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

(11) PI 0318446-3 B1

(22) Data do Depósito: 26/08/2003

(45) Data de Concessão: 16/05/2017

(54) Título: DISPOSITIVO PARA AUTENTICAÇÃO DE MULTIMÍDIA DE UM USUÁRIO, EQUIPAMENTO DE USUÁRIO, MÉTODO PARA AUTENTICAR UM USUÁRIO ACESSANDO UM DOMÍNIO DE MULTIMÍDIA POR UMA REDE DE ACESSO, E, ENTIDADES DE SERVIÇO, PRÓXI E INTERROGANTE

(51) Int.Cl.: H04L 29/06; H04W 12/06; H04L 29/08

(52) CPC: H04L 65/1016,H04L 63/0815,H04L 63/0853,H04W 12/06,H04L 67/306,H04L 67/14

(73) Titular(es): TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)

(72) Inventor(es): JOHN MICHAEL WALKER PINA; JUAN ANTONIO SANCHEZ HERRERO

"DISPOSITIVO PARA AUTENTICAÇÃO DE MULTIMÍDIA DE UM USUÁRIO, EQUIPAMENTO DE USUÁRIO, MÉTODO PARA AUTENTICAR UM USUÁRIO ACESSANDO UM DOMÍNIO DE MULTIMÍDIA POR UMA REDE DE ACESSO, E, ENTIDADES DE SERVIÇO, PRÓXI E INTERROGANTE"

CAMPO DA INVENÇÃO

[0001] A presente invenção relaciona-se a um procedimento simplificado para autenticar um usuário acessando uma rede de Multimídia por uma rede de acesso onde o usuário já tinha sido autenticado.

FUNDAMENTOS

[0002] Muitas das redes móveis presentemente existentes, como também possíveis redes futuras sendo definidas por corpos de padronização, requerem os usuários finais e agentes de usuário se autenticarem ao acessar uma rede e, mais exatamente, ao acessar serviços associados à rede. Neste respeito, domínios de GSM, GPRS, Rede de Área Local Sem Fio (WLAN) e Multimídia (IMS), como definidos por padrões de 3GPP e 3GPP2, todos eles requerem o equipamento de usuário ou terminais arranjados correrem um procedimento de autenticação específico para cada domínio tecnológico particular antes de conceder a usuários ou agentes de usuário o acesso a ditos domínios. Em particular, os domínios tecnológicos citados acima, como também outros domínios tecnológicos emergentes, requerem níveis de segurança diferentes que complicam mais o acesso ao longo de domínios tecnológicos diferentes. Este acesso por toda parte implica em segurança extra que não é sempre precisada e, como consequência, capacidades de processamento e sinalização extras como também complexidade extra no equipamento de usuário ou terminais.

[0003] Atualmente, o procedimento de autenticação em um domínio de Multimídia de 3GPP é executado como descrito no padrão de 3G TS 33.203 e descrito na Figura 1 em termos de um fluxo de sinalização baseado em Protocolo de Iniciação de Sessão (SIP). Como Figura 1 ilustra e as especificações técnicas referidas descrevem, autenticação de Multimídia sempre deverá ser executada quando um usuário está se registrando no domínio de Multimídia, o que é

tipicamente começado enviando uma mensagem de Registro de SIP para uma dada identidade privada e pública.

[0004] Uma condição inicial assumida antes de começar o fluxo citado acima é que um usuário final deve ter uma conexão de dados aberta antes de acessar o domínio de Multimídia. Esta conexão pode ser tanto uma conexão de GPRS em termos de ter um contexto de PDP ativado, ou uma conexão de WLAN em termos de ter estabelecido uma conexão de dados como especificado pelos padrões de IEEE 802. 11, ou outra rede de acesso provendo o lado de usuário com uma conexão de dados. Neste cenário, um usuário final ou um agente de usuário já foi autenticado pela rede de acesso, se GPRS ou WLAN ou outro, a fim de estabelecer tal conexão de dados e antes de enviar um Registro de SIP ao domínio de Multimídia.

[0005] Em particular, ambas as redes de acesso atualmente usadas, isto é GPRS e WLAN, estão oferecendo mecanismo de autenticação respectivo, SIM/USIM-AKA para GPRS e EAP-SIM/AKA para WLAN, enquanto o domínio de Multimídia faz uso atualmente de um mecanismo de autenticação oferecendo um nível semelhante de segurança como as redes de acesso acima, o denominado USIM-AKA, que é executado quando a mensagem de Registro de SIP alcança uma entidade de Função de Controle de Estado de Chamada de Serviço (S-CSCF) como mostrado na Figura 1. Neste respeito, Figura 2 ilustra a sequência de ações seguidas para executar uma autenticação de EAP AKA para um usuário tendo acessado uma rede de WLAN, em que RADIUS e MAP parecem ser as alternativas de protocolo mais prováveis, embora DIAMETER também poderia ser usado em vez de RADIUS ou MAP.

[0006] No momento, um usuário querendo adquirir acesso ao domínio de Multimídia requer um estabelecimento prévio de uma conexão de dados, o que é frequentemente executado por uma rede de acesso tal como GPRS ou WLAN e, consequentemente, o usuário foi autenticado primeiramente com um EAP-SIM/AKA para uma rede de acesso de WLAN, e adicionalmente o usuário deveria ser autenticado secundariamente com um USIM-AKA ao se registrar no domínio de Multimídia.

[0007] Alguém pode concluir que no momento não há nenhum mecanismo de autenticação executando uma autenticação de domínio cruzado para um dado usuário entre uma rede de acesso tal como GPRS ou WLAN e um domínio de Multimídia baseado em SIP. Em outras palavras, não há nenhum serviço ou dispositivo existente que seja capaz de administrar dados de autenticação em nome de um usuário ou um agente de usuário de SIP e aliviar dito usuário ou agente de usuário de SIP de ter que executar operações de autenticação no domínio de Multimídia uma vez que uma autenticação já aconteceu na rede de acesso por onde o usuário está acessando, dita rede de acesso sendo provavelmente GPRS ou WLAN.

[0008] Nesta situação, a autenticação para domínio de Multimídia como descrito em 3G TS 33.203 e ilustrado na Figura 1 adiciona sinalização extra no trajeto de rádio que, sob alguns cenários, poderia ser desnecessário. Primeiramente, depois que um Registro de SIP é recebido pela S-SCSF, a S-SCSF tipicamente envia uma mensagem de Intimação de Autenticação ao agente de usuário de SIP. Se esta operação tiver êxito, então a S-CSCF enviará periodicamente um pedido de vetor de Autenticação ao agente de usuário de SIP, que por sua vez deve responder com uma resposta de Vetor de Autenticação. Ambas destas mensagens adicionam carga extra no domínio de multimídia como também tempos de registro mais longos. Quer dizer, agentes de usuários de SIP deveriam processar e responder a ambos a Intimação de Autenticação e pedido de Vetor de Autenticação. Estas mensagens requerem processamento extra pelo agente de usuário de SIP, que significa que o agente de usuário de SIP tem que fazer uso de potência para este processo em lugar de usar tanta potência quanto possível para serviços de Multimídia que são prováveis de uma natureza de consumo de alta potência, e ter em mente a potência limitada de baterias.

[0009] Por esse meio, a presente invenção é visada para prover um mecanismo de autenticação de inter-domínio executando uma autenticação de domínio cruzado para um dado usuário entre um domínio de rede de acesso e um domínio de Multimídia, este mecanismo de autenticação de inter-domínio sendo mais simples do

que o atualmente existente, e aplicável onde uma autenticação de usuário foi executada pela rede de acesso.

SUMÁRIO DA INVENÇÃO

[0010] O objetivo acima é realizado de acordo com a presente invenção pela provisão do dispositivo de acordo com a reivindicação 1, do equipamento de usuário de acordo com a reivindicação 10, e do método de acordo com a reivindicação 15, todos arranjados para reutilizar dados de autenticação entre redes diferentes ou entre domínios tecnológicos diferentes, e com a ajuda da entidade de serviço de acordo com a reivindicação 23 na função de autenticar o usuário no domínio de Multimídia e da entidade próxi de acordo com a reivindicação 29 e da entidade interrogante de acordo com a reivindicação 32, ambas sendo entidades de um domínio de Multimídia de acordo com padrões de 3GPP e 3GPP2. Portanto, há uma nova característica provida de acordo com a invenção, e referida em seguida como "Autenticação Implícita para domínio de Multimídia", que pode ser implementada como um dispositivo de Autenticação de Multimídia dedicado em cooperação íntima com um servidor de assinante, ou ser integrada completamente em dito servidor de assinante. Dito servidor de assinante sendo um banco de dados de assinante envolvido durante a autenticação de assinante, por exemplo um Servidor de Assinante Doméstico (HSS) ou um servidor de Autenticação-Autorização-Contabilidade (AAA), e o dispositivo de Autenticação de Multimídia contendo a lógica e componentes necessários para habilitar a reutilização de dados de autenticação entre uma rede de acesso tal como uma Rede de Área Local Sem Fio (WLAN), uma rede de Sistema de Rádio de Pacote Geral (GPRS), um Sistema de Telecomunicação Móvel Universal (UMTS), ou uma rede de Acesso Múltiplo por Divisão de Código (CDMA 2000), e dito domínio de Multimídia. O dispositivo, que de acordo com a invenção é útil para autenticação de Multimídia de um usuário acessando um domínio de Multimídia por uma rede de acesso, é arranjado para uso em, ou em cooperação com um servidor de assinante da rede de acesso contendo dados de autenticação para o usuário e acessível ao domínio de Multimídia. Dito dispositivo inclui meio para decidir que uma autenticação implícita entre o usuário

ou, mais exatamente, entre o equipamento de usuário e o domínio de Multimídia pode acontecer, e meio para instruir uma entidade de serviço na função de autenticar o usuário no domínio de Multimídia que uma autenticação implícita pode acontecer. O uso deste dispositivo assim saltando a necessidade por uma autenticação explícita.

[0011] Neste dispositivo, o meio para decidir que uma autenticação implícita pode acontecer preferivelmente inclui meio para determinar a segurança potencial do trajeto de sinalização para acessar o domínio de Multimídia por dita rede de acesso. Para este propósito, o dispositivo pode incluir igualmente meio de dados de provisão de configuração arranjado para avaliar a segurança de trajetos de sinalização diferentes. Além disso, o meio para decidir que uma autenticação implícita pode acontecer, pode incluir meio para processar uma proposta de autenticação implícita originada do equipamento de usuário.

[0012] O dispositivo é arranjado vantajosamente para determinar se uma autenticação implícita é apenas uma proposta para o equipamento de usuário, que pode forçar uma autenticação explícita, ou é uma decisão final tomada pela rede, de forma que nenhuma autenticação explícita pode ser executada. Portanto, o meio para instruir a entidade de serviço que uma autenticação implícita pode acontecer inclui meio para indicar que a decisão final é no equipamento de usuário e meio para indicar que esta é uma decisão final tomada pela rede.

[0013] Neste respeito, o dispositivo adicionalmente inclui meio para notificar o usuário que uma autenticação implícita do usuário para acessar o domínio de Multimídia pode ser executada pela rede. Não obstante, este meio de notificação pode igualmente residir em outras entidades do domínio de Multimídia.

[0014] Além disso, dado que a decisão final sobre se ou não executar uma autenticação implícita pode ser no lado de equipamento de usuário de acordo com a invenção, o dispositivo adicionalmente inclui meio para receber uma indicação originada do lado de equipamento de usuário para confirmar a aceitação da autenticação implícita proposta pela rede. No caso de receber tal confirmação de aceitação, o dispositivo também inclui meio para indicar à entidade de serviço na

função de autenticar o usuário no domínio de Multimídia que o equipamento de usuário confirmou a autenticação implícita. Ainda adicionalmente, o dispositivo pode ter o meio para prover dados de autenticação adicionais para dita entidade de serviço, ditos dados de autenticação adicionais incluindo pelo menos um elemento selecionado de um grupo de elementos incluindo: tipo de autenticação; informação de acesso; e marca de tempo de autenticação.

[0015] Convencionalmente, equipamento de um usuário está habilitado para adquirir acesso a um domínio de Multimídia por uma rede de acesso, e é assim arranjado para executar um primeiro procedimento de Autenticação explícita com a rede de acesso, e um segundo procedimento de autenticação explícita com um domínio de Multimídia. A rede de acesso inclui um servidor de assinante para conter dados de autenticação para o usuário e, para o propósito da presente invenção, dito servidor de assinante é acessível ao domínio de Multimídia. O equipamento de usuário, de acordo com a invenção, inclui meio para processar pelo menos uma notificação selecionada de um grupo de notificações incluindo: uma notificação do domínio de Multimídia indicando que uma autenticação implícita para o usuário pode ser executada; e uma notificação para o domínio de Multimídia indicando que o equipamento de usuário propõe uma autenticação implícita à rede.

[0016] Este meio pode incluir vantajosamente meio para receber uma indicação do domínio de Multimídia que a decisão final é no lado de equipamento de usuário, que poderia forçar uma autenticação explícita, ou que é uma decisão final tomada pela rede, de forma que nenhuma autenticação explícita pode ser executada. Especialmente arranjado para o caso onde a decisão final está no lado do usuário, o equipamento de usuário adicionalmente inclui meio para enviar para o domínio de Multimídia uma indicação para confirmar a aceitação de uma autenticação implícita proposta pela rede. Além disso, o equipamento de usuário pode ter o meio para prover dados de autenticação adicionais para o domínio de Multimídia, ditos dados de autenticação adicionais incluindo pelo menos um elemento selecionado de um grupo de elementos incluindo: tipo de autenticação; informação de acesso; e marca de tempo de autenticação.

[0017] Também é provido um método para autenticar um usuário em um domínio de Multimídia quando o usuário acessa a ele por uma rede de acesso, o método incluindo convencionalmente uma etapa de autenticar o usuário na rede de acesso, dita rede de acesso tendo um servidor de assinante com dados de autenticação para o usuário e acessível ao domínio de Multimídia; e uma etapa de registrar o usuário no domínio de Multimídia.

[0018] Este método, de acordo com a invenção, também inclui:

- uma etapa de decidir que uma autenticação implícita entre o usuário e o domínio de Multimídia pode acontecer, assim saltando as necessidades por uma autenticação explícita; e

- uma etapa de instruir uma entidade de serviço na função de autenticar o usuário no domínio de Multimídia que autenticação implícita pode acontecer.

[0019] Este método pode adicionalmente incluir uma etapa de notificar do domínio de Multimídia ao equipamento de usuário que uma autenticação implícita do usuário para acessar o domínio de Multimídia pode ser executada.

[0020] Neste método, a etapa de decidir que uma autenticação implícita pode acontecer, preferivelmente inclui uma etapa de determinar a segurança potencial do trajeto de sinalização para acessar o domínio de Multimídia por dita rede de acesso. Além disso, a etapa acima de decidir que uma autenticação implícita pode acontecer, pode incluir igualmente uma etapa de propor do equipamento de usuário para o domínio de Multimídia uma autenticação implícita a ser executada entre dito equipamento de usuário e domínio de Multimídia.

[0021] Também neste método, a etapa de instruir a entidade de serviço que uma autenticação implícita pode acontecer, preferivelmente inclui uma etapa de indicar se a decisão final está no equipamento de usuário, que poderia forçar uma autenticação explícita, ou a decisão final é tomada pela rede, de forma que nenhuma autenticação explícita pode ser executada. Além disso, e especificamente para o caso onde a decisão final está no lado do usuário, o método pode adicionalmente incluir uma etapa de confirmar do equipamento de usuário a aceitação da autenticação implícita proposta pela rede. Além disso, e alinhado com a etapa

acima, o método pode adicionalmente incluir uma etapa de indicar para a entidade de serviço na função de autenticar o usuário no domínio de Multimídia que o usuário confirmou a autenticação implícita.

[0022] A invenção adicionalmente provê uma entidade de serviço na função de autenticar o equipamento de um usuário no domínio de Multimídia quando o usuário acessa a ele por uma rede de acesso onde dito usuário tinha sido autenticado previamente. Esta entidade de serviço inclui, de acordo com a invenção, meio para receber instruções do dispositivo acima indicando que uma autenticação implícita pode acontecer; e meio para notificar o equipamento de usuário que uma autenticação implícita do usuário para acessar o domínio de Multimídia pode ser executada pela rede.

[0023] Esta entidade de serviço é arranjada vantajosamente de tal maneira que o meio para notificar o usuário que uma autenticação implícita pode ser executada pela rede inclua meio para indicar ao usuário se a autenticação implícita é uma decisão final tomada pela rede e nenhuma autenticação explícita pode ser executada, ou a autenticação implícita é uma proposta da rede que o usuário pode aceitar ou recusar forçando uma autenticação explícita.

[0024] No caso que a autenticação implícita é uma proposta pela rede, a entidade de serviço vantajosamente inclui meio para receber uma indicação originada do equipamento de usuário para confirmar a aceitação de tal autenticação implícita proposta pela rede. Além disso, esta entidade de serviço preferivelmente inclui meio para receber tal indicação que o usuário confirmou a autenticação implícita do dispositivo acima.

[0025] Esta entidade de serviço pode vantajosamente incluir meio adicional para verificar o casamento de dados de autenticação adicionais respectivamente recebidos do dispositivo acima e equipamento de usuário a fim de prover um suporte de segurança extra. Estes dados de autenticação adicionais incluem pelo menos um elemento de um grupo de elementos incluindo: tipo de autenticação, informação de acesso e marca de tempo de autenticação.

[0026] A invenção é adicionalmente complementada com a provisão de algumas

outras entidades, tal como uma entidade próxi e uma entidade interrogante, a fim de endereçar uma topologia típica seguindo um padrão de 3GPP ou 3GPP2.

[0027] A entidade próxi, de acordo com padrões de 3GPP e 3GPP2, é destinada a atuar como um ponto de entrada no domínio de Multimídia para usuários acessando a ele por uma rede de acesso onde o usuário já foi autenticado. Esta entidade próxi, de acordo com a invenção, inclui meio para processar pelo menos uma notificação selecionada de um grupo de notificações incluindo:

- uma notificação enviada para o equipamento de usuário para indicar que uma autenticação implícita do usuário para acessar o domínio de Multimídia pode ser executada pela rede; e

- uma notificação recebida do equipamento de usuário para propor uma autenticação implícita para o domínio de Multimídia entre dito equipamento de usuário e domínio de Multimídia.

[0028] Esta entidade próxi também é arranjada vantajosamente de forma que o meio para notificar o usuário que uma autenticação implícita pode ser executada pela rede inclui meio para indicar ao usuário se a autenticação implícita é uma decisão final tomada pela rede e nenhuma autenticação explícita pode ser executada, ou a autenticação implícita é uma proposta da rede que o usuário pode aceitar ou recusar forçando uma autenticação explícita.

[0029] No caso que a autenticação implícita é uma proposta pela rede, a entidade próxi inclui vantajosamente meio para receber uma indicação do equipamento de usuário aceitando tal autenticação implícita proposta pela rede.

[0030] A entidade interrogante, de acordo com padrões de 3GPP e 3GPP2, é destinada a investigar um servidor de assinante no domínio de Multimídia sobre um usuário tendo acessado dito domínio de Multimídia por outra rede de acesso. Esta entidade interrogante tem meio para receber um pedido de registro do usuário, e meio para reconhecer tal registro para o usuário e, de acordo com a invenção, a entidade interrogante também inclui meio para transmitir uma indicação para o equipamento de usuário que uma autenticação implícita do usuário para acessar o domínio de Multimídia pode ser executada.

[0031] A entidade interrogante, a fim de realizar outras características vantajosas providas pela invenção, inclui preferivelmente meio para receber uma indicação originada do equipamento de usuário para confirmar aceitação de uma autenticação implícita proposta pela rede, ou para propor tal autenticação implícita por si mesmo; e meio para transmitir tal confirmação de aceitação do usuário para pelo menos uma entidade selecionada de um grupo de entidades incluindo o dispositivo acima e entidade de serviço.

[0032] Além disso, e também para realizar outras características vantajosas providas pela invenção, a entidade interrogante adicionalmente inclui meio para transmitir para o equipamento de usuário uma indicação que a autenticação implícita é uma decisão final tomada pela rede e nenhuma autenticação explícita pode ser executada.

BREVE DESCRIÇÃO DOS DESENHOS

[0033] As características, objetivos e vantagens da invenção se tornarão aparentes lendo esta descrição junto com os desenhos acompanhantes, em que:

[0034] Figura 1 mostra um diagrama básico do fluxo de autenticação em um domínio de Multimídia de acordo com o padrão de 3GPP TS 33.203.

[0035] Figura 2 ilustra um panorama de componentes arquitetônicos e fluxo de sinalização durante autenticação de um usuário seguindo um mecanismo de EAP-AKA por uma rede de acesso de WLAN.

[0036] Figura 3 mostra um fluxograma descrevendo uma concretização atualmente preferida para reutilizar autenticação prévia de um usuário tendo acesso por uma rede de GPRS ou UMTS ao domínio de Multimídia, onde o equipamento de usuário recebe uma notificação a este respeito e é dada a possibilidade para aceitar ou não uma Autenticação Implícita.

[0037] Figura 4 mostra um fluxograma descrevendo uma concretização alternativa à mostrada na Figura 3, onde o equipamento de usuário recebe uma notificação neste respeito e sem ser dada a possibilidade para aceitar ou não uma Autenticação Implícita, mas em lugar disso sendo informado que tal Autenticação Implícita aconteceu.

[0038] Figura 5 mostra um fluxograma alternativo descrevendo uma concretização alternativa às mostradas na Figura 3 e Figura 4, onde o equipamento de usuário recebe um convite durante o procedimento de localização para adicionalmente executar uma Autenticação Implícita para o domínio de Multimídia, ao usuário assim sendo dada a possibilidade para aceitar ou não uma Autenticação Implícita.

[0039] Figura 6 mostra um fluxograma alternativo ao mostrado na Figura 5, onde o equipamento de usuário recebe um convite com um Serviço de Mensagem Curta (SMS) para adicionalmente executar uma Autenticação Implícita para o domínio de Multimídia, ao usuário assim sendo dada a possibilidade para aceitar ou não uma Autenticação Implícita.

[0040] Figura 7 mostra um fluxograma descrevendo uma concretização atualmente preferida para reutilizar autenticação prévia de um usuário tendo acesso por uma rede de WLAN ao domínio de Multimídia, onde o equipamento de usuário recebe uma notificação neste respeito e é dada a possibilidade para aceitar ou não uma Autenticação Implícita.

[0041] Figura 8 mostra um fluxograma descrevendo outra concretização preferida para reutilizar autenticação prévia de um usuário por uma rede de CDMA 2000, o usuário acessando por uma rede de Serviço de Dados de Pacote ao domínio de Multimídia, onde o equipamento de usuário recebe uma notificação neste respeito e é dada a possibilidade para aceitar ou não uma Autenticação Implícita.

[0042] Figura 9 mostra um fluxograma alternativo àqueles apresentados nas Figuras 5 e 6, onde o equipamento de usuário não recebe um convite, com uma mensagem de Resposta de Localização de Atualização ou com um Serviço de Mensagem Curta (SMS) respectivamente, para adicionalmente executar uma Autenticação Implícita, mas em lugar disso o equipamento de usuário gera uma proposta para uma autenticação implícita à rede.

DESCRIÇÃO DETALHADA DAS CONCRETIZAÇÕES PREFERIDAS

[0043] O seguinte descreve concretizações atualmente preferidas de um aparelho, equipamento de um usuário e método para oferecer a um usuário a

possibilidade para ser autenticado implicitamente por um domínio de Multimídia ao acessar por uma rede de acesso onde o usuário já foi autenticado. A rede de acesso sendo preferivelmente uma Rede de Área Local Sem Fio (WLAN), uma rede de Sistema de Rádio de Pacote Geral (GPRS), uma rede de Sistema Global para Comunicações Móveis (GSM), uma rede de Sistema de Telecomunicação Móvel Universal (UMTS), ou uma rede de Acesso Múltiplo por Divisão de Código (CDMA 2000).

[0044] A presente invenção apresenta vários aspectos com relação ao lugar em que a característica "Autenticação Implícita para domínio de Multimídia" reside, que em particular pode ser executada por um dispositivo isolado em cooperação íntima com um servidor de assinante ou pode ser executada pelo próprio servidor de assinante.

[0045] Além disso, a presente invenção também apresenta vários aspectos com relação ao equipamento de usuário, isto é o terminal do usuário, ou SIM, ou USIM, ou combinações deles, dependendo do grau de decisão que é deixado no lado do usuário ou no lado de rede.

[0046] De acordo com um primeiro aspecto da presente invenção, o próprio servidor de assinante, que em particular pode ser um HSS em 3GPP ou um servidor de AAA em padrões de 3GPP2 e redes de CDMA 2000, ou um dispositivo de Autenticação de Multimídia suportando o acesso ao domínio de Multimídia para um usuário específico determina que uma autenticação explícita para o domínio de Multimídia poderia ser desnecessária baseado em uma autenticação de assinante prévia executada pela rede de acesso por onde o usuário está acessando, e baseado em uma suposição que um portador seguro para sinalização de Multimídia é executado pela rede de acesso. Tal portador seguro pode ser por exemplo um contexto de PDP no caso de GPRS sendo a rede de acesso, ou um túnel seguro no caso de WLAN sendo a rede de acesso para a rede doméstica, enquanto executando a autenticação de assinante.

[0047] De acordo com a invenção, o servidor de assinante, ou o dispositivo de Autenticação de Multimídia dedicado, provê a uma entidade de serviço na função de

autenticar o usuário, isto é uma Função de Controle de Estado de Chamada de Serviço (S-CSCF), uma política de autenticação indicando que um procedimento de Autenticação Implícita pode ser executado para dito usuário acessando o domínio de Multimídia, baseado em uma autenticação de portador prévia pela rede de acesso.

[0048] À parte de autenticar um usuário pela rede onde o usuário está acessando, os procedimentos de autenticação de 3GPP suportam a autenticação da rede pelo usuário. Portanto, e de acordo com outro aspecto da invenção, o servidor de assinante ou o dispositivo de Autenticação de Multimídia dedicado pode opcionalmente indicar ao equipamento de usuário outra política de autenticação para sugerir uma possível Autenticação Implícita mútua que o usuário pode ou não aceitar.

[0049] Graças à característica "Autenticação Implícita para domínio de Multimídia", a quantidade de operações de autenticação executadas tanto pelo usuário ou pelo equipamento de usuário, e pela rede é reduzida e, assim, uma redução de mensagens de sinalização evitáveis no domínio de Multimídia é alcançada enquanto mantendo o nível de segurança requerido, realizando um objetivo da presente invenção.

[0050] A invenção é aplicável a cenários diferentes onde um usuário faz uso de uma rede de acesso particular para acessar o domínio de Multimídia, assim resultando em concretizações diferentes da invenção. Além disso, diversas variações podem ser introduzidas de uma concretização para outra sem partir substancialmente da extensão da presente invenção.

[0051] Um primeiro cenário acontece onde um usuário foi autenticado por uma rede de UMTS e está adicionalmente acessando o domínio de Multimídia por uma rede de GPRS.

[0052] Sob este cenário e de acordo com uma primeira concretização da presente invenção ilustrada na Figura 3, é provido um mecanismo simplificado para autenticar o usuário no domínio de Multimídia, em que o usuário é notificado de uma possível autenticação implícita. O usuário, ou mais exatamente o lado de equipamento de usuário (UE), ao receber esta notificação, pode aceitar a

autenticação implícita ou forçar uma autenticação explícita de acordo com o padrão aplicável para o domínio de Multimídia como a Figura 1 ilustra. Além disso, esta autenticação implícita pode se aplicar a ambas autenticação do usuário pela rede como também autenticação da rede pelo usuário. Além disso, dita autenticação implícita poderia ser ativada por um servidor de assinante tal como o Servidor de Assinante Doméstico (HSS) responsável pela autenticação prévia do usuário na rede de UMTS, como ilustrado na Figura 3, ou por um dispositivo de Autenticação de Multimídia dedicado em cooperação com dito servidor de assinante.

[0053] Portanto, de acordo com esta primeira concretização mostrada na Figura 3, um usuário final ou equipamento de usuário é conectado e autenticado em UMTS e tem um contexto aberto de GPRS PDP. Neste estágio, o usuário final e agente de usuário ganham acesso ao domínio de Multimídia iniciando um procedimento de Registro de SIP.

[0054] Este procedimento de Registro de SIP inclui o envio de uma mensagem de Registro de SIP do lado de usuário (UE) para uma Função de Controle de Estado de Chamada Próxi (P-CSCF), e desta entidade para uma Função de Controle de Estado de Chamada Interrogante (I-CSCF). A I-CSCF inicia um procedimento convencionalmente chamado Cx-Seleção-Info para o Servidor de Assinante Doméstico (HSS) a fim de identificar a Função de Controle de Estado de Chamada de Serviço (S-CSCF) atualmente na função do usuário. Uma vez que tal S-CSCF seja identificada, a I-CSCF envia uma mensagem de Registro de SIP correspondente à S-CSCF. A S-CSCF recebendo tal mensagem de registro inicia um procedimento convencionalmente chamado Cx-pôr para o Servidor de Assinante Doméstico (HSS).

[0055] Dado que o HSS tinha participado previamente na autenticação de acesso de GPRS do usuário trocando um perfil de usuário e vetores de autenticação com um Nó de Suporte de GPRS de Serviço (SGSN), o HSS usa sua informação sobre o SGSN onde o assinante está localizado, além de outra informação de topologia de rede, para determinar a segurança potencial do trajeto de sinalização para acessar o domínio de Multimídia por dita rede de acesso. Por esse meio, de

acordo com a invenção, o próprio HSS, ou um dispositivo de Autenticação de Multimídia dedicado, pode decidir uma Autenticação Implícita para o usuário. Para este fim, o HSS inclui uma indicação de "Autenticação Implícita" na mensagem Cx-pôr resposta para a S-CSCF.

[0056] A decisão para enviar esta mensagem para a S-CSCF é feita vantajosamente quando o Nó de Suporte de GPRS de Ponto de conexão (GGSN) pertence ao mesmo domínio doméstico como o HSS e o GGSN é assim considerado seguro e confiado. Um cenário adequado particular é quando o HSS também confia no SGSN, onde o assinante está localizado como eles ambos pertencem a uma mesma operadora de rede, por exemplo, e independente de se ao usuário é dada ou não a possibilidade para adicionalmente recusar a autenticação implícita proposta.

[0057] Além disso, a característica "Autenticação Implícita para domínio de Multimídia" pode incluir provisão de dados e configuração de dados na base de assinante de forma que quando um usuário tem este serviço provido e o usuário é confiado, o próprio HSS, ou um dispositivo de Autenticação de Multimídia dedicado, possa determinar uma Autenticação Implícita para esse usuário. Neste respeito e levando em conta que a um usuário particular pode ser dada uma pluralidade de identificadores do usuário no domínio de Multimídia, a autenticação implícita referida em seguida, e descrita sob concretizações diferentes, pode se aplicar a todos ou a identificadores do usuário específicos no domínio de Multimídia.

[0058] Adicionalmente, outra informação relevante também pode ser enviada para a S-CSCF na mensagem de Cx-pôr resposta, tal como tipo de autenticação, informação de acesso como por exemplo endereço de IP e informação de contato, marca de tempo de autenticação, e outros dados significantes a fim de prover um suporte de segurança extra.

[0059] Por conseguinte com um aspecto da invenção comentada acima, o usuário pode ser notificado de uma Autenticação Implícita proposta pela rede e destinada para o usuário aceitá-la ou não. Portanto, a S-CSCF envia ao agente de usuário de SIP uma nova mensagem de SIP chamada "Autenticação Implícita 4xx de SIP" na especificação imediata de forma que o agente de usuário de SIP, se achado

aceitável, desabilite internamente o procedimento de Autenticação de Multimídia explícito executado convencionalmente. Quer dizer, o agente de usuário de SIP não deverá esperar ou esperar para receber, tanto uma mensagem de Intimação de Autenticação ou vetores de autenticação como descrito em 3G TS 33.203. Além disso, o agente de usuário de SIP ou, mais geralmente, o equipamento de usuário deverá considerar a rede suportando o domínio de Multimídia como autenticada implicitamente. Por outro lado, o agente de usuário de SIP poderia considerar a Autenticação Implícita não sendo aceitável em qual caso um reconhecimento negativo apropriado não mostrado em qualquer desenho é enviado para a rede a fim de forçar um mecanismo de autenticação explícita convencional de acordo com o padrão aplicável acima.

[0060] Ainda com referência à Figura 3, uma vez que o agente de usuário de SIP tenha aceitado a Autenticação Implícita, ele responde a esta mensagem com uma nova mensagem de Registro de SIP.

[0061] Neste estágio, alguém pode estar ciente que graças à Autenticação Implícita executada de acordo com a invenção reutilizando na autenticação de domínio de Multimídia dados de uma rede de acesso confiada, a presente invenção também provê uma solução vantajosa para suportar Marcação Única (SSO) no domínio de Multimídia para usuários que já tinham sido autenticados por uma rede de acesso antes de acessar dito domínio de Multimídia.

[0062] Alinhada com esta solução vantajosa, Figura 3 mostra que o Registro de SIP enviado finalmente do agente de usuário de SIP do equipamento de usuário à S-CSCF inclui uma indicação de "habilitado para SSO" destinada a indicar à rede que a Autenticação Implícita está aceita. A rede submete tal mensagem de Registro de SIP para a S-CSCF, que por sua vez envia de volta um resultado de êxito "SIP 200 OK" para o equipamento de usuário. O usuário final está agora registrado no domínio de Multimídia sem aqueles processos de autenticação periódicos extras ocorrendo convencionalmente ao longo do registro de Multimídia do usuário final.

[0063] Em geral, isto também é aplicável a outras concretizações adicionalmente descritas, e contanto que haja uma notificação do equipamento de usuário sobre

uma autenticação implícita, a entidade de serviço (S-CSCF) poderia verificar igualmente se outros dados relevantes, respectivamente incluídos no Registro de SIP e na Cx-pôr resposta, são coincidentes com respeito à autenticação implícita e acesso de marcação única. Dito dados relevantes podem ser, por exemplo, um tipo de autenticação, informação de acesso como por exemplo endereço de IP e informação de contato, uma marca de tempo de autenticação, ou combinações disso, e outros dados significantes para prover um suporte de segurança extra.

[0064] Ainda sob o cenário acima onde um usuário foi autenticado por uma rede de UMTS e está adicionalmente acessando o domínio de Multimídia por uma rede de GPRS, e de acordo com uma segunda concretização ilustrada na Figura 4, é provido um mecanismo ainda mais simplificado para autenticar um usuário no domínio de Multimídia, em que o usuário é apenas notificado de uma decisão tomada pela rede para executar uma autenticação implícita. Sob esta segunda concretização, o usuário se conecta à rede de UMTS e é autenticado nela com participação do servidor de assinante doméstico (HSS), um contexto de PDP é ativado com entidades de GPRS (SGSN, GGSN), e uma mensagem de Registro de SIP é enviada para as entidades de Função de Controle de Estado de Chamada (P-CSCF, I-CSCF, S-CSCF) a fim de registrar no domínio de Multimídia de uma maneira semelhante como feita na primeira concretização. A diferença entre estas primeira e segunda concretizações é que o próprio HSS, ou um dispositivo de Autenticação de Multimídia dedicado, faz uma decisão final para executar uma Autenticação Implícita para o usuário. Para este fim, o HSS inclui uma indicação "Autenticação Implícita pela rede" na mensagem de Cx-pôr resposta para a S-CSCF.

[0065] Então, depois de ter completado um "Cx-puxar processo" entre a S-CSCF e o HSS, e sem ter pedido a aceitação do usuário, a S-CSCF notifica ao usuário que a rede executou uma Autenticação Implícita por sua conta incluindo uma indicação "Autenticação Implícita pela rede" em uma resposta de "SIP 2xx OK" específica, em vez de usar a nova mensagem acima de "SIP 4xx".

[0066] Na recepção de dita resposta de "SIP 2xx OK" com uma indicação "Autenticação Implícita pela rede", o agente de usuário de SIP não deverá esperar,

ou esperar receber, tanto uma mensagem de Intimação de Autenticação ou vetores de autenticação como descrito em 3G TS 33.203. Além disso, o agente de usuário de SIP ou, mais geralmente, o equipamento de usuário pode considerar a rede suportando o domínio de Multimídia como autenticada implicitamente, contanto que o equipamento de usuário seja configurado para executar tal autenticação da rede.

[0067] O usuário final agora está registrado no domínio de Multimídia sem aqueles processos de autenticação periódicos extras ocorrendo convencionalmente ao longo do registro de Multimídia do usuário final, e ainda com um mecanismo mais simples do que o descrito na primeira concretização.

[0068] Um segundo cenário acontece onde um usuário foi autenticado por uma rede de UMTS seguindo um procedimento de conexão de GSM e atualização de local, e está adicionalmente acessando um domínio de Multimídia por uma rede de GPRS. Neste respeito e para o propósito de clareza, o Servidor de Assinante Doméstico (HSS) de uma rede de UMTS inclui toda a funcionalidade básica e se comporta como um Registrador de Local Doméstico (HLR) tradicional de uma rede de GSM, mais toda a funcionalidade requerida para atuar como um servidor de assinante em um domínio de Multimídia. Não obstante, contanto que a funcionalidade de HLR tradicional resida em uma entidade diferente do servidor de assinante para o domínio de Multimídia, uma interface adicional entre ambas as entidades, isto é o HLR de GSM e o servidor de assinante para o domínio de Multimídia, é usada para compartilhar dados de autenticação de usuário.

[0069] Uma terceira concretização sob o segundo cenário acima é ilustrada na Figura 5, em que um novo campo é retornado ao agente de usuário de SIP do equipamento de usuário durante procedimentos de conexão de GSM e atualização de local. Portanto, o servidor de assinante (HSS) do domínio de Multimídia inclui uma indicação de "Autenticação Implícita" na operação de GSM "Inserir Dados de Assinante" para o Nó de Suporte de GPRS de Serviço (SGSN) na rede de acesso. Então, o SGSN também inclui esta indicação de "Autenticação Implícita" na operação de GSM "Resposta de Local de Atualização" para o agente de usuário de SIP.

[0070] Esta indicação pode se aplicar a todos ou identificadores específicos do usuário no domínio de Multimídia, e é compreendido pelo equipamento de usuário (UE) como um convite implícito para habilitar um acesso de Marcação Única (SSO) para o domínio de Multimídia que o equipamento de usuário pode ou não aceitar. Contanto que a autenticação implícita seja aceitável para o usuário final (UE) como nenhuma segurança extra é requerida, uma mensagem de Registro de SIP é enviada ao domínio de Multimídia (P-CSCF, I-CSCF), a mensagem de Registro de SIP incluindo uma indicação de "habilitado para SSO" destinada a indicar à rede que a Autenticação Implícita está aceita.

[0071] Na recepção de tal mensagem de Registro de SIP em uma entidade de Função de Controle de Estado de Chamada Interrogante (I-CSCF), a indicação de "habilitado para SSO" é incorporada em um novo campo de uma mensagem de "Cx-consulta" incluída em um denominado procedimento de "Cx-seleção-Info" contido com o servidor de assinante de domínio de Multimídia (HSS). Neste estágio, a característica "Autenticação Implícita para domínio de Multimídia" no próprio HSS, ou em um dispositivo de Autenticação de Multimídia dedicado, processa a indicação de "habilitado para SSO" a fim de prover adicionalmente dados de autenticação para o usuário no pedido.

[0072] A indicação de "habilitado para SSO" também é incorporada no Registro de SIP enviado da I-CSCF para a entidade de Função de Controle de Estado de Chamada de Serviço (S-CSCF) selecionada atualmente para servir o usuário. Como em concretizações prévias, a presente concretização ilustrada na Figura 5 também mostra uma operação de "Cx-pôr" executada da S-CSCF ao HSS. O HSS assim instrui a S-CSCF com uma operação de "Cx-pôr resposta" que inclui uma indicação de "Autenticação Implícita confirmada por usuário" a fim de impedir uma autenticação adicional do usuário final e para evitar enviar vetores de autenticação para dito usuário final. Por sua vez, a S-CSCF poderia verificar igualmente se outros dados relevantes incluídos respectivamente no Registro de SIP e na Cx-pôr resposta, são coincidentes com respeito à autenticação implícita e acesso de marcação única, dados relevantes tais como tipo de autenticação, informação de

acesso como por exemplo endereço de IP e informação de contato, marca de tempo de autenticação, ou combinações disso, e outros dados significantes para prover um suporte de segurança extra.

[0073] Eventualmente, depois de ter concluído um "Cx-puxar processo" entre a S-CSCF e o servidor de assinante (HSS), a S-CSCF retorna ao usuário um resultado de êxito convencional "SIP 200 OK" para o agente de usuário de SIP ao equipamento de usuário.

[0074] Uma quarta concretização adicional sob o segundo cenário acima é ilustrada na Figura 6, em que a única diferença com a terceira concretização prévia mostrada na Figura 5 é que a indicação de "Autenticação Implícita" é retornada ao agente de usuário de SIP do equipamento de usuário em uma Mensagem Curta enviada de um Centro de Serviço de Mensagem Curta (SMSC) como instruído previamente pelo próprio servidor de assinante (HSS), ou por um dispositivo de Autenticação de Multimídia dedicado, e então os procedimentos de conexão de GSM e autenticação são terminados, em vez de serem feitos durante o procedimento de atualização de local. Por causa de clareza nos desenhos, o par de entidades de GPRS, SGSN e GGSN na Figura 5, é substituído com uma denominada entidade de "GSN" na Figura 6. Esta indicação de "Autenticação Implícita", como para uma concretização acima, também pode se aplicar a todos ou identificadores específicos do usuário no domínio de Multimídia. Uma vez que o equipamento de usuário esteja ciente de ter recebido esta indicação de "Autenticação Implícita", e contanto que tal autenticação implícita seja achada aceitável, o equipamento de usuário processa a mensagem, e inclui uma indicação de "habilitado para SSO" em uma mensagem de Registro de SIP sendo enviada para acessar o domínio de Multimídia (P-CSCF, I-CSCF), a indicação de "habilitado para SSO" destinada a indicar à rede que a Autenticação Implícita está aceita pelo equipamento de usuário. Deste ponto em diante, o fluxo de sinalização pode ser o mesmo como na terceira concretização prévia.

[0075] Também nas concretizações sob este segundo cenário, o usuário final é registrado no domínio de Multimídia sem esses processos de autenticação

periódicos extras ocorrendo convencionalmente ao longo do registro de Multimídia do usuário final, e com um mecanismo mais simples do que o executado convencionalmente.

[0076] Um terceiro cenário aparece onde um usuário acessando por uma Rede de Área Local Sem Fios, foi autenticado por uma rede de UMTS e está adicionalmente acessando o domínio de Multimídia por esta Rede de Área Local Sem Fios (WLAN).

[0077] De acordo com uma quinta concretização ilustrada na Figura 7 sob este terceiro cenário, um usuário final está conectado e autenticado na WLAN pela rede de UMTS, o usuário final, ou mais exatamente o equipamento de usuário (UE), obteve uma sessão de IP aberta preferivelmente usando um denominado convencionalmente túnel seguro à rede doméstica. Este túnel seguro é estabelecido preferivelmente entre o equipamento de usuário e um Ponto de conexão de Dados de Pacote (PD-GW) encapsulando dados da sessão de IP acima, geralmente um endereço de IP, dentro da carga útil de mensagem codificada, enquanto um endereço de IP externo não relacionado à sessão de IP é usado entre o equipamento de usuário (UE) e o Ponto de conexão de Dados de Pacote (PD-GW).

[0078] Neste estágio e da mesma maneira como para a primeira concretização mostrada na Figura 3, o fluxo de sinalização na Figura 7 mostra como o usuário final e agente de usuário de SIP, isto é o equipamento de usuário (UE), ganham acesso ao domínio de Multimídia enviando uma mensagem de Registro de SIP do lado de usuário (UE) para o domínio de Multimídia (P-CSCF, I-CSCF).

[0079] Uma entidade de Função de Controle de Estado de Chamada Interrogante (I-CSCF) inicia um procedimento convencionalmente chamado "Cx-seleção-Info" para o Servidor de Assinante Doméstico (HSS), isto é o servidor de assinante no domínio de Multimídia, a fim de identificar uma Função de Controle de Estado de Chamada de Serviço (S-CSCF) atualmente na função do usuário. Uma vez que tal S-CSCF seja identificada, a I-CSCF envia uma mensagem de Registro de SIP correspondente à S-CSCF. A S-CSCF recebendo tal mensagem de registro inicia um procedimento convencionalmente chamado Cx-pôr para o Servidor de

Assinante Doméstico (HSS).

[0080] Dado que o HSS tinha previamente participado na autenticação do usuário para acesso à WLAN trocando um perfil do usuário e vetores de autenticação de usuário com um denominado servidor de "Autenticação, Autorização e Contabilidade" seguindo os padrões de 3GPP (em seguida referido como AAA-3GPP), como ilustrado na Figura 2, o HSS pode usar sua informação sobre o túnel seguro além de outra informação de topologia de rede para determinar a segurança potencial do trajeto de sinalização para acessar o domínio de Multimídia por dita rede de acesso. Por esse meio, de acordo com a invenção, o próprio HSS, ou um dispositivo de Autenticação de Multimídia dedicado, pode decidir uma Autenticação Implícita para dito usuário. Esta decisão é feita vantajosamente quando o Ponto de conexão de Dados de Pacote (PD-GW) pertence ao mesmo domínio doméstico como o HSS, ou em outras situações onde o PD-GW é considerado seguro e confiado. Além disso, a característica "Autenticação Implícita para domínio de Multimídia" pode Incluir, como em concretizações prévias, provisão de dados e configuração de dados na base de assinante de forma que quando um usuário tem este serviço provido e o usuário é confiado, o próprio HSS, ou um dispositivo de Autenticação de Multimídia dedicado, possa determinar uma Autenticação Implícita para esse usuário.

[0081] Portanto, o HSS incorpora uma indicação de "Autenticação Implícita" na "Cx-pôr resposta" para a S-CSCF. Vantajosamente e por causa de segurança, outra informação relevante também pode ser enviada para a S-CSCF na mensagem de "Cx-pôr resposta", tal como tipo de autenticação, informação de acesso como por exemplo endereço de IP e informação de contato, marca de tempo de autenticação, e outros dados significantes para prover um suporte de segurança extra.

[0082] Esta quinta concretização na Figura 7 está alinhada com a primeira concretização na Figura 3 e ambas estão de acordo com um aspecto da invenção comentado acima, onde o usuário pode ser notificado de uma Autenticação Implícita proposta pela rede e destinada para o usuário aceitá-la ou não.

[0083] Portanto, a S-CSCF envia ao agente de usuário de SIP uma nova

mensagem de SIP chamada "SIP 4xx Autenticação Implícita" na especificação imediata de forma que o agente de usuário de SIP, se achado aceitável, desabilite internamente o procedimento de Autenticação de Multimídia explícita convencionalmente executado. Quer dizer, o agente de usuário de SIP não deverá esperar ou espera receber, tanto uma mensagem de Intimação de Autenticação ou vetores de autenticação como descrito em 3G TS 33.203.

[0084] Uma vez que o agente de usuário de SIP tenha aceito a Autenticação Implícita, ele responde a esta mensagem de "SIP 4xx Autenticação Implícita" com uma nova mensagem de Registro de SIP que inclui uma indicação de "habilitado para SSO" destinada a indicar à rede que a Autenticação Implícita está aceita. A rede (P-CSCF, I-CSCF) submete tal mensagem de Registro de SIP para a S-CSCF, que por sua vez envia de volta um resultado de êxito "SIP 200 OK" para o equipamento de usuário (UE). O usuário final, tendo acessado por uma rede de WLAN, está agora registrado no domínio de Multimídia sem aqueles processos de autenticação periódicos extras ocorrendo tipicamente ao longo do registro de Multimídia do usuário final.

[0085] A descrição para a quinta concretização ilustrada na Figura 7 foi casada tanto quanto possível com a para a primeira concretização mostrada na Figura 3. Semelhantemente, o ensinamento da segunda concretização mostrada na Figura 4, onde GPRS é a rede de acesso, pode ser aplicável convenientemente à outra concretização, onde WLAN é a rede de acesso, a última não requerendo explicação adicional devido às concretizações anteriores.

[0086] Por outro lado, a terceira concretização anterior, onde GPRS é a rede de acesso, é praticamente aplicável igualmente a outra concretização, onde WLAN é a rede de acesso visto que as indicações de autenticação relevantes enviadas ao equipamento de usuário estão incluídas como Par de Valores de Atributo específico (AVP) nas mensagens correspondentes de um protocolo de RADIUS ou Diameter usado por acesso de WLAN.

[0087] Eventualmente, a quarta concretização anterior, onde GPRS é a rede de acesso, também é aplicável a outra concretização, onde WLAN é a rede de acesso

assumindo um suporte para Serviços de Mensagem Curta (SMS) em WLAN, ou usando a tecnologia de Comutação por Circuito de uma infra-estrutura de GRPS para SMS no caso de ter terminais duais como o equipamento de usuário.

[0088] Um quarto cenário aparece onde um usuário foi autenticado por uma rede de CDMA 2000 seguindo um procedimento de conexão de Serviço de Dados de Pacote, e está adicionalmente acessando um domínio de Multimídia por uma rede de Serviço de Dados de Pacote. Figura 8 ilustra uma sexta concretização alinhada com a na Figura 4 sob o primeiro cenário, em que um servidor de Autenticação, Autorização e Contabilidade (AAA) atua como servidor de assinante de uma rede de CDMA 2000. Neste respeito e por causa de clareza, o Servidor de Autenticação, Autorização e Contabilidade (AAA) da rede de CDMA 2000 inclui toda a funcionalidade básica requerida para permitir o acesso a Serviços de Dados de Pacote em uma rede de CDMA 2000, e toda a funcionalidade requerida para atuar como um servidor de assinante em um domínio de Multimídia.

[0089] Não obstante, contanto que a funcionalidade de AAA tradicionalmente conhecida para acesso a Serviços de Dados de Pacote de CDMA 2000 resida em uma entidade diferente do servidor de assinante para o domínio de Multimídia, uma interface adicional entre ambas as entidades, isto é entre um servidor de AAA de CDMA 2000 e de assinante tradicional para o domínio de Multimídia, é usada para compartilhar dados de autenticação de usuário.

[0090] À parte destas considerações, as concretizações anteriores também são aplicáveis a este cenário envolvendo uma rede de CDMA 2000 assumindo que a informação relevante pode ser transportada usando extensões para as interfaces de RADIUS e Diameter atuais.

[0091] Uma concretização ainda adicional é apresentada sobre o primeiro cenário exemplar acima e ilustrada na Figura 9, em que a proposta para uma autenticação implícita (Proposta de SSO) é ativada de fato do próprio equipamento de usuário (UE) e sem ter recebido um convite prévio do domínio de Multimídia (IMS). Assim, o fluxograma na Figura 9 apresenta uma concretização alternativa àquelas nas Figuras 5 e 6, em que o equipamento de usuário (UE) submete

diretamente ao domínio de Multimídia (IMS) sua proposta para uma autenticação implícita (Proposta de SSO), sem ter recebido o convite prévio com uma mensagem de Resposta de Local de Atualização ou com um Serviço de Mensagem Curta (SMS), e a fim de executar tal autenticação implícita entre dito equipamento de usuário e domínio de Multimídia.

[0092] Esta nova abordagem poderia ser aplicada igualmente para modificar outras concretizações anteriores e independentemente do cenário de aplicação.

[0093] A invenção é descrita acima em relação a várias concretizações de uma maneira ilustrativa e não restritiva. Obviamente, modificações e variações da presente invenção são possíveis à luz dos ensinamentos anteriores, e qualquer modificação das concretizações que caía dentro da extensão das reivindicações é pretendida ser incluída nelas.

REIVINDICAÇÕES

1. Dispositivo de autenticação de multimídia para autenticação de Multimídia de um usuário (UE), o usuário acessando um domínio de Multimídia (IMS) por uma rede de acesso (UMTS; WLAN; GPRS; CDMA 2000) onde o usuário é previamente autenticado, o dispositivo de autenticação de multimídia para uso em cooperação com um servidor de assinante (HSS; AAA) da rede de acesso, o servidor de assinante contendo dados de autenticação para o usuário e acessível ao domínio de Multimídia (IMS), o dispositivo de autenticação de multimídia caracterizado pelo fato de compreender:

- meio para decidir em cooperação com o servidor de assinante que uma autenticação implícita entre o usuário (UE) e o domínio de Multimídia (IMS) é possível com base em uma autenticação prévia do usuário (UE) pela rede de acesso (UMTS; WLAN; GPRS; CDMA 2000), assim, saltando a necessidade por uma autenticação explícita; e

- meio para instruir uma entidade de serviço (S-CSCF) na função de autenticar o usuário (UE) no domínio de multimídia (IMS) que a autenticação implícita é possível.

2. Dispositivo de autenticação de multimídia de acordo com a reivindicação 1, caracterizado pelo fato de que o meio para decidir que uma autenticação implícita é possível inclui meio de dados de provisão e configuração arranjado para avaliar a segurança de trajetos de sinalização diferentes, e meio para determinar a segurança potencial do trajeto de sinalização para acessar o domínio de Multimídia por dita rede de acesso.

3. Dispositivo de autenticação de multimídia de acordo com a reivindicação 1, caracterizado pelo fato de que o meio para instruir a entidade de serviço que uma autenticação implícita é possível inclui meio para indicar (Autenticação Implícita) que a decisão final é no lado do usuário (UE) que poderia forçar uma autenticação explícita.

4. Dispositivo de autenticação de multimídia de acordo com a reivindicação 1, caracterizado pelo fato de que o meio para instruir a entidade de

serviço que uma autenticação implícita é possível inclui meio para indicar (Autenticação Implícita pela rede) que esta é uma decisão final tomada pela rede e nenhuma autenticação explícita deve ser executada.

5. Dispositivo de autenticação de multimídia de acordo com a reivindicação 1, caracterizado pelo fato de incluir adicionalmente meio (Autenticação Implícita; Autenticação Implícita pela rede) para notificar o equipamento de usuário que uma autenticação implícita do usuário pela rede é possível para acessar o domínio de Multimídia.

6. Dispositivo de autenticação de multimídia de acordo com a reivindicação 1, caracterizado pelo fato de que o meio para decidir que uma autenticação implícita entre o usuário (UE) e o domínio de Multimídia (IMS) é possível inclui meio para receber uma proposta de autenticação implícita (proposta de SSO) originada do equipamento de usuário (UE).

7. Dispositivo de autenticação de multimídia de acordo com a reivindicação 3, caracterizado pelo fato de compreender meio para receber uma indicação (habilitado para SSO) originada do equipamento de usuário (UE) para confirmar a aceitação da autenticação implícita proposta pela rede.

8. Dispositivo de autenticação de multimídia de acordo com a reivindicação 7, caracterizado pelo fato de compreender meio para indicar (Autenticação Implícita confirmada por usuário) à entidade de serviço (S-CSCF) na função de autenticar o usuário no domínio de Multimídia (IMS) que o usuário confirmou a autenticação implícita.

9. Dispositivo de autenticação de multimídia de acordo com a reivindicação 8, caracterizado pelo fato de compreender meio para prover dados de autenticação adicionais para dita entidade de serviço (S-CSCF), ditos dados de autenticação adicionais incluindo pelo menos um elemento selecionado de um grupo de elementos compreendendo: tipo de autenticação; informação de acesso; e marca de tempo de autenticação.

10. Equipamento de usuário (UE) habilitado para adquirir acesso a um domínio de Multimídia (IMS) por uma rede de acesso (UMTS; WLAN; GPRS; CDMA

2000), e arranjado para executar um primeiro procedimento de Autenticação explícita com a rede de acesso e um segundo procedimento de autenticação explícita com o domínio de Multimídia (IMS), caracterizado pelo fato de ter meio para processar pelo menos uma notificação selecionada de um grupo de notificações incluindo:

- uma notificação (Autenticação Implícita; Autenticação Implícita pela rede) recebida do domínio de Multimídia (IMS) indicando que uma autenticação implícita do usuário pela rede é possível; e

- uma notificação (Proposta de SSO) proposta do equipamento de usuário (UE) para o domínio de Multimídia (IMS) executar uma autenticação implícita entre dito equipamento de usuário e domínio de Multimídia.

11. Equipamento de usuário (UE) de acordo com a reivindicação 10, caracterizado pelo fato de que o meio para processar uma notificação recebida do domínio de Multimídia (IMS) inclui meio para receber e processar uma indicação (Autenticação Implícita) que a decisão final está no equipamento de usuário (UE) que poderia forçar uma autenticação explícita.

12. Equipamento de usuário (UE) de acordo com a reivindicação 11, caracterizado pelo fato de compreender meio para enviar para o domínio de Multimídia (IMS) uma indicação (habilitado para SSO) para confirmar a aceitação da autenticação implícita proposta pela rede.

13. Equipamento de usuário (UE) de acordo com a reivindicação 12, caracterizado pelo fato de compreender meio para prover dados de autenticação adicionais para o domínio de Multimídia (IMS), ditos dados de autenticação adicionais incluindo pelo menos um elemento selecionado de um grupo de elementos incluindo: tipo de autenticação; informação de acesso; e marca de tempo de autenticação.

14. Equipamento de usuário (UE) de acordo com a reivindicação 10, caracterizado pelo fato de que o meio para processar uma notificação recebida do domínio de Multimídia (IMS) inclui meio para receber e processar uma indicação (Autenticação Implícita pela rede) que a autenticação implícita é uma decisão final

tomada pela rede e nenhuma autenticação explícita deve ser executada.

15. Método para autenticar um usuário (UE) acessando um domínio de Multimídia (IMS) por uma rede de acesso (UMTS; WLAN; GPRS; CDMA 2000), compreendendo:

- uma etapa de autenticar o usuário na rede de acesso (UMTS; WLAN; GPRS; CDMA 2000) por onde o usuário acessa, a rede de acesso tendo um servidor de assinante (HSS; AAA) com dados de autenticação para o usuário e acessível ao domínio de Multimídia (IMS); e

- uma etapa de registrar o usuário (UE) no domínio de Multimídia (IMS);

caracterizado pelo fato de compreender:

- uma etapa de decidir, por um dispositivo de autenticação de multimídia em cooperação com o servidor de assinante, que uma autenticação implícita entre o usuário (UE) e o domínio de Multimídia (IMS) é possível com base na autenticação prévia do usuário (UE) na rede de acesso (UMTS; WLAN; GPRS; CDMA 2000), assim, saltando a necessidade por uma autenticação explícita; e

- uma etapa de instruir uma entidade de serviço (S-CSCF) na função de autenticar o usuário (UE) no domínio de Multimídia (IMS) que a autenticação implícita é possível.

16. Método de acordo com a reivindicação 15, caracterizado pelo fato de compreender uma etapa de notificar do domínio de Multimídia (IMS) (Autenticação Implícita; Autenticação Implícita pela rede) ao equipamento de usuário (UE) que autenticação implícita do usuário é possível para acessar o domínio de Multimídia.

17. Método de acordo com a reivindicação 15, caracterizado pelo fato de que a etapa de decidir que uma autenticação implícita é possível inclui uma etapa de avaliar a segurança de trajetos de sinalização diferentes, e uma etapa de determinar a segurança potencial do trajeto de sinalização para acessar o domínio de Multimídia por dita rede de acesso.

18. Método de acordo com a reivindicação 15, caracterizado pelo fato de que a etapa de decidir que uma autenticação implícita é possível inclui uma etapa de propor do equipamento de usuário (UE) para o domínio de Multimídia (IMS) uma

autenticação implícita a ser executada entre dito equipamento de usuário e o domínio de Multimídia.

19. Método de acordo com a reivindicação 15, caracterizado pelo fato de que a etapa de instruir a entidade de serviço que uma autenticação implícita é possível inclui uma etapa de indicar (Autenticação Implícita pela rede) que esta é uma decisão final tomada pela rede e nenhuma autenticação explícita deve ser executada.

20. Método de acordo com a reivindicação 15, caracterizado pelo fato de que a etapa de instruir a entidade de serviço que uma autenticação implícita é possível inclui uma etapa de indicar (Autenticação Implícita) que a decisão final está no equipamento de usuário que poderia forçar uma autenticação explícita.

21. Método de acordo com a reivindicação 20, caracterizado pelo fato de compreender adicionalmente uma etapa de confirmar (habilitado para SSO) do equipamento de usuário (UE) aceitação da autenticação implícita proposta pela rede.

22. Método de acordo com a reivindicação 21, caracterizado pelo fato de compreender adicionalmente uma etapa de indicar (Autenticação Implícita confirmada por usuário) à entidade de serviço (S-CSCF) na função de autenticar o usuário (UE) no domínio de Multimídia (IMS) que o usuário confirmou a autenticação implícita.

23. Entidade de serviço (S-CSCF) na função de autenticar um usuário (UE) no domínio de Multimídia (IMS) quando o usuário o acessa por uma rede de acesso (UMTS; WLAN; GPRS; CDMA 2000) onde dito usuário tinha sido autenticado previamente, a entidade de serviço (S-CSCF) caracterizada pelo fato de compreender:

- meio para receber e processar instruções (Autenticação Implícita; Autenticação Implícita pela rede) originada de um dispositivo de autenticação de multimídia para autenticação de Multimídia do usuário, as instruções indicando que uma autenticação implícita entre o usuário (UE) e o domínio de Multimídia (IMS) é possível com base na autenticação prévia do usuário (UE) pela rede de acesso

(UMTS; WLAN; GPRS; CDMA 2000); e

- meio para notificar (Autenticação Implícita; Autenticação Implícita pela rede) a um equipamento de um usuário (UE) que uma autenticação implícita do usuário pela rede é possível para acessar o domínio de Multimídia (IMS).

24. Entidade de serviço (S-CSCF) de acordo com a reivindicação 23, caracterizada pelo fato de compreender meio para receber uma indicação (habilitado para SSO) originada do equipamento de usuário (UE) para confirmar aceitação de uma autenticação implícita proposta pela rede.

25. Entidade de serviço (S-CSCF) de acordo com a reivindicação 23, caracterizada pelo fato de compreender meio para receber uma indicação (Autenticação Implícita confirmada por usuário) originada do dispositivo de autenticação de multimídia indicando que o usuário confirmou a autenticação implícita.

26. Entidade de serviço (S-CSCF) de acordo com a reivindicação 25, caracterizada pelo fato de compreender adicionalmente meio para verificar um casamento de dados de autenticação adicionais recebidos respectivamente do dispositivo de autenticação de multimídia e do equipamento de usuário a fim de prover um suporte de segurança extra.

27. Entidade de serviço (S-CSCF) de acordo com a reivindicação 26, caracterizada pelo fato de que ditos dados de autenticação adicionais incluem pelo menos um elemento selecionado de um grupo de elementos compreendendo: tipo de autenticação; informação de acesso; e marca de tempo de autenticação.

28. Entidade de serviço (S-CSCF) de acordo com a reivindicação 23, caracterizada pelo fato de que o meio para notificar o usuário (UE) que uma autenticação implícita pela rede é possível inclui meio para indicar (Autenticação Implícita pela rede) ao usuário (UE) que a autenticação implícita é uma decisão final tomada pela rede e nenhuma autenticação explícita deve ser executada.

29. Entidade próxi (P-CSCF) destinada a atuar como um ponto de entrada no domínio de Multimídia (IMS) para usuários (UE) o acessando por uma rede de acesso (UMTS; WLAN; GPRS; CDMA 2000) onde o usuário tinha sido autenticado

previamente, a entidade próxi caracterizada pelo fato de ter meio para processar pelo menos uma notificação selecionada de um grupo de notificações incluindo:

- uma notificação (Autenticação Implícita; autenticação Implícita pela rede) enviada para o equipamento de usuário (UE) para indicar que uma autenticação implícita do usuário, pela rede, é possível para acessar o domínio de Multimídia (IMS); e

- uma notificação (Proposta de SSO) recebida do equipamento de usuário (UE) para propor uma autenticação implícita para o domínio de Multimídia (IMS) entre dito equipamento de usuário e domínio de Multimídia.

30. Entidade próxi (P-CSCF) de acordo com a reivindicação 29, caracterizada pelo fato de compreender adicionalmente meio para receber uma indicação (habilitado para SSO) do equipamento de usuário (UE) aceitando a autenticação implícita proposta pela rede.

31. Entidade próxi (P-CSCF) de acordo com a reivindicação 29, caracterizada pelo fato de compreender adicionalmente meio para indicar (Autenticação Implícita pela rede) ao usuário (UE) que a autenticação implícita é uma decisão final tomada pela rede e nenhuma autenticação explícita deve ser executada.

32. Entidade interrogante (I-CSCF) consultando um servidor de assinante (HSS; AAA-3GPP) no domínio de Multimídia (IMS) sobre um usuário (UE) tendo acessado dito domínio de Multimídia por uma rede de acesso (WLAN; GPRS), a entidade interrogante tendo meio para receber um pedido de registro do usuário, e meio para reconhecer tal registro para o usuário, e caracterizada pelo fato de compreender meio para transmitir uma indicação (Autenticação Implícita; autenticação Implícita pela rede) para o usuário (UE) que uma autenticação implícita do usuário, pela rede, é possível para acessar o domínio de Multimídia (IMS).

33. Entidade interrogante (I-CSCF) de acordo com a reivindicação 32, caracterizada pelo fato de compreender adicionalmente:

- meio para receber uma indicação (habilitado para SSO; proposta de SSO) originada do equipamento de usuário (UE) para habilitar uma autenticação

implícita; e

- meio para transmitir tal indicação do equipamento de usuário para pelo menos uma entidade selecionada de um grupo de entidades compreendendo um dispositivo de autenticação de multimídia para autenticação de Multimídia de um usuário e uma entidade de serviço (S-CSCF) na função de autenticar o usuário no domínio de Multimídia (IMS).

34. Entidade interrogante (I-CSCF) de acordo com a reivindicação 32, caracterizada pelo fato de compreender adicionalmente meio para transmitir para o usuário (UE) uma indicação (Autenticação Implícita pela rede) que a autenticação implícita é uma decisão final tomada pela rede e nenhuma autenticação explícita deve ser executada.

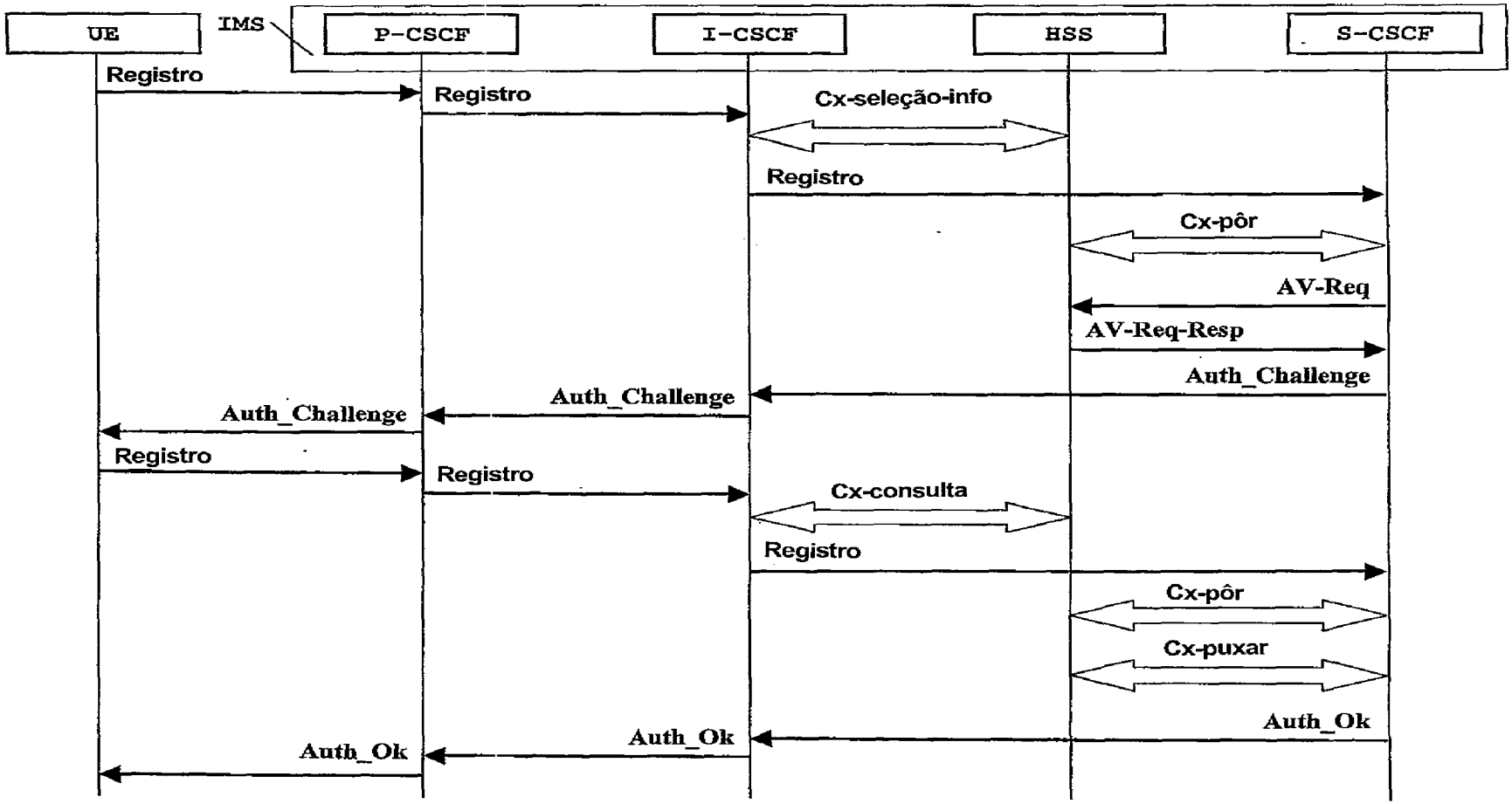

FIG. 1- Estado da Arte

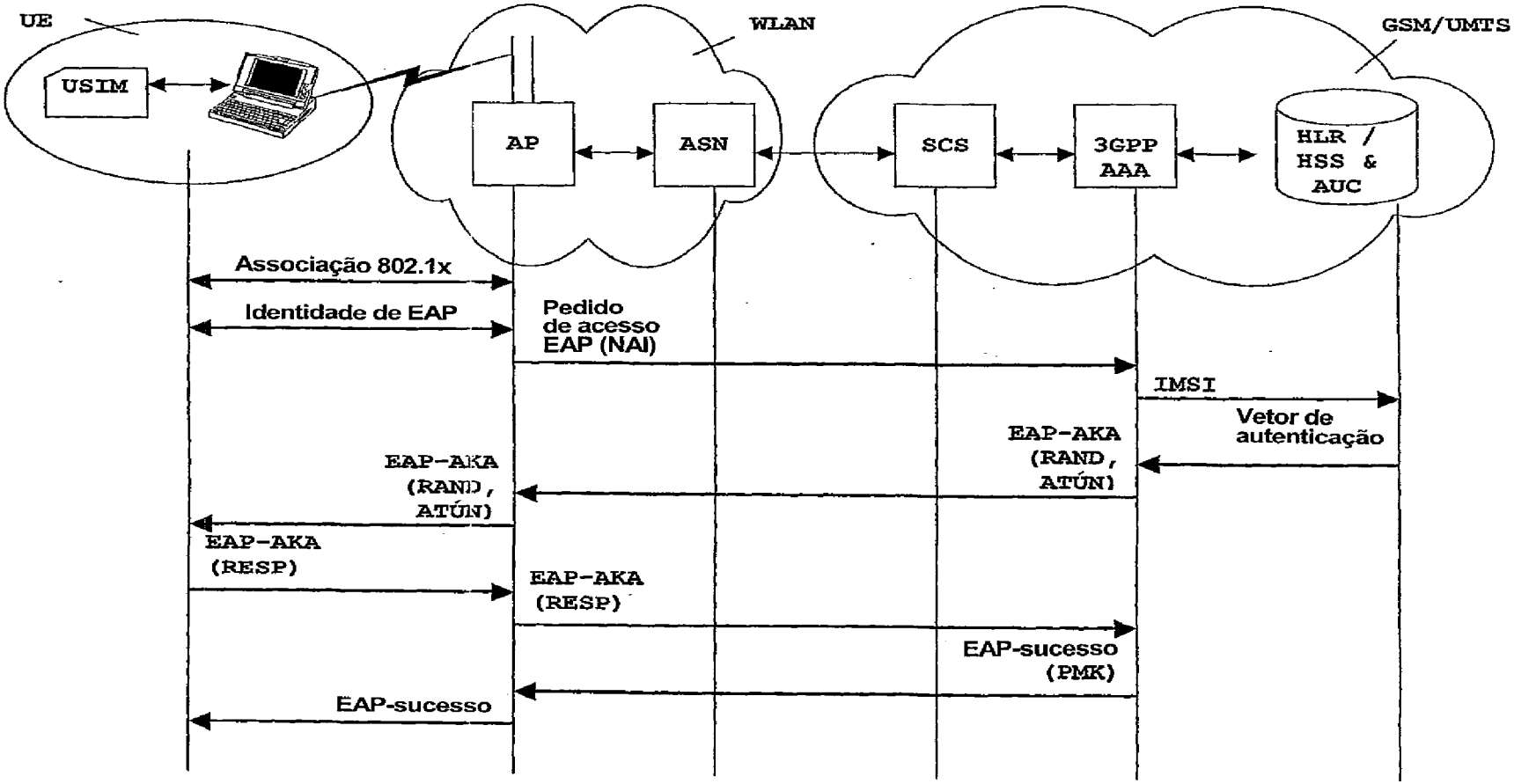

FIG. 2- Estado da Arte

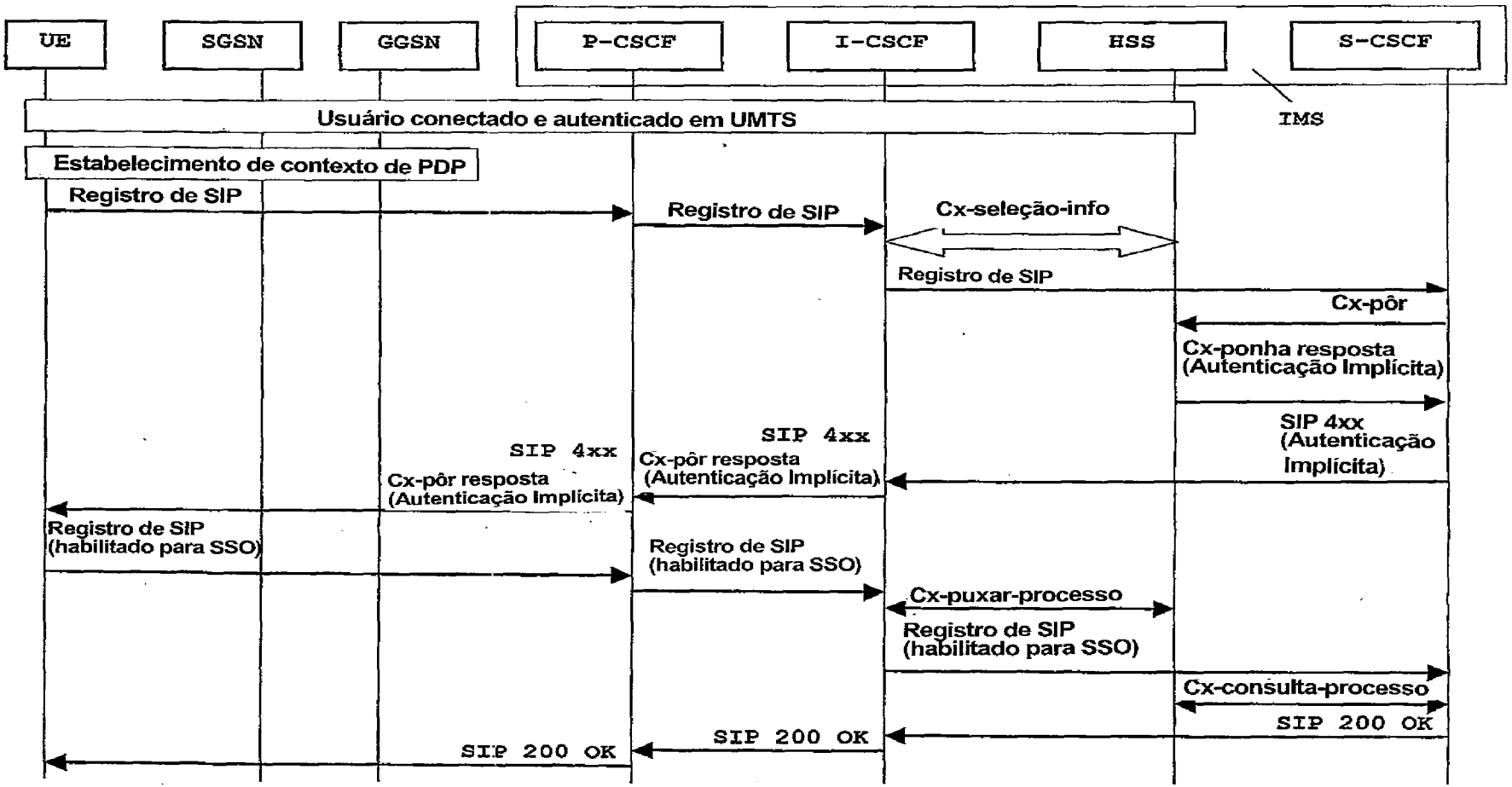
UE
SGSN
GGSN
P-CSCF
I-CSCF
HSS
S-CSCF
IMS
Usuário conectado e autenticado em UMTS
Estabelecimento de contexto de PDP
Registro de SIP
Registro de SIP
Cx-seleção-info
Registro de SIP
Cx-pôr
Cx-ponha resposta (Autenticação Implícita)
SIP 4xx (Autenticação Implícita)
SIP 4xx
Cx-pôr resposta (Autenticação Implícita)
Cx-pôr resposta (Autenticação Implícita)
Registro de SIP (habilitado para SSO)
Registro de SIP (habilitado para SSO)
Cx-puxar-processo
Registro de SIP (habilitado para SSO)
Cx-consulta-processo
SIP 200 OK
SIP 200 OK
SIP 200 OK

FIG.-3-

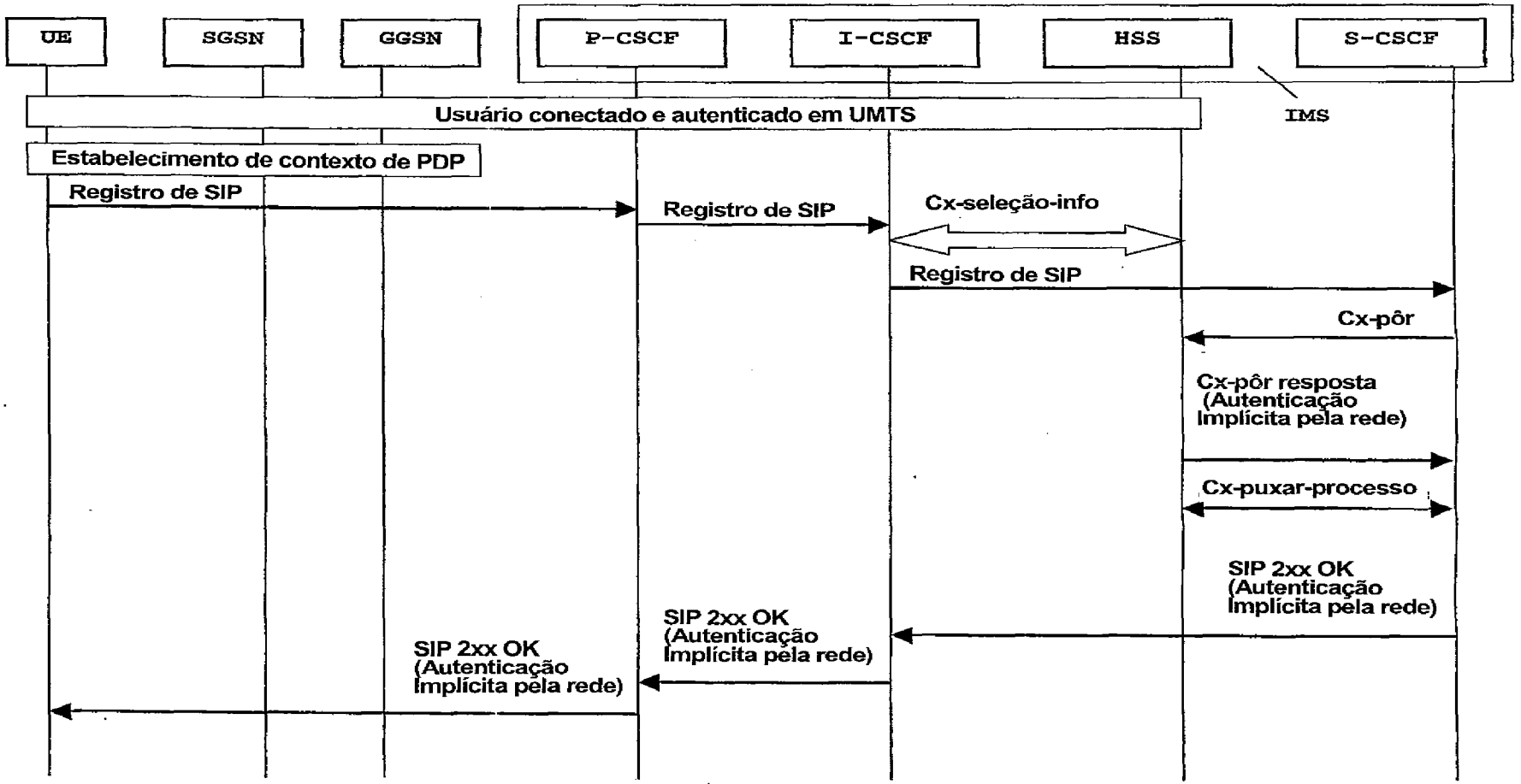
UE
SGSN
GGSN
P-CSCF
I-CSCF
HSS
S-CSCF
IMS
Usuário conectado e autenticado em UMTS
Estabelecimento de contexto de PDP
Registro de SIP
Registro de SIP
Cx-seleção-info
Registro de SIP
Cx-pôr
Cx-pôr resposta
(Autenticação
Implícita pela rede)
Cx-puxar-processo
SIP 2xx OK
(Autenticação
Implícita pela rede)
SIP 2xx OK
(Autenticação
Implícita pela rede)
SIP 2xx OK
(Autenticação
Implícita pela rede)

FIG.-4-

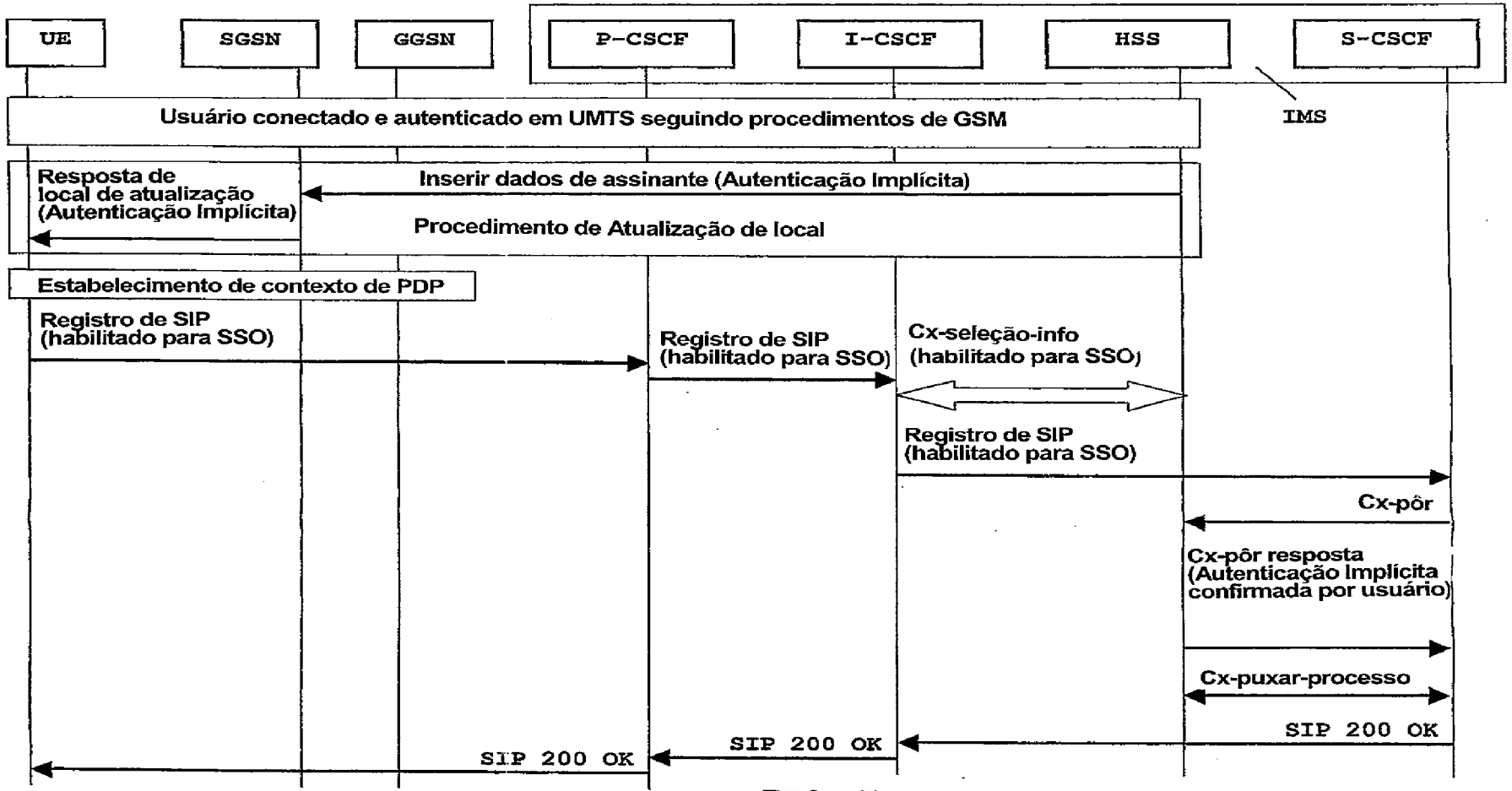
UE
SGSN
GGSN
P-CSCF
I-CSCF
HSS
S-CSCF
IMS
Usuário conectado e autenticado em UMTS seguindo procedimentos de GSM
Resposta de local de atualização (Autenticação Implícita)
Inserir dados de assinante (Autenticação Implícita)
Procedimento de Atualização de local
Estabelecimento de contexto de PDP
Registro de SIP (habilitado para SSO)
Registro de SIP (habilitado para SSO)
Cx-seleção-info (habilitado para SSO)
Registro de SIP (habilitado para SSO)
Cx-pôr
Cx-pôr resposta (Autenticação Implícita confirmada por usuário)
Cx-puxar-processo
SIP 200 OK
SIP 200 OK
SIP 200 OK

FIG.-5-

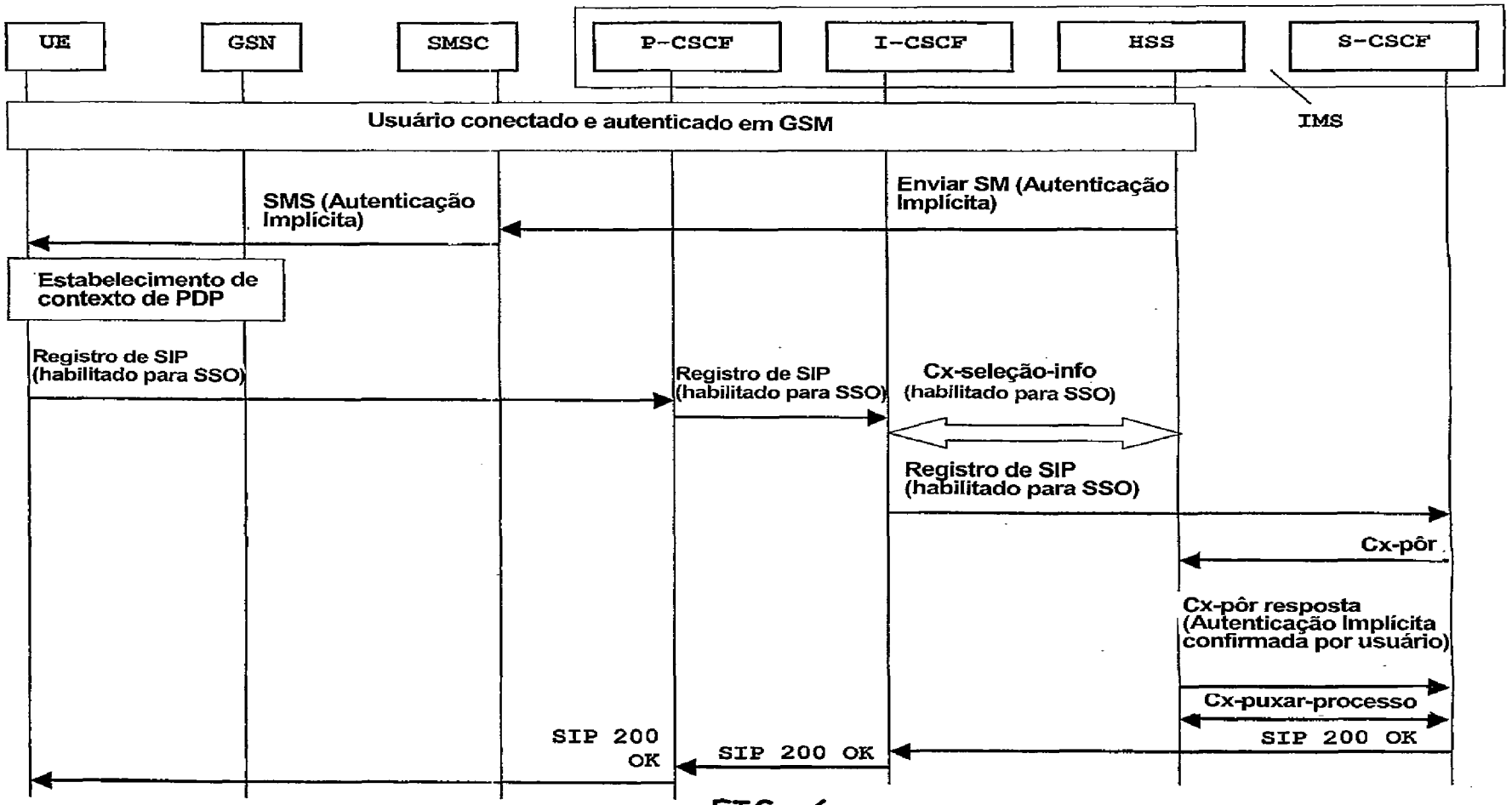
UE
GSN
SMSC
P-CSCF
I-CSCF
HSS
S-CSCF
IMS
Usuário conectado e autenticado em GSM
SMS (Autenticação Implícita)
Enviar SM (Autenticação Implícita)
Estabelecimento de contexto de PDP
Registro de SIP (habilitado para SSO)
Registro de SIP (habilitado para SSO)
Cx-seleção-info (habilitado para SSO)
Registro de SIP (habilitado para SSO)
Cx-pôr
Cx-pôr resposta (Autenticação Implícita confirmada por usuário)
Cx-puxar-processo
SIP 200 OK
SIP 200 OK
SIP 200 OK

FIG.-6-

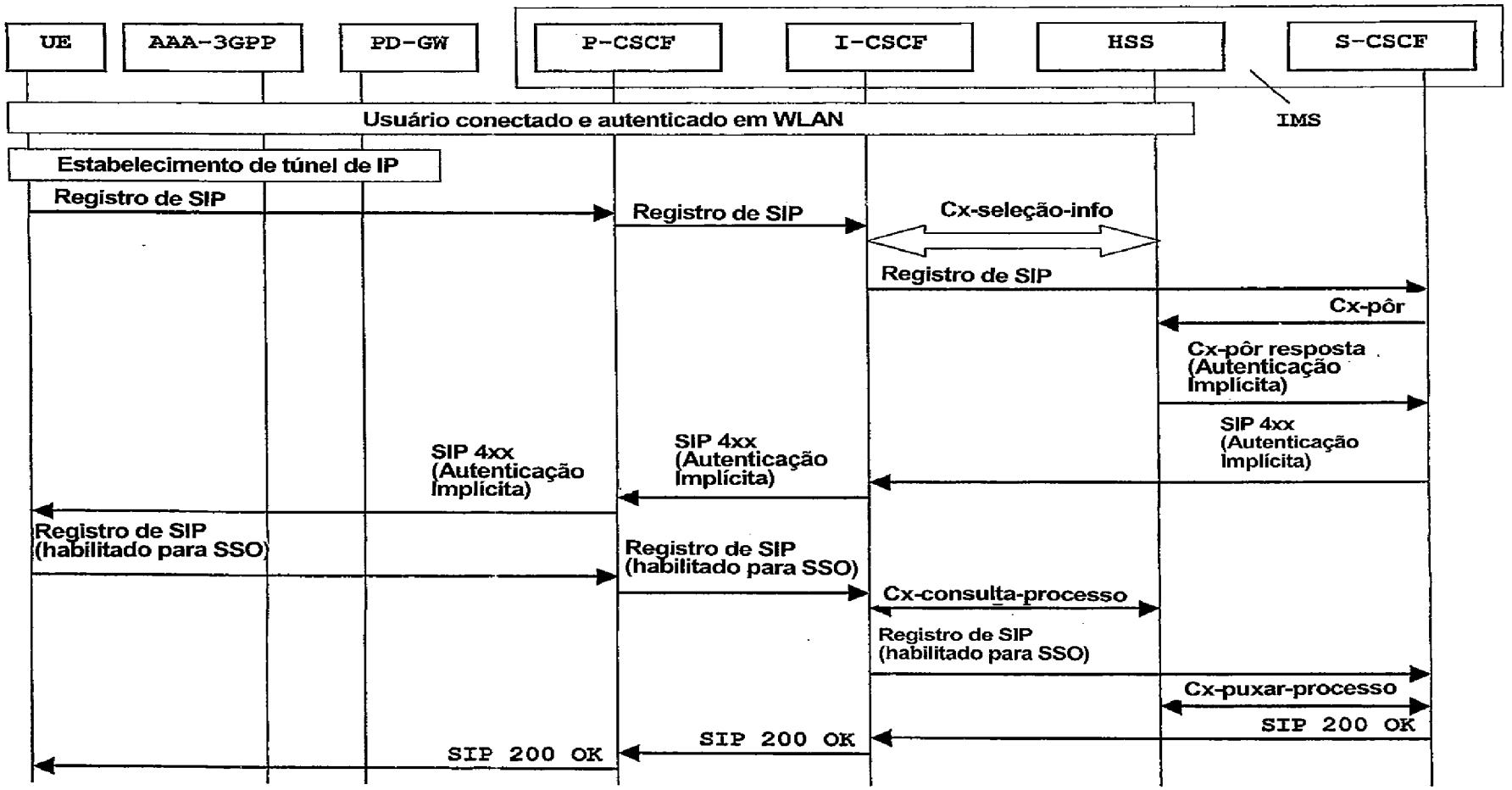
UE
AAA-3GPP
PD-GW
P-CSCF
I-CSCF
HSS
S-CSCF
IMS
Usuário conectado e autenticado em WLAN
Estabelecimento de túnel de IP
Registro de SIP
Registro de SIP
Cx-seleção-info
Registro de SIP
Cx-pôr
Cx-pôr resposta (Autenticação Implícita)
SIP 4xx (Autenticação Implícita)
SIP 4xx (Autenticação Implícita)
SIP 4xx (Autenticação Implícita)
Registro de SIP (habilitado para SSO)
Registro de SIP (habilitado para SSO)
Cx-consulta-processo
Registro de SIP (habilitado para SSO)
Cx-puxar-processo
SIP 200 OK
SIP 200 OK
SIP 200 OK

FIG.-7-

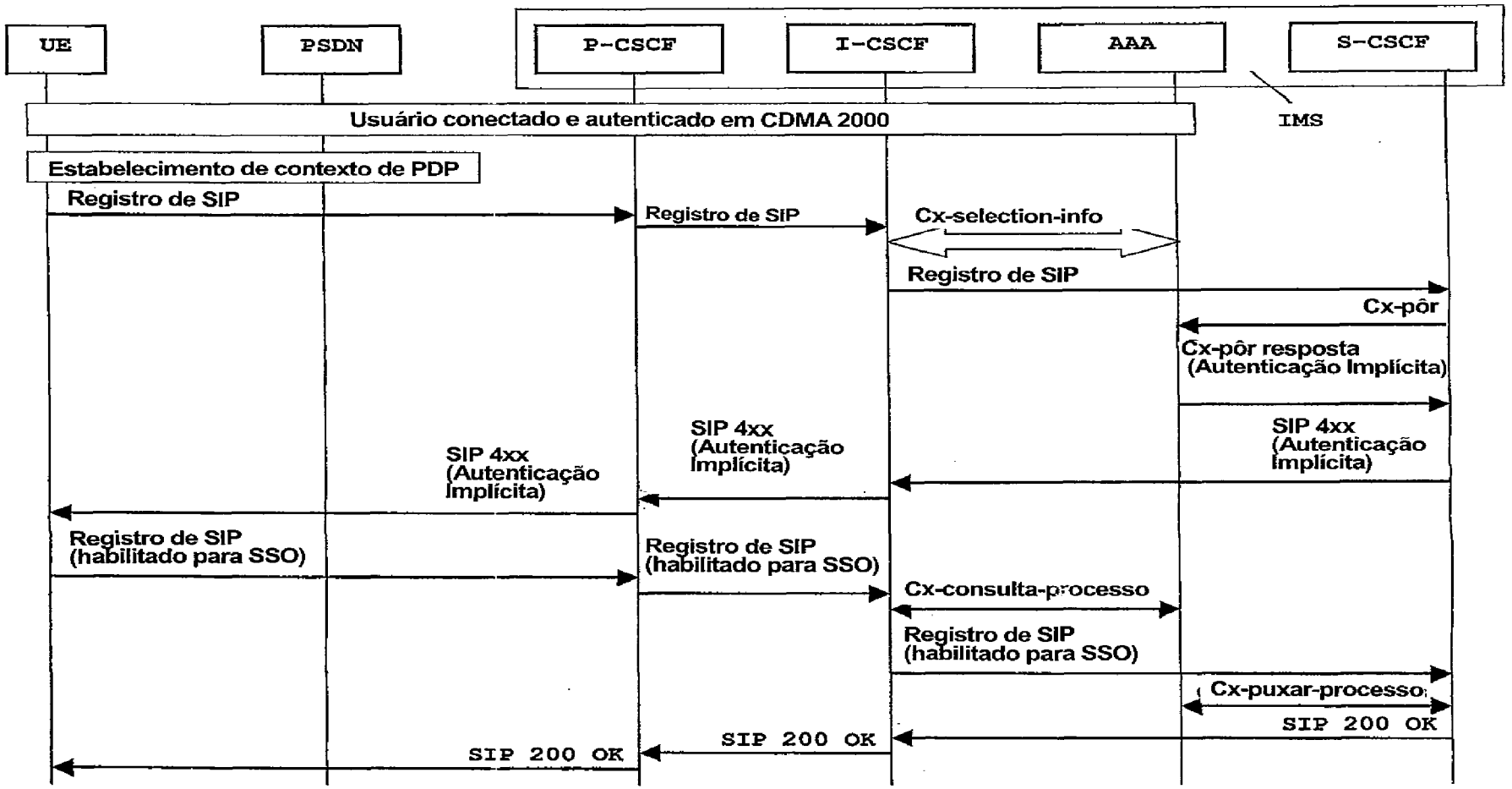
UE
PSDN
P-CSCF
I-CSCF
AAA
S-CSCF
IMS
Usuário conectado e autenticado em CDMA 2000
Estabelecimento de contexto de PDP
Registro de SIP
Registro de SIP
Cx-selection-info
Registro de SIP
Cx-pôr
Cx-pôr resposta
(Autenticação Implícita)
SIP 4xx
(Autenticação
Implícita)
SIP 4xx
(Autenticação
Implícita)
SIP 4xx
(Autenticação
Implícita)
Registro de SIP
(habilitado para SSO)
Registro de SIP
(habilitado para SSO)
Cx-consulta-processo
Registro de SIP
(habilitado para SSO)
Cx-puxar-processo
SIP 200 OK
SIP 200 OK
SIP 200 OK

FIG.-8-

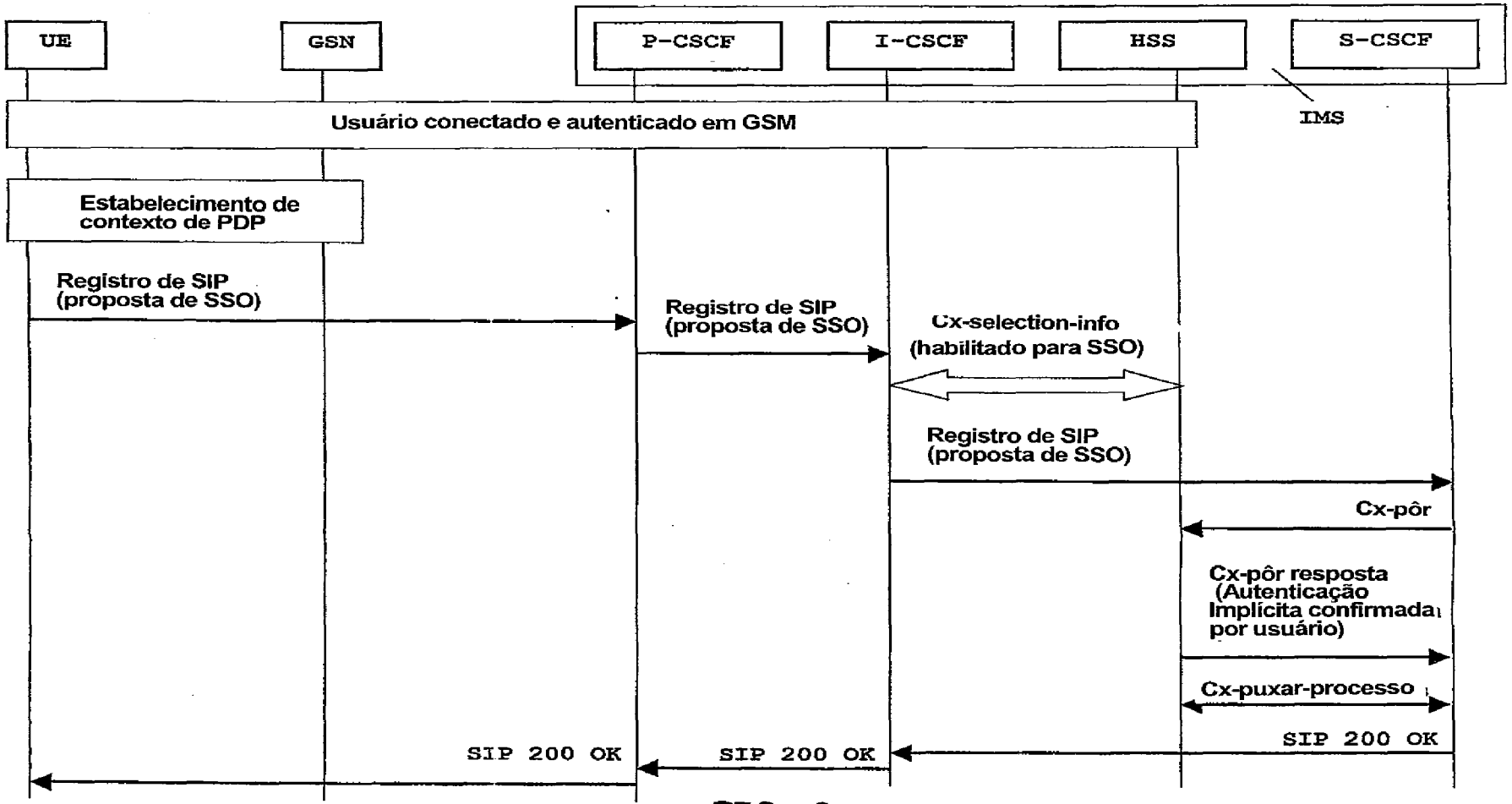
UE
GSN
P-CSCF
I-CSCF
HSS
S-CSCF
IMS
Usuário conectado e autenticado em GSM
Estabelecimento de contexto de PDP
Registro de SIP (proposta de SSO)
Registro de SIP (proposta de SSO)
Cx-selection-info (habilitado para SSO)
Registro de SIP (proposta de SSO)
Cx-pôr
Cx-pôr resposta (Autenticação Implícita confirmada por usuário)
Cx-puxar-processo
SIP 200 OK
SIP 200 OK
SIP 200 OK

FIG.-9-