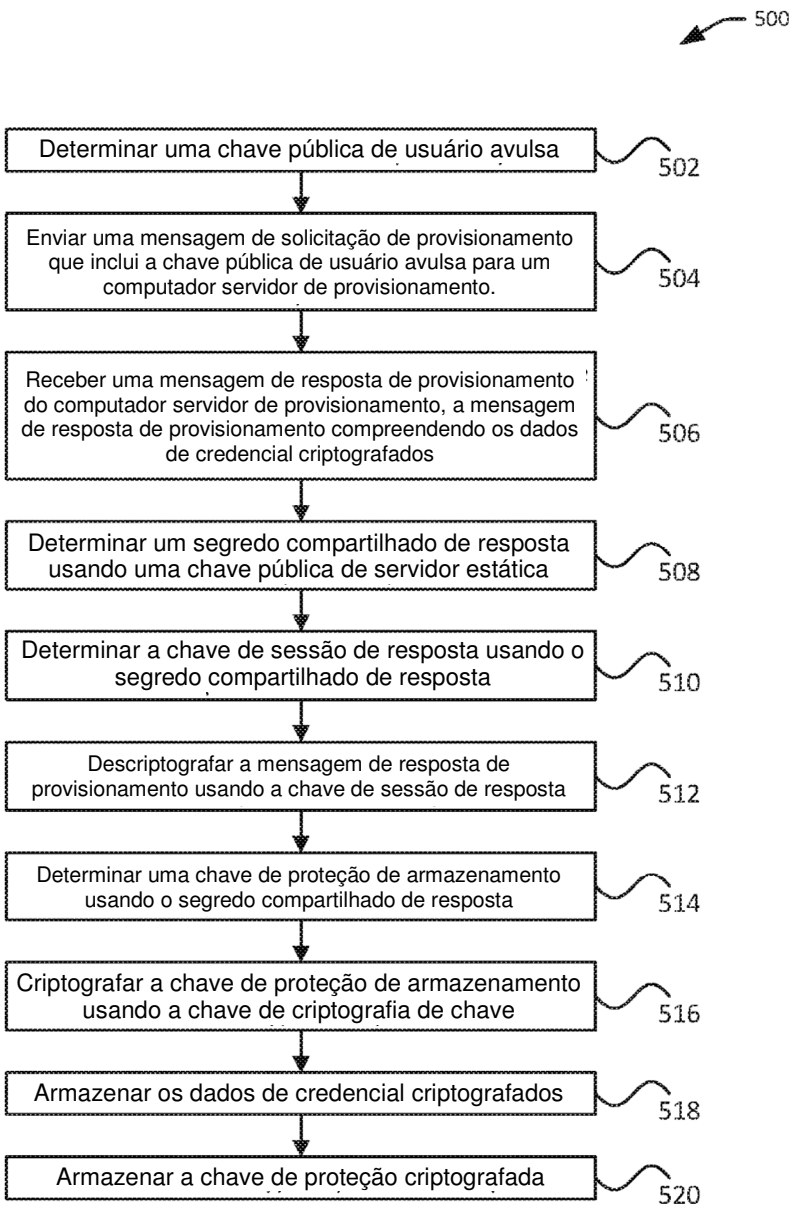
500
Determinar uma chave pública de usuário avulsa
502
Enviar uma mensagem de solicitação de provisionamento que inclui a chave pública de usuário avulsa para um computador servidor de provisionamento.
504
Receber uma mensagem de resposta de provisionamento do computador servidor de provisionamento, a mensagem de resposta de provisionamento compreendendo os dados de credencial criptografados
506
Determinar um segredo compartilhado de resposta usando uma chave pública de servidor estática
508
Determinar a chave de sessão de resposta usando o segredo compartilhado de resposta
510
Descriptografar a mensagem de resposta de provisionamento usando a chave de sessão de resposta
512
Determinar uma chave de proteção de armazenamento usando o segredo compartilhado de resposta
514
Criptografar a chave de proteção de armazenamento usando a chave de criptografia de chave
516
Armazenar os dados de credencial criptografados
518
Armazenar a chave de proteção criptografada
520

FIG. 5

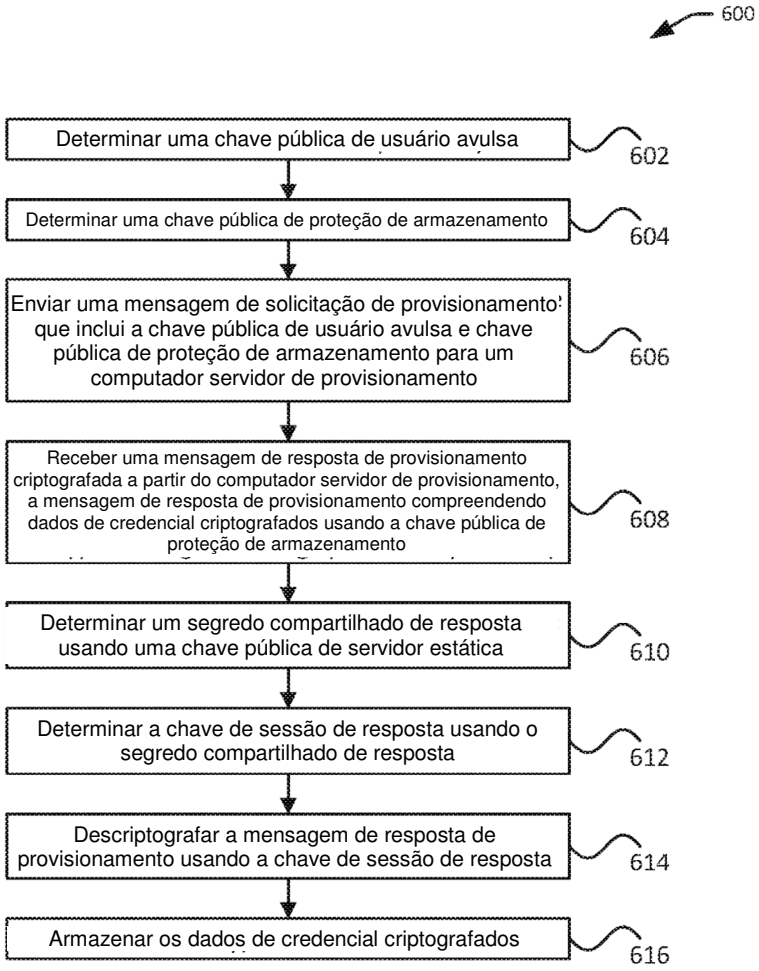
600
Determinar uma chave pública de usuário avulsa
602
Determinar uma chave pública de proteção de armazenamento
604
Enviar uma mensagem de solicitação de provisionamento que inclui a chave pública de usuário avulsa e chave pública de proteção de armazenamento para um computador servidor de provisionamento
606
Receber uma mensagem de resposta de provisionamento criptografada a partir do computador servidor de provisionamento, a mensagem de resposta de provisionamento compreendendo dados de credencial criptografados usando a chave pública de proteção de armazenamento
608
Determinar um segredo compartilhado de resposta usando uma chave pública de servidor estática
610
Determinar a chave de sessão de resposta usando o segredo compartilhado de resposta
612
Descriptografar a mensagem de resposta de provisionamento usando a chave de sessão de resposta
614
Armazenar os dados de credencial criptografados
616

FIG. 6

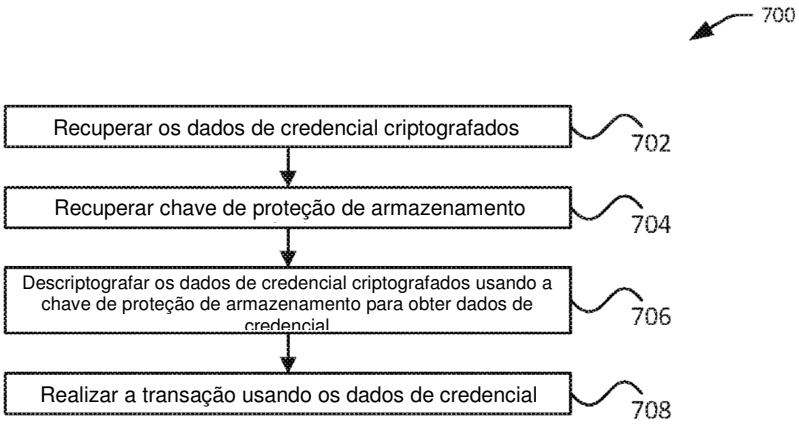
700
Recuperar os dados de credencial criptografados
702
Recuperar chave de proteção de armazenamento
704
Descriptografar os dados de credencial criptografados usando a chave de proteção de armazenamento para obter dados de credencial
706
Realizar a transação usando os dados de credencial
708

FIG. 7

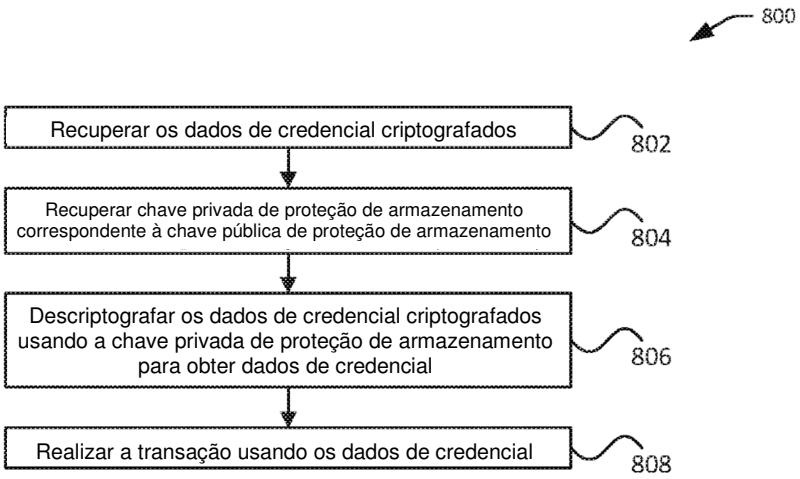
800
Recuperar os dados de credencial criptografados
802
Recuperar chave privada de proteção de armazenamento correspondente à chave pública de proteção de armazenamento
804
Descriptografar os dados de credencial criptografados usando a chave privada de proteção de armazenamento para obter dados de credencial
806
Realizar a transação usando os dados de credencial
808

FIG. 8

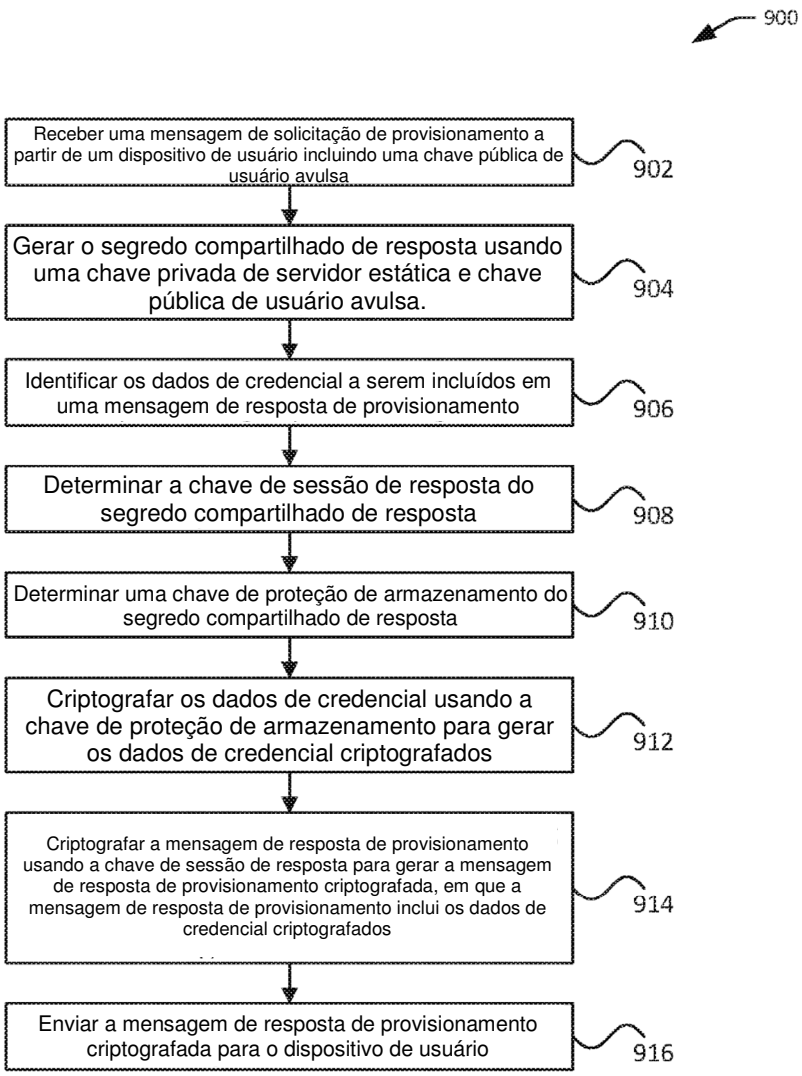
900
Receber uma mensagem de solicitação de provisionamento a partir de um dispositivo de usuário incluindo uma chave pública de usuário avulsa
902
Gerar o segredo compartilhado de resposta usando uma chave privada de servidor estática e chave pública de usuário avulsa.
904
Identificar os dados de credencial a serem incluídos em uma mensagem de resposta de provisionamento
906
Determinar a chave de sessão de resposta do segredo compartilhado de resposta
908
Determinar uma chave de proteção de armazenamento do segredo compartilhado de resposta
910
Criptografar os dados de credencial usando a chave de proteção de armazenamento para gerar os dados de credencial criptografados
912
Criptografar a mensagem de resposta de provisionamento usando a chave de sessão de resposta para gerar a mensagem de resposta de provisionamento criptografada, em que a mensagem de resposta de provisionamento inclui os dados de credencial criptografados
914
Enviar a mensagem de resposta de provisionamento criptografada para o dispositivo de usuário
916

FIG. 9

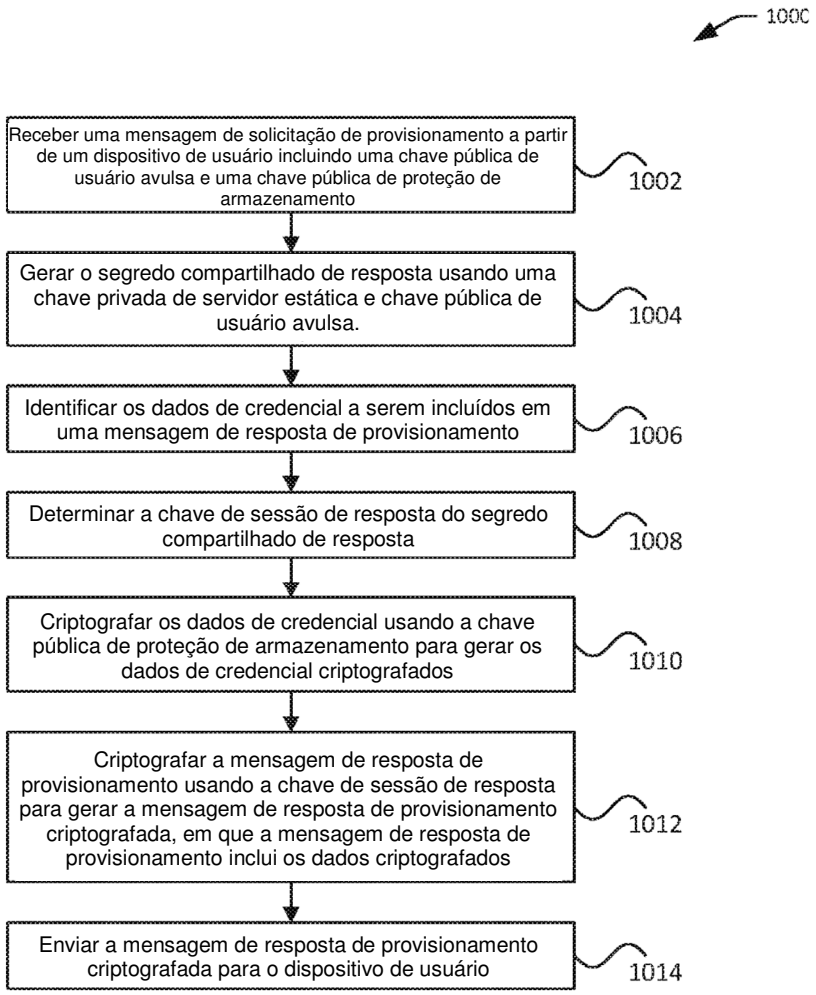
1000
Receber uma mensagem de solicitação de provisionamento a partir de um dispositivo de usuário incluindo uma chave pública de usuário avulsa e uma chave pública de proteção de armazenamento
1002
Gerar o segredo compartilhado de resposta usando uma chave privada de servidor estática e chave pública de usuário avulsa.
1004
Identificar os dados de credencial a serem incluídos em uma mensagem de resposta de provisionamento
1006
Determinar a chave de sessão de resposta do segredo compartilhado de resposta
1008
Criptografar os dados de credencial usando a chave pública de proteção de armazenamento para gerar os dados de credencial criptografados
1010
Criptografar a mensagem de resposta de provisionamento usando a chave de sessão de resposta para gerar a mensagem de resposta de provisionamento criptografada, em que a mensagem de resposta de provisionamento inclui os dados criptografados
1012
Enviar a mensagem de resposta de provisionamento criptografada para o dispositivo de usuário
1014

FIG. 10

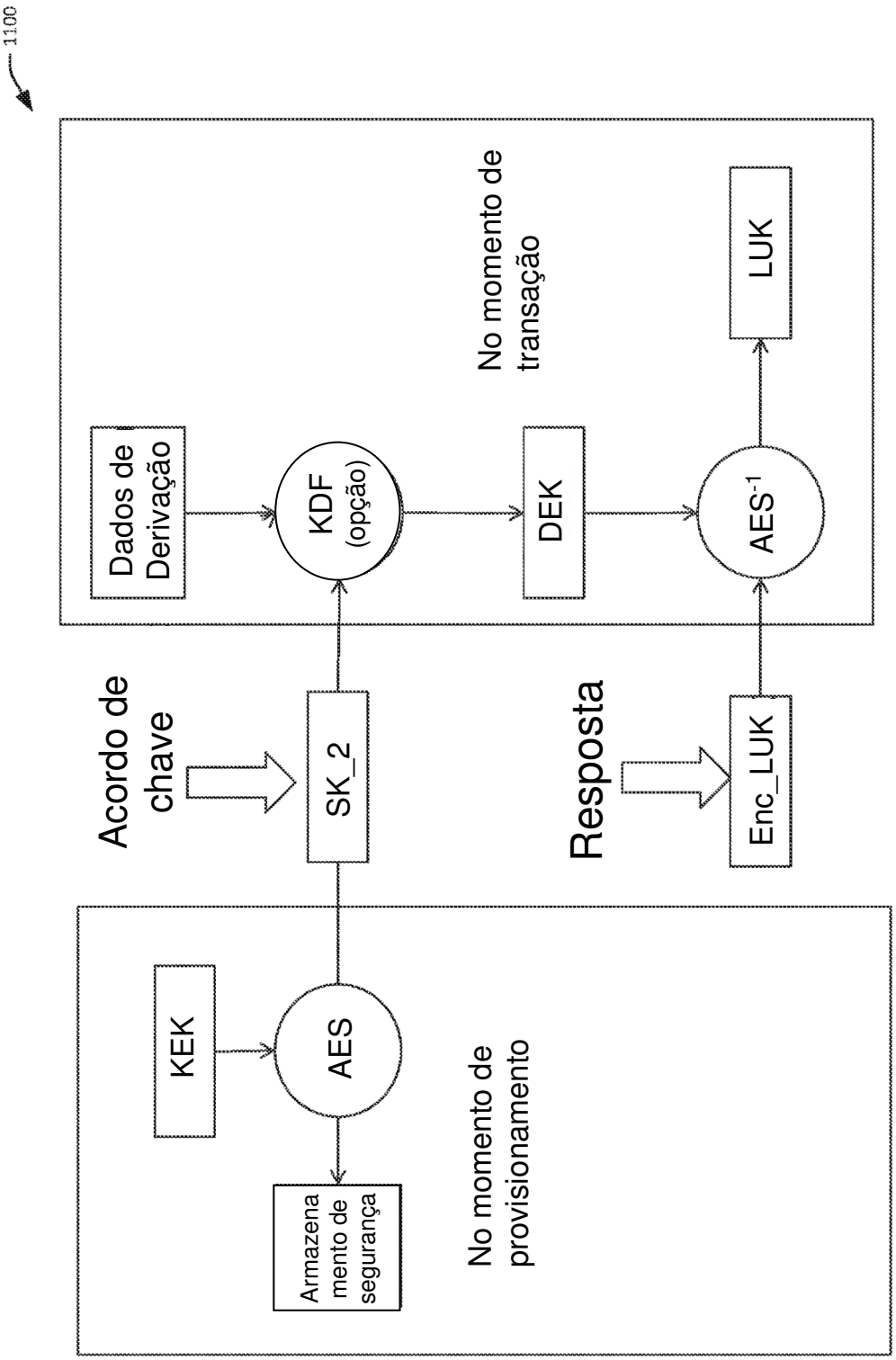
1100
No momento de provisionamento
KEK
AES
Armazenamento de segurança
Acordo de chave
SK_2
Resposta
Enc_LUK
No momento de transação
Dados de Derivação
KDF (opção)
DEK
AES-1
LUK

FIG. 11

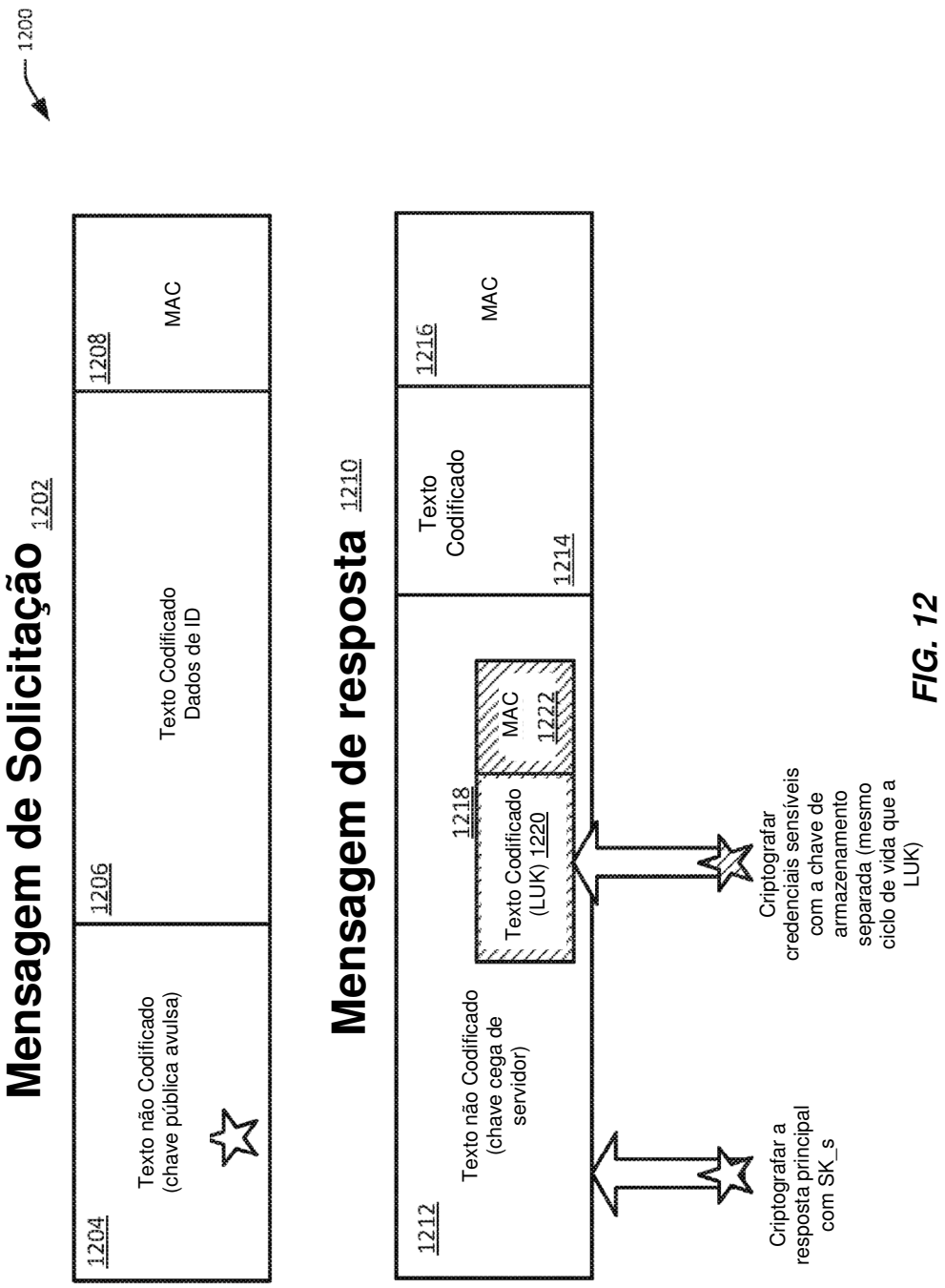
1200
Mensagem de Solicitação 1202
1204
Texto não Codificado (chave pública avulsa)
1206
Texto Codificado Dados de ID
1208
MAC
Mensagem de resposta 1210
1212
Texto não Codificado (chave cega de servidor)
1218
Texto Codificado (LUK) 1220
MAC 1222
1214
Texto Codificado
1216
MAC
Criptografar a resposta principal com SK_s
Criptografar credenciais sensíveis com a chave de armazenamento separada (mesmo ciclo de vida que a LUK)

FIG. 12

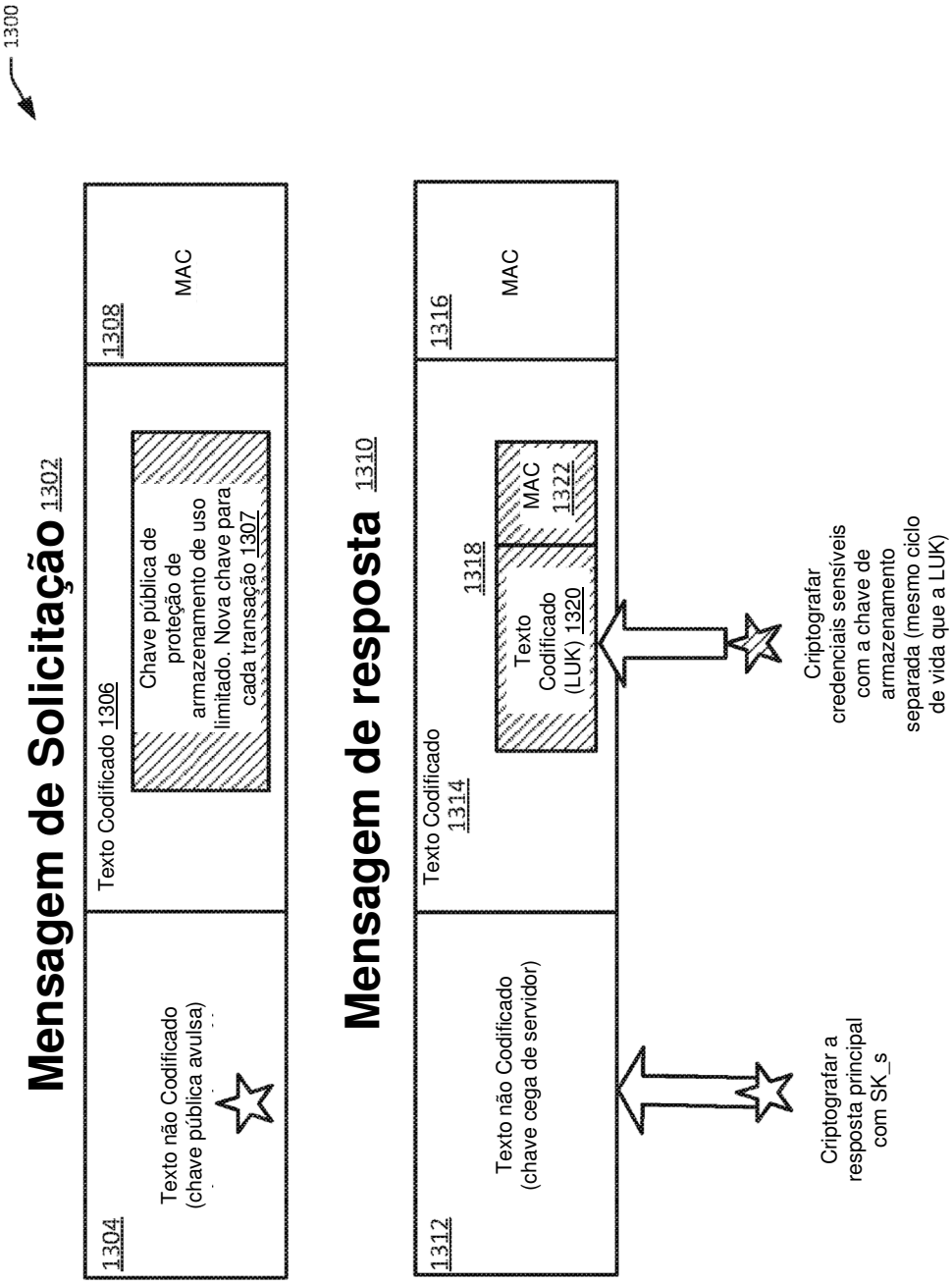
1300
Mensagem de Solicitação 1302
1304
Texto não Codificado (chave pública avulsa)
Texto Codificado 1306
Chave pública de proteção de armazenamento de uso limitado. Nova chave para cada transação 1307
1308
MAC
Mensagem de resposta 1310
1312
Texto não Codificado (chave cega de servidor)
Texto Codificado 1314
1318
Texto Codificado (LUK) 1320
MAC 1322
1316
MAC
Criptografar a resposta principal com SK_s
Criptografar credenciais sensíveis com a chave de armazenamento separada (mesmo ciclo de vida que a LUK)

FIG. 13

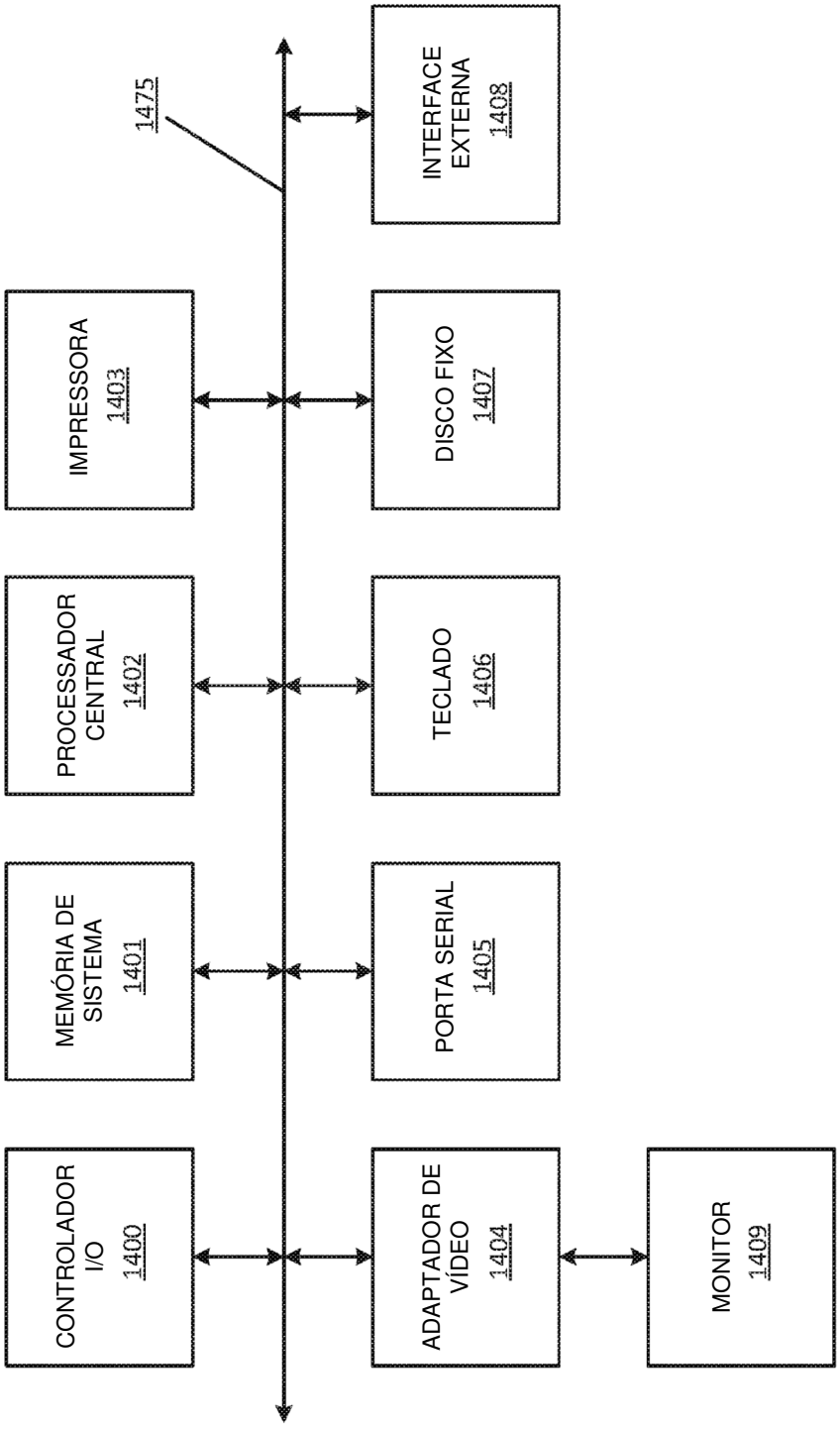
1475
INTERFACE EXTERNA 1408
IMPRESSORA 1403
DISCO FIXO 1407
PROCESSADOR CENTRAL 1402
TECLADO 1406
MEMÓRIA DE SISTEMA 1401
PORTA SERIAL 1405
CONTROLADOR I/O 1400
ADAPTADOR DE VÍDEO 1404
MONITOR 1409

FIG. 14