



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

(11) PI 0612687-1 B1



(22) Data do Depósito: 05/07/2006

(45) Data de Concessão: 14/05/2019

(54) Título: MÉTODO DE AUTENTICAÇÃO EM SUBSISTEMA MULTIMÍDIA IP

(51) Int.Cl.: H04L 29/06.

(52) CPC: H04L 63/08; H04L 63/205; H04L 65/1016.

(30) Prioridade Unionista: 05/07/2005 CN 200510082907.8; 18/10/2005 CN 200510109162.X; 19/08/2005 CN 200510093216.8.

(73) Titular(es): HUAWEI TECHNOLOGIES CO., LTD..

(72) Inventor(es): JUN YAN; YING WANG; CHENG DONG HE.

(86) Pedido PCT: PCT CN2006001569 de 05/07/2006

(87) Publicação PCT: WO 2007/003140 de 11/01/2007

(85) Data do Início da Fase Nacional: 07/01/2008

(57) Resumo: MÉTODO DE AUTENTICAÇÃO EM SUBSISTEMA MULTIMÍDIA IP. A presente invenção refere-se a um método de autenticação em IMS que inclui: após receber a mensagem de registro do UE, localizar, através da P-CSCF, uma CLF de acordo com informação contida na mensagem de Registro e uma relação pré-configurada; inquirir, através da P-CSCF, a CLF sobre informação de conexão NASS do UE para obter um resultado inquirido, e enviar a mensagem de registro transportando o resultado inquirido para uma I-CSCF; encaminhar, através da I-CSCF, a mensagem de Registro transmitido o resultado inquirido para uma S-CSCF designada por uma UPSF ou um HSS; autenticar o UE e enviar um resultado de autenticação para o UE através da S-CSCF. Uma modalidade da presente invenção, a UPSF ou o HSS na camada de serviço determina o mecanismo de autenticação do usuário, e a S-CSCF implementa a autenticação, o que é mais razoável. A presente invenção também proporciona combinações de NBA com outros mecanismo de autenticação, o que garante a autenticação do usuário depois que a autenticação NBA falha.

Relatório Descritivo da Patente de Invenção para
"MÉTODO DE AUTENTICAÇÃO EM SUBSISTEMA MULTIMÍDIA IP".

Campo da Invenção

[001] A presente invenção refere-se a um Subsistema de Multimídia de IP (IMS) e, mais particularmente, a um método de autenticação no IMS.

Antecedentes da Invenção

[002] Uma Rede de Próxima Geração (NGN) bem-conhecida como uma rede móvel, geralmente pode ser dividida em uma rede de acesso e uma rede de serviço. Um usuário pode acessar uma rede de IP através da rede de acesso provida em uma operadora de rede de acesso e, então, desfrutar de diferentes serviços, tais como voz, vídeo, mídia de fluxo, etc., através de redes de serviço providas por uma ou múltiplas operadoras de rede de serviço.

[003] Quando a rede de acesso e a rede de serviço pertencem a operadoras diferentes, as autenticações de uso na rede de acesso e na rede de serviço são independentes. Em um cenário como esse, o usuário precisa duas vezes de autenticações antes de desfrutar do serviço. Uma autenticação é na camada de acesso; após a autenticação na camada de acesso ser bem-sucedida, o usuário é capaz de acessar a rede NGN. A outra autenticação é na camada de serviço; e, após a autenticação na camada de serviço ser bem-sucedida, o usuário é capaz de desfrutar dos serviços providos pela rede de serviço.

[004] Quando a rede de serviço e a rede de acesso pertencem a mesma operadora, ou quando existe uma cooperação entre a operadora de rede de acesso e a operadora de rede de serviço, a operadora de rede de serviço pode vincular a autenticação na camada de serviço àquela na camada de acesso, sob alguns cenários de ligação de rede. Em outras palavras, o usuário é considerado como

sendo legal após a autenticação na camada de acesso ser bem-sucedida, e a autenticação na camada de serviço não é mais requerida.

[005] Na camada de acesso de IMS, um esquema de Autenticação e Acordo de Chave (AKA) é empregado, usualmente, para a autenticação do UE na camada de serviço de IMS.

[006] Com referência à Figura 1, o esquema de AKA de IMS inclui:

[007] Bloco s101: um Equipamento de Usuário (UE) envia uma mensagem Register (Registrar) para uma Função de Controle de Sessão de Chamada de Proxy (P-CSCF).

[008] Bloco s102: A P-CSCF, atuando como um servidor de proxy de Protocolo Inicial de Sessão (SIP) encaminha a mensagem Register do UE para uma CSCF de Interrogação (I-CSCF).

[009] Bloco s103: A I-CSCF interage com um Servidor de Assinante Doméstico (HSS) através de uma mensagem Cx-Selection-Info para a seleção de uma CSCF de Serviço (S-CSCF), isto é, a I-CSCF envia uma requisição para o HSS para buscar um perfil de usuário no HSS para selecionar a S-CSCF para processamento da mensagem Register.

[0010] Bloco s104: A I-CSCF encaminha a mensagem Register do UE para a S-CSCF selecionada no Bloco s103.

[0011] Bloco s105: A S-CSCF envia Mensagem Cx-Put para o HSS para atualização da indicação de S-CSCF no HSS e notificar o HSS que ele foi atribuído para servir a este usuário.

[0012] Bloco s106: A S-CSCF envia uma Mensagem AV-Req para o HSS requisitando um vetor de autenticação do usuário.

[0013] Bloco s107: O HSS retorna uma mensagem AV-Req-Resp para a S-CSCF portando o vetor de autenticação do usuário.

[0014] Bloco s108: A S-CSCF determina que o UE precisa ser

autenticado de acordo com o vetor de autenticação recebido no Bloco s107 e a mensagem Register do UE, então, a S-CSCF envia uma mensagem 4xx Auth_Challenge contendo uma informação relevante de autenticação indicando que o UE precisa ser autenticado para a I-CSCF. O 4xx denota um tipo de erro e o xx significa um número em 00~99.

[0015] Bloco s109: A I-CSCF encaminha a mensagem 4xx Auth_Challenge para a P-CSCF.

[0016] Bloco s110: A P-CSCF encaminha a mensagem 4xx Auth_Challenge para o UE.

[0017] Bloco s111: após o recebimento da mensagem 4xx Auth_Challenge, o UE envia uma outra mensagem Register para a P-CSCF, neste momento, a mensagem Register porta um parâmetro de autenticação.

[0018] Bloco s112: A P-CSCF encaminha a mensagem Register do UE para a I-CSCF.

[0019] Bloco s113: após receber a mensagem Register, a I-CSCF envia uma mensagem Cx-Query para o HSS para determinar a S-CSCF para processamento da mensagem Register, i.e., a I-CSCF consulta o HSS sobre a S-CSCF a qual foi atribuída para servir a esse usuário. O HSS retorna o nome de S-CSCF o qual foi previamente selecionado para a I-CSCF de acordo com a informação de indicação de S-CSCF armazenada no HSS.

[0020] Bloco s114: A I-CSCF encaminha a mensagem Register para a S-CSCF determinada no Bloco s113.

[0021] Bloco s115: A S-CSCF envia uma Mensagem Cx-Put para o HSS para atualização da informação de indicação de S-CSCF no HSS e notificar o HSS que ele foi atribuído para servir a este usuário.

[0022] Bloco s116: A S-CSCF transfere (via download) um perfil de usuário a partir do HSS através de uma mensagem Cx-Pull.

[0023] Bloco s117: A S-CSCF autentica o UE de acordo com o perfil de usuário e o parâmetro de autenticação na mensagem Register do UE. Caso a autenticação seja bem-sucedida, a S-CSCF envia uma mensagem 2xx Auth_OK para a I-CSCF indicando que o registro é bem-sucedido, onde 2xx indica que a mensagem é relevante para sucesso, e o xx é um número em 00~99. Caso a autenticação falhe, a S-CSCF envia uma mensagem de falha de autenticação indicando que a autenticação falhou para a I-CSCF.

[0024] Bloco s118: caso a autenticação seja bem-sucedida, a I-CSCF encaminha a mensagem 2xx Auth_OK para a P-CSCF. Caso a autenticação falhe, a I-CSCF encaminha a mensagem de falha de autenticação para a P-CSCF.

[0025] Bloco s119: caso a autenticação seja bem-sucedida, a P-CSCF encaminha a mensagem 2xx Auth_OK para o UE. Caso a autenticação falhe, a P-CSCF encaminha a mensagem de falha de autenticação para o UE.

[0026] A France Telecom propôs um esquema de Autenticação em Feixe (NBA) de Subsistema de Anexação de Rede (NASS) para a implementação de uma autenticação em feixe IMS-NASS nos Serviços de Telecomunicações e Internet de Convergência e Protocolos para Ligação de Rede Avançada (TISPAN) #6bis. No esquema NBA, uma Função de Localização de Conexão (CLF) no NASS mantém uma indicação em feixe e uma relação correspondente entre um endereço de IP do UE e a informação de associação do UE na rede de acesso. Cada conexão do usuário mantém um pedaço de informação de associação.

[0027] Com referência à Figura 2, o esquema de NBA inclui:

[0028] Bloco s201: O UE envia uma mensagem Register para a P-CSCF.

[0029] Bloco s202: A P-CSCF consulta a CLF sobre uma

informação de anexação do UE de acordo com um endereço de IP de fonte da mensagem Register, onde a informação de anexação contém a informação de associação do UE e a indicação em feixe.

[0030] Bloco s203: A P-CSCF compara a informação de associação e uma Identidade Privada de Multimídia de (IMPI) em um cabeçalho de autenticação da mensagem Register. Caso a informação de associação seja consistente com a IMPI, significa que a autenticação na camada de serviço de IMS é bem-sucedida, prossegue-se para o Bloco s205; caso contrário, significa que a autenticação na camada de serviço de IMS falhou, prossegue-se para o Bloco s204 para enviar uma 403 Forbidden (403 Proibido) para o UE.

[0031] Bloco s205: A P-CSCF encaminha a mensagem Register portando um indicador indicando se a autenticação é bem-sucedida para a I-CSCF.

[0032] Bloco s206: A I-CSCF interage com o HSS através de uma mensagem Cx-Selection-Info para selecionar uma S-CSCF correspondente, isto é, a I-CSCF envia uma requisição para o HSS para buscar um perfil de usuário no HSS para selecionar a S-CSCF para processamento da mensagem Register.

[0033] Bloco s207: A I-CSCF encaminha a mensagem Register para a S-CSCF selecionada no Bloco s206.

[0034] Bloco s208: após confirmar que o usuário se registrou de forma bem-sucedida, sem requisitar o HSS para o vetor de autenticação do usuário, a S-CSCF envia uma Mensagem Cx-Put para o HSS para a atualização da informação de indicação de S-CSCF no HSS e notificar o HSS que ele foi atribuído para servir a este usuário, e transfere (via download) o perfil de usuário a partir do HSS através de uma mensagem Cx-Pull.

[0035] Bloco s209: A S-CSCF retorna a mensagem 2xx Auth_OK

para a I-CSCF indicando que a autenticação foi bem-sucedida.

[0036] Bloco s210: A I-CSCF encaminha a mensagem 2xx Auth_OK para a P-CSCF.

[0037] Bloco s211: A P-CSCF encaminha a mensagem 2xx Auth_OK para o UE.

[0038] No esquema acima, é requerido que a IMPI contida na mensagem Register seja consistente com a informação de associação, isto é, a IMPI na camada de serviço e a informação de associação na camada de acesso são da mesma identidade. Contudo, a operadora de rede de serviço usualmente não é a mesma que a operadora de rede de acesso. Assim, a exigência de uso da mesma identidade para a operadora de rede de serviço e a operadora de rede de acesso restringe a flexibilidade de operações de rede. Mais ainda, não é razoável que a indicação em feixe seja salva no NASS. O método razoável deve ser que a indicação em feixe seja salva na camada de serviço (por exemplo, no HSS), enquanto a camada de acesso é apenas responsável pela provisão de uma informação relevante. Ainda, também não é razoável que a P-CSCF implemente a autenticação. É mais razoável que a S-CSCF em uma rede doméstica implemente a autenticação na camada de serviço, e a P-CSCF apenas proveja uma informação relevante para a autenticação.

[0039] Ainda, quando o estado do usuário muda, por exemplo, o usuário pode empregar terminais diferentes quando em localizações diferentes, a autenticação adotando a autenticação de IMS em feixe com NASS, o qual é configurado como um mecanismo de autenticação padrão, falhará. Assim, a qualidade de serviço é diminuída. Portanto, um segundo mecanismo de autenticação pré-configurado no HSS é requerido para a autenticação do usuário. Contudo, não há tais soluções na técnica relacionada.

Sumário da Invenção

[0040] As modalidades da presente invenção provêem um método de autenticação em um Subsistema de Multimídia de IP (IMS) no qual um mecanismo de autenticação é determinado por uma camada de serviço, de modo a se garantir uma compatibilidade retrógrada e uma sustentabilidade da autenticação.

[0041] De acordo com um aspecto da presente invenção, o método de autenticação no IMS inclui:

após o recebimento de uma mensagem Register de um Equipamento de Usuário (UE), a localização por uma Função de Controle de Sessão de Chamada de Proxy (P-CSCF) de uma Função de Localização de Conexão (CLF) de acordo com a informação contida na mensagem Register e uma relação correspondente pré-configurada entre a informação contida na mensagem Register e a CLF;

consulta, pela P-CSCF, à CLF sobre uma informação de Subsistema de Anexação de Rede (NASS) do UE em uma rede de acesso para a obtenção de um resultado de consulta, e envio da mensagem Register portando o resultado de consulta para uma Função de Controle de Sessão de Chamada de Interrogação (I-CSCF);

encaminhamento, pela I-CSCF, da mensagem Register portando o resultado de consulta para uma Função de Controle de Sessão de Chamada de Serviço (S-CSCF);

autenticação, pela S-CSCF, do UE de acordo com um mecanismo de autenticação obtido a partir de uma Função de Serviço de Perfil de Usuário (UPSF) ou de um Servidor de Assinante Doméstico (HSS), e envio de um resultado de autenticação para o UE.

[0042] Pode ser visto a partir da solução técnica acima que, no método provido pelas modalidades da presente invenção, a UPSF ou o HSS determina o mecanismo de autenticação do usuário e a S-

CSCF implementa a autenticação, a qual é de acordo com o princípio de implementação da autenticação na camada de serviço e pode ser mais razoável. Comparada com a técnica relacionada, a solução técnica provida pelas modalidades da presente invenção requer pouca modificação no procedimento de AKA de IMS existente, desse modo sendo mais aplicável e flexível e mais compatível com o AKA de IMS existente.

[0043] Adicionalmente, a UPSF ou o HSS pré-armazena o mecanismo de autenticação do usuário. Assim, ao usuário podem ser providos tipos diferentes de combinações de mecanismos de autenticação.

Breve Descrição dos Desenhos

[0044] A Figura 1 é um fluxo de mensagem que ilustra um esquema de AKA de IMS de acordo com a técnica relacionada.

[0045] A Figura 2 é um fluxo de mensagem que ilustra o esquema de NBA de acordo com a técnica relacionada.

[0046] As Figuras 3a e 3b são fluxos de mensagem de uma autenticação de acordo com uma primeira modalidade da presente invenção.

[0047] As Figuras 4a e 4b são fluxos de mensagem de uma autenticação de acordo com uma segunda modalidade da presente invenção.

[0048] As Figuras 5a e 5b são fluxos de mensagem de uma autenticação de acordo com uma terceira modalidade da presente invenção.

[0049] As Figuras 6a e 6b são fluxos de mensagem de uma autenticação de acordo com uma quarta modalidade da presente invenção.

[0050] As Figuras 7a e 7b são fluxos de mensagem de uma autenticação de acordo com uma quinta modalidade da presente invenção.

[0051] A Figura 8 é um fluxo de mensagem que ilustra uma autenticação HTTP DIGEST.

[0052] As Figuras 9a e 9b são fluxos de mensagem de uma autenticação de acordo com uma sexta modalidade da presente invenção.

[0053] As Figuras 10a e 10b são fluxos de mensagem de uma autenticação de acordo com uma sétima modalidade da presente invenção.

[0054] As Figuras 11a e 11b são fluxos de mensagem de uma autenticação de acordo com uma oitava modalidade da presente invenção.

[0055] As Figuras 12a e 12b são fluxos de mensagem de uma autenticação de acordo com uma nona modalidade da presente invenção.

Descrição Detalhada da Invenção

[0056] De modo a tornar mais claros a solução técnica e os méritos da presente invenção, uma descrição detalhada da presente invenção é dada, a partir deste ponto, com referência aos desenhos associados e às modalidades preferidas.

[0057] Uma primeira modalidade da presente invenção é baseada no esquema de AKA de IMS provê um método de autenticação de IMS em feixe com NASS. Na primeira modalidade, a UPSF ou o HSS pré-armazena um perfil de usuário indicando se o mecanismo de autenticação do usuário é autenticação de IMS em feixe com NASS.

[0058] Com referência às Figuras 3a e 3b, o método da primeira modalidade inclui:

[0059] Bloco **101**: O UE envia uma mensagem Register para a P-

CSCF.

[0060] Bloco **102**: A P-CSCF encaminha a mensagem Register do UE para a I-CSCF.

[0061] Bloco **103**: A I-CSCF interage com a UPSF ou o HSS através de uma mensagem Cx-Selection-Info para a seleção de uma S-CSCF correspondente, isto é, a I-CSCF envia uma requisição para a UPSF ou o HSS para selecionar a S-CSCF para o processamento da mensagem Register pela análise do perfil de usuário na UPSF ou no HSS.

[0062] Bloco **104**: A I-CSCF encaminha a mensagem Register do UE para a S-CSCF selecionada no Bloco **103**.

[0063] Bloco **105**: A S-CSCF envia uma mensagem Cx-Put para o HSS para a atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[0064] Bloco **106**: A S-CSCF envia uma mensagem AV-Req para a UPSF ou o HSS requisitando dados de autenticação do usuário.

[0065] Bloco **107**: A UPSF ou o HSS checa o perfil de usuário para obter o mecanismo de autenticação o qual indica que a autenticação de IMS é em feixe com NASS.

[0066] Bloco **108**: A UPSF ou o HSS retorna uma mensagem AV-Req-Resp para a S-CSCF. Diferentemente dos dados de autenticação enviados na técnica relacionada, uma indicação do mecanismo de autenticação é enviada em conjunto com os dados de autenticação para a S-CSCF.

[0067] Bloco **109**: A S-CSCF determina que o mecanismo de autenticação do usuário é a autenticação de IMS em feixe com NASS de acordo com a indicação do mecanismo de autenticação e, então, envia para a I-CSCF uma mensagem 4xx Auth_Challenge portando a indicação do mecanismo de autenticação, isto é, uma indicação em

feixe, no cabeçalho de autenticação da mensagem 4xx Auth_Challenge (por exemplo, WWW-Authenticate (Autenticação WWW)) para indicar que o mecanismo de autenticação do usuário é a autenticação de IMS em feixe com NASS.

[0068] Bloco **110**: A I-CSCF encaminha a mensagem 4xx Auth_Challenge portando a indicação em feixe para a P-CSCF.

[0069] Bloco **111**: Após receber a mensagem 4xx Auth_Challenge, a P-CSCF determina que um parâmetro “algorithm” (de algoritmo) em um cabeçalho WWW-Authenticate da mensagem 4xx Auth_Challenge indica que o mecanismo de autenticação do usuário é a autenticação de IMS em feixe com NASS. Portanto, a P-CSCF não precisa estabelecer uma associação de segurança com o UE. A P-CSCF encaminha a mensagem 4xx Auth_Challenge portando a indicação em feixe, mas nenhum cabeçalho de Security-Server (Servidor de Segurança) para o UE.

[0070] Bloco **112**: Após receber a mensagem 4xx Auth_Challenge, o UE determina que o parâmetro “algorithm” no cabeçalho WWW-Authenticate da mensagem 4xx Auth_Challenge indica que o mecanismo de autenticação do usuário é a autenticação de IMS em feixe com NASS. Portanto, o UE não precisa estabelecer uma associação de segurança com a P-CSCF. O UE envia para a P-CSCF uma outra mensagem Register portando uma identidade de rede de acesso e uma informação de associação do UE na rede de acesso.

[0071] Bloco **113**: A P-CSCF localiza a CLF de acordo com a identidade de rede de acesso na mensagem Register e a relação correspondente pré-regulada entre a CLF e a identidade de rede de acesso.

[0072] Bloco **114**: A P-CSCF consulta a CLF localizada no bloco 113 sobre a informação de anexação do UE na camada de acesso de acordo com a informação de associação na mensagem Register.

Diferentemente daquilo da técnica relacionada, a CLF pré-armazena o registro de dados da informação de anexação correspondente à informação de associação, onde a informação de anexação inclui uma informação de endereço de IP, uma informação de localização, etc., mas não uma indicação em feixe. Se não houver um registro de dados na informação de anexação correspondente à informação de associação, a CLF retornará uma mensagem de falha de consulta para a P-CSCF.

[0073] Bloco **115**: A P-CSCF envia a mensagem Register portando o resultado de consulta do bloco 114 e o endereço de IP de origem da mensagem Register recebida pela P-CSCF para a I-CSCF; se a consulta no bloco **114** for bem-sucedida, a P-CSCF enviará a informação de anexação consultada para a I-CSCF; caso contrário, a P-CSCF reportará uma mensagem de falha de consulta para a I-CSCF.

[0074] Bloco **116**: A I-CSCF envia uma mensagem Cx-Query para a UPSF ou o HSS para determinar a S-CSCF para processamento da mensagem Register, isto é, a I-CSCF consulta a UPSF ou o HSS sobre a S-CSCF a qual foi atribuída para servir a este usuário. A UPSF ou o HSS retorna o nome de S-CSCF, o qual foi previamente selecionado no bloco **103** para a I-CSCF de acordo com a informação de indicação de S-CSCF armazenada no HSS.

[0075] Bloco **117**: A I-CSCF encaminha a mensagem Register portando o resultado de consulta e o endereço de IP de origem da mensagem Register recebida pela P-CSCF para a S-CSCF determinada no Bloco **116**. Se a consulta for bem-sucedida, o resultado de consulta será a informação de anexação; caso contrário, o resultado de consulta será a mensagem de falha de consulta reportada.

[0076] Bloco **118**: Caso o resultado de consulta seja a informação

de anexação, a S-CSCF compara o endereço de IP de origem da mensagem Register recebida pela P-CSCF com o endereço de IP na informação de anexação consultada a partir da CLF. Caso o endereço de IP de origem da mensagem Register recebida pela P-CSCF seja consistente com o endereço de IP na informação de anexação consultada a partir da CLF, isto significa que a autenticação é bem-sucedida, prossegue-se para o Bloco **119**, isto é, envia-se uma mensagem de sucesso de autenticação para o UE; caso contrário, isto significa que a autenticação falhou, prossegue-se para o Bloco **131**, isto é, envia-se uma mensagem de falha de autenticação para o UE.

[0077] Caso o resultado de consulta seja a mensagem de falha de consulta reportada, isto também significa que a autenticação falhou, prossegue-se para o Bloco **131**, isto é, envia-se a mensagem de falha de autenticação para o UE.

[0078] Bloco **119**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[0079] Bloco **120**: A S-CSCF transfere (via download) o perfil de usuário a partir da UPSF ou do HSS através de uma mensagem Cx-Pull.

[0080] Bloco **121**: A S-CSCF envia uma mensagem 2xx Auth_OK para a I-CSCF indicando que a autenticação foi bem-sucedida.

[0081] Bloco **122**: A I-CSCF encaminha a mensagem 2xx Auth_OK para a P-CSCF.

[0082] Bloco **123**: A P-CSCF encaminha a mensagem 2xx Auth_OK para o UE.

[0083] Bloco **131**, conforme mostrado na Figura 3b: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e

notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[0084] Bloco **132**: A S-CSCF transfere (via download) o perfil de usuário a partir da UPSF ou do HSS através de uma mensagem Cx-Pull.

[0085] Bloco **133**: A S-CSCF envia uma mensagem de falha de autenticação para a I-CSCF para indicar que a autenticação falhou.

[0086] Bloco **134**: A I-CSCF encaminha uma mensagem de falha de autenticação para a P-CSCF.

[0087] Bloco **135**: A P-CSCF encaminha uma mensagem de falha de autenticação para o UE.

[0088] Quando a operadora de rede é a mesma que a operadora de rede de serviço, uma vez que a informação de associação e a IMPI são as mesmas, o NASS não emite a identidade de rede de acesso e a informação de associação para o UE. Neste momento, uma segunda modalidade pode ser adotada, conforme mostrado nas Figura 4a e 4b. A segunda modalidade é uma simplificação da primeira modalidade. Na segunda modalidade, o endereço de IP de origem da mensagem Register pode ser usado para a localização da CLF, e a IMPI na camada de serviço de IMS pode ser usada para se consultar a informação de anexação do UE na camada de acesso. De modo similar à primeira modalidade, a UPSF ou o HSS também pré-armazena o perfil de usuário indicando se o mecanismo de autenticação do usuário é uma autenticação de IMS em feixe com NASS.

[0089] Com referência às Figuras 4a e 4b, o método de autenticação de acordo com a segunda modalidade da presente invenção inclui:

[0090] Os Blocos **201 a 211** são respectivamente os mesmos que os Blocos **101 a 111** na primeira modalidade.

[0091] Bloco **201**: O UE envia uma mensagem Register para a P-CSCF.

[0092] Bloco **202**: A P-CSCF encaminha a mensagem Register do UE para a I-CSCF.

[0093] Bloco **203**: A I-CSCF interage com a UPSF ou o HSS através de uma mensagem Cx-Selection-Info para selecionar a S-CSCF correspondente, isto é, I-CSCF envia uma requisição para a UPSF ou o HSS para buscar o perfil de usuário na UPSF ou no HSS para selecionar qual S-CSCF processará a mensagem Register.

[0094] Bloco **204**: A I-CSCF encaminha a mensagem Register do UE para a S-CSCF selecionada no Bloco 203.

[0095] Bloco **205**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[0096] Bloco **206**: A S-CSCF envia uma mensagem AV-Req para a UPSF ou o HSS requisitando os dados de autenticação do usuário.

[0097] Bloco **207**: A UPSF ou o HSS checa o perfil de usuário para obter o mecanismo de autenticação o qual indica que a autenticação de IMS é em feixe com NASS.

[0098] Bloco **208**: A UPSF ou o HSS retorna uma mensagem AV-Req-Resp para a S-CSCF. Diferentemente dos dados de autenticação enviados na técnica relacionada, a indicação do mecanismo de autenticação é enviada em conjunto com os dados de autenticação para a S-CSCF.

[0099] Bloco **209**: A S-CSCF determina que o mecanismo de autenticação do usuário é a autenticação de IMS em feixe com NASS de acordo com a indicação do mecanismo de autenticação obtida no Bloco 208, e, então, envia para a I-CSCF uma mensagem 4xx Auth_Challenge portando a indicação do mecanismo de autenticação,

isto é, a indicação em feixe, no cabeçalho de autenticação da mensagem 4xx Auth_Challenge para indicar que o mecanismo de autenticação do usuário é a autenticação de IMS em feixe com NASS.

[00100] Bloco **210**: A I-CSCF encaminha a mensagem 4xx Auth_Challenge portando a indicação em feixe para a P-CSCF.

[00101] Bloco **211**: Após receber a mensagem 4xx Auth_Challenge, a P-CSCF determina que o parâmetro “algorithm” no cabeçalho WWW-Authenticate da mensagem 4xx Auth_Challenge indica que o mecanismo de autenticação do usuário é autenticação de IMS em feixe com NASS. Portanto, a P-CSCF não precisa estabelecer uma associação de segurança com o UE. A P-CSCF encaminha a mensagem 4xx Auth_Challenge portando a indicação em feixe, mas nenhum cabeçalho de Security-Server para o UE.

[00102] Bloco **212**: Após receber a mensagem 4xx Auth_Challenge, o UE determina que o parâmetro “algorithm” no cabeçalho WWW-Authenticate da 4xx Auth_Challenge indica que o mecanismo de autenticação do usuário é autenticação de IMS em feixe com NASS. Portanto, o UE não precisa estabelecer uma associação de segurança com a P-CSCF. O UE envia uma mensagem Register para a P-CSCF de novo. Diferentemente daquilo na primeira modalidade, a mensagem Register não precisa portar a identidade de rede de acesso e a informação de associação; ao invés disso, a mensagem Register porta a IMPI no cabeçalho de autenticação.

[00103] Bloco **213**: A P-CSCF localiza a CLF de acordo com o endereço de IP de origem da mensagem Register e a pré-regulagem correspondente à relação entre o endereço de IP de origem e a CLF.

[00104] Bloco **214**: A P-CSCF consulta a CLF sobre a informação de anexação do UE na camada de acesso de acordo com a IMPI portada no cabeçalho de autenticação da mensagem Register. A CLF pré-armazena o registro de dados da informação de anexação

correspondente à IMPI. A informação de anexação inclui a informação de endereço de IP, uma informação de localização, etc., mas nenhuma informação em feixe na técnica relacionada. Se a CLF não tiver um registro de dados correspondente à IMPI, a CLF retornará uma mensagem de falha de consulta para a P-CSCF.

[00105] Os Blocos **215** a **223** são respectivamente os mesmos que os Blocos **115** a **123** na primeira modalidade.

[00106] Bloco **215**: A P-CSCF envia a mensagem Register para a I-CSCF com o resultado de consulta do bloco **214** e o endereço de IP de origem da mensagem Register recebida pela P-CSCF; se a consulta no bloco **214** for bem-sucedida, a P-CSCF enviará a informação de anexação consultada para a I-CSCF; caso contrário, a P-CSCF reportará uma mensagem de falha de consulta para a I-CSCF.

[00107] Bloco **216**: A I-CSCF envia uma mensagem Cx-Query para a UPSF ou o HSS para determinar a S-CSCF para processamento da mensagem Register, isto é, a I-CSCF consulta a UPSF ou o HSS sobre a S-CSCF a qual foi atribuída para servir a este usuário. A UPSF ou o HSS retorna o nome de S-CSCF, o qual foi previamente selecionado no bloco **203** para a I-CSCF de acordo com a informação de indicação de S-CSCF armazenada no HSS.

[00108] Bloco **217**: A I-CSCF encaminha a mensagem Register portando o resultado de consulta e o endereço de IP de origem da mensagem Register recebida pela P-CSCF para a S-CSCF determinada no Bloco **216**. Caso a consulta seja bem-sucedida, o resultado de consulta é a informação de anexação obtida; caso contrário, o resultado de consulta é a mensagem de falha de consulta reportada.

[00109] Bloco **218**: se o resultado de consulta for a informação de anexação consultada, a S-CSCF compara o endereço de IP de origem

da mensagem Register recebida pela P-CSCF com o endereço de IP na informação de anexação consultada a partir da CLF. Caso o endereço de IP de origem da mensagem Register recebida pela P-CSCF seja consistente com o endereço de IP na informação de anexação consultada a partir da CLF, isto significa que a autenticação é bem-sucedida, prossegue-se para o Bloco **219**, isto é, envia-se uma mensagem de sucesso de autenticação para o UE; caso contrário, isto significa que a autenticação falhou, prossegue-se para o Bloco **231**, isto é, envia-se uma mensagem de falha de autenticação para o UE.

[00110] Caso o resultado de consulta seja a mensagem de falha de consulta reportada, isto também significa que a autenticação falhou, prossegue-se para o Bloco **231**, isto é, envia-se a mensagem de falha de autenticação para o UE.

[00111] Bloco **219**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[00112] Bloco **220**: A S-CSCF transfere (via download) o perfil de usuário a partir da UPSF ou do HSS através de uma mensagem Cx-Pull.

[00113] Bloco **221**: A S-CSCF envia uma mensagem 2xx Auth_OK para a I-CSCF indicando que a autenticação foi bem-sucedida.

[00114] Bloco **222**: A I-CSCF encaminha a mensagem 2xx Auth_OK para a P-CSCF.

[00115] Bloco **223**: A P-CSCF encaminha a mensagem 2xx Auth_OK para o UE.

[00116] Bloco **231**, conforme mostrado na Figura 4b: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este

usuário.

[00117] Bloco **232**: A S-CSCF transfere (via download) o perfil de usuário a partir da UPSF ou do HSS através de uma mensagem Cx-Pull.

[00118] Bloco **233**: A S-CSCF envia uma mensagem de falha de autenticação para a I-CSCF indicando que a autenticação falhou.

[00119] Bloco **234**: A I-CSCF encaminha uma mensagem de falha de autenticação para a P-CSCF.

[00120] Bloco **235**: A P-CSCF encaminha uma mensagem de falha de autenticação para o UE.

[00121] Nós métodos de acordo com as primeira e segunda modalidades, o UE não enviará a mensagem Register portando a identidade de rede de acesso e a informação de associação até determinar que o mecanismo de autenticação é uma autenticação de IMS em feixe com NASS. Enquanto isso, na terceira modalidade, o UE envia a mensagem Register portando a identidade de rede de acesso e a informação de associação bem no começo. De modo similar às primeira e segunda modalidades, a UPSF ou o HSS pré-armazena o perfil de usuário indicando se o mecanismo de autenticação do usuário é uma autenticação de IMS em feixe com NASS.

[00122] Com referência às Figuras 5a e 5b, o método de autenticação de acordo com a terceira modalidade é conforme se segue:

[00123] Bloco **301**: O UE envia uma mensagem Register portando a identidade de rede de acesso e a informação de associação para a P-CSCF.

[00124] Bloco **302**: A P-CSCF localiza a CLF de acordo com a identidade de rede de acesso na mensagem Register e a relação correspondente pré-regulada entre a CLF e a identidade de rede de acesso.

[00125] Bloco **303**: A P-CSCF consulta a CLF localizada no bloco **302** sobre a informação de anexação do UE na camada de acesso de acordo com a informação de associação na mensagem Register. A CLF pré-armazena o registro dados da informação de anexação correspondente à informação de associação, onde a informação de anexação inclui uma informação de endereço de IP, uma informação de localização, etc., mas não uma indicação em feixe na técnica relacionada. Se não houver um registro de dados na informação de anexação correspondente à informação de associação, a CLF retornará uma mensagem de falha de consulta para a P-CSCF.

[00126] Bloco **304**: A P-CSCF envia para a I-CSCF a mensagem Register portando o resultado de consulta no bloco **303** e o endereço de IP de origem da mensagem Register recebida pela P-CSCF; se a consulta no bloco **303** for bem-sucedida, a P-CSCF enviará a informação de anexação consultada para a I-CSCF; caso contrário, a P-CSCF reportará uma mensagem de falha de consulta para a I-CSCF.

[00127] Bloco **305**: A I-CSCF interage com a UPSF ou o HSS através de uma mensagem Cx-Selection-Info para selecionar a S-CSCF correspondente, isto é, a I-CSCF envia uma requisição para UPSF ou o HSS para buscar o perfil de usuário na UPSF ou no HSS para selecionar a S-CSCF para processamento da mensagem Register.

[00128] Bloco **306**: A I-CSCF encaminha a mensagem Register portando o resultado de consulta e o endereço de IP de origem da mensagem Register recebida pela P-CSCF para a S-CSCF selecionada no Bloco **305**. Caso a consulta seja bem-sucedida, o resultado de consulta é a informação de anexação consultada; caso contrário, o resultado de consulta é a mensagem de falha de consulta reportada.

[00129] Bloco **307**: A S-CSCF envia uma mensagem Cx-Put para o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ele foi atribuído para servir a este usuário.

[00130] Bloco **308**: A S-CSCF envia uma mensagem AV-Req para a UPSF ou o HSS requisitando os dados de autenticação do usuário.

[00131] Bloco **309**: A UPSF ou o HSS checa o perfil de usuário e determina que o mecanismo de autenticação do usuário é a autenticação de IMS em feixe com NASS.

[00132] Bloco **310**: A UPSF ou o HSS retorna uma mensagem AV-Req-Resp para a S-CSCF. Diferentemente dos dados de autenticação enviados na técnica relacionada, uma indicação do mecanismo de autenticação é enviada em conjunto com os dados de autenticação para a S-CSCF.

[00133] Bloco **311**: se o resultado de consulta for a informação de anexação consultada, a S-CSCF compara o endereço de IP de origem da mensagem Register recebida pela P-CSCF com o endereço de IP na informação de anexação consultada a partir da CLF. Caso o endereço de IP de origem da mensagem Register recebida pela P-CSCF seja consistente com o endereço de IP na informação de anexação consultada a partir da CLF, isto significa que a autenticação é bem-sucedida, prossegue-se para o Bloco **312**, isto é, envia-se uma mensagem de sucesso de autenticação para o UE; caso contrário, isto significa que a autenticação falhou, prossegue-se para o Bloco **321**, isto é, envia-se uma mensagem de falha de autenticação para o UE.

[00134] Caso o resultado de consulta seja a mensagem de falha de consulta reportada, isto também significa que a autenticação falhou, prossegue-se para o Bloco **321**, isto é, envia-se a mensagem de falha de autenticação para o UE.

[00135] Bloco **312**: A S-CSCF envia uma mensagem Cx-Put para a

UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[00136] Bloco **313**: A S-CSCF transfere (via download) o perfil de usuário a partir da UPSF ou do HSS através de uma mensagem Cx-Pull.

[00137] Bloco **314**: A S-CSCF envia uma mensagem 2xx Auth_OK para a I-CSCF indicando que a autenticação foi bem-sucedida.

[00138] Bloco **315**: A I-CSCF encaminha a mensagem 2xx Auth_OK para a P-CSCF.

[00139] Bloco **316**: após receber a mensagem 2xx Auth_OK, a P-CSCF determina que ela não recebeu uma mensagem 4xx Auth_Challenge antes; portanto, a P-CSCF não precisa estabelecer uma associação de segurança com o UE. A P-CSCF encaminha a mensagem 2xx Auth_OK para o UE; e, após receber a mensagem 2xx Auth_OK, o UE determina que ele não recebeu a mensagem 4xx Auth_Challenge antes; portanto, o UE não precisa estabelecer uma associação de segurança com a P-CSCF.

[00140] Bloco **321**, conforme mostrado na Figura 5b: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[00141] Bloco **322**: A S-CSCF transfere (via download) o perfil de usuário a partir da UPSF ou do HSS através de uma mensagem Cx-Pull.

[00142] Bloco **323**: A S-CSCF envia uma mensagem de falha de autenticação para a I-CSCF indicando que a autenticação falhou.

[00143] Bloco **324**: A I-CSCF encaminha uma mensagem de falha de autenticação para a P-CSCF.

[00144] Bloco **325**: A P-CSCF encaminha uma mensagem de falha de autenticação para o UE.

[00145] De modo similar à segunda modalidade, quando a operadora de rede é a mesma que a operadora de rede de serviço, uma vez que a informação de associação e a IMPI são as mesmas, o NASS não emite a identidade de rede de acesso e a informação de associação para o UE. Neste momento, uma quarta modalidade pode ser adotada, conforme mostrado nas Figura 6a e 6b. A quarta modalidade é uma simplificação da terceira modalidade. Na quarta modalidade, a operadora de rede de acesso e a CLF são reconhecidas através do endereço de IP de origem da mensagem Register, e a informação de anexação do UE na camada de acesso é consultada a partir da CLF de acordo com a IMPI na camada de serviço de IMS. De modo similar à primeira modalidade, a UPSF ou o HSS também pré-armazena o perfil de usuário indicando se o mecanismo de autenticação do usuário é uma autenticação de IMS em feixe com NASS.

[00146] Com referência às Figuras 6a e 6b, o método da quarta modalidade inclui:

[00147] Bloco **401**: O UE envia uma mensagem Register para a P-CSCF. Diferentemente da terceira modalidade, a mensagem Register não precisa portar a identidade de rede de acesso e a informação de associação. Ao invés disso, a mensagem Register porta a IMPI no cabeçalho de autenticação.

[00148] Bloco **402**: A P-CSCF localiza a CLF de acordo com o endereço de IP de origem da mensagem Register e a pré-regulagem correspondente à relação entre o endereço de IP de origem e a CLF

[00149] Bloco **403**: A P-CSCF consulta a CLF sobre a informação de anexação do UE na camada de acesso de acordo com a IMPI portada no cabeçalho de autenticação da mensagem Register. A CLF

pré-armazena o registro de dados da informação de anexação correspondente à IMPI. A informação de anexação inclui a informação de endereço de IP, uma informação de localização, etc., mas nenhuma informação em feixe na técnica relacionada. Se a CLF não tiver um registro de dados correspondente à IMPI, a CLF retornará uma mensagem de falha de consulta para a P-CSCF.

[00150] Os Blocos **404** a **425** são respectivamente os mesmos que os Blocos **304** a **325** na terceira modalidade.

[00151] Bloco **404**: A P-CSCF envia para a I-CSCF a mensagem Register portando o resultado de consulta no bloco 403 e o endereço de IP de origem da mensagem Register recebida pela P-CSCF; se a consulta no bloco **403** for bem-sucedida, a P-CSCF enviará a informação de anexação consultada para a I-CSCF; caso contrário, a P-CSCF reportará uma mensagem de falha de consulta para a I-CSCF.

[00152] Bloco **405**: A I-CSCF interage com a UPSF ou o HSS através de uma mensagem Cx-Selection-Info para selecionar a S-CSCF correspondente, isto é, a I-CSCF envia uma requisição para UPSF ou o HSS para buscar o perfil de usuário na UPSF ou no HSS para selecionar a S-CSCF para processamento da mensagem Register.

[00153] Bloco **406**: A I-CSCF encaminha a mensagem Register portando o resultado de consulta e o endereço de IP de origem da mensagem Register recebida pela P-CSCF para a S-CSCF selecionada no Bloco **405**. Caso a consulta seja bem-sucedida, o resultado de consulta é a informação de anexação consultada; caso contrário, o resultado de consulta é a mensagem de falha de consulta reportada.

[00154] Bloco **407**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-

CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[00155] Bloco **408**: A S-CSCF envia uma mensagem AV-Req para a UPSF ou o HSS requisitando os dados de autenticação do usuário.

[00156] Bloco **409**: A UPSF ou o HSS checa o perfil de usuário para obter o mecanismo de autenticação o qual indica que a autenticação de IMS é em feixe com NASS.

[00157] Bloco **410**: A UPSF ou o HSS retorna uma mensagem AV-Req-Resp para a S-CSCF. Diferentemente dos dados de autenticação enviados na técnica relacionada, uma indicação do mecanismo de autenticação é enviada em conjunto com os dados de autenticação para a S-CSCF.

[00158] Bloco **411**: se o resultado de consulta for a informação de anexação consultada, a S-CSCF compara o endereço de IP de origem da mensagem Register recebida pela P-CSCF com o endereço de IP na informação de anexação consultada a partir da CLF. Caso o endereço de IP de origem da mensagem Register recebida pela P-CSCF seja consistente com o endereço de IP na informação de anexação consultada a partir da CLF, isto significa que a autenticação é bem-sucedida, prossegue-se para o Bloco **412**, isto é, envia-se uma mensagem de sucesso de autenticação para o UE; caso contrário, isto significa que a autenticação falhou, prossegue-se para o Bloco **421**, isto é, envia-se uma mensagem de falha de autenticação para o UE.

[00159] Caso o resultado de consulta seja a mensagem de falha de consulta reportada, isto também significa que a autenticação falhou, prossegue-se para o Bloco **421**, isto é, envia-se a mensagem de falha de autenticação para o UE.

[00160] Bloco **412**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi

atribuída(o) para servir a este usuário.

[00161] Bloco **413**: A S-CSCF transfere (via download) o perfil de usuário a partir da UPSF ou do HSS através de uma mensagem Cx-Pull.

[00162] Bloco **414**: A S-CSCF envia uma mensagem 2xx Auth_OK para a I-CSCF indicando que a autenticação foi bem-sucedida.

[00163] Bloco **415**: A I-CSCF encaminha a mensagem 2xx Auth_OK para a P-CSCF.

[00164] Bloco **416**: após receber a mensagem 2xx Auth_OK, a P-CSCF determina que ela não recebeu uma mensagem 4xx Auth_Challenge antes, portanto, a P-CSCF não precisa estabelecer uma associação de segurança com o UE. A P-CSCF encaminha a mensagem 2xx Auth_OK para o UE; e, após receber a mensagem 2xx Auth_OK, o UE determina que ele não recebeu a mensagem 4xx Auth_Challenge antes, portanto, o UE não precisa estabelecer uma associação de segurança com a P-CSCF.

[00165] Bloco **421**, conforme mostrado na Figura 6b: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[00166] Bloco **422**: A S-CSCF transfere (via download) o perfil de usuário a partir da UPSF ou do HSS através de uma mensagem Cx-Pull.

[00167] Bloco **423**: A S-CSCF envia uma mensagem de falha de autenticação para a I-CSCF indicando que a autenticação falhou.

[00168] Bloco **424**: A I-CSCF encaminha uma mensagem de falha de autenticação para a P-CSCF.

[00169] Bloco **425**: A P-CSCF encaminha uma mensagem de falha de autenticação para o UE.

[00170] Nos métodos de acordo com da primeira à quarta modalidade, a S-CSCF autentica o UE ao comparar se o endereço de IP de origem da mensagem Register recebida pela P-CSCF é consistente com o endereço de IP consultado a partir da CLF. Na quinta modalidade da presente invenção, a S-CSCF autentica o UE ao comparar se a informação de associação do UE na rede de acesso pré-armazenada na UPSF ou no HSS é consistente com aquela consultada a partir da CLF. A informação de associação pode ser uma identidade de usuário de acesso, uma informação de localização, uma informação de endereço de IP, etc. Na quinta modalidade, a identidade de usuário de acesso é tomada como um exemplo para ilustração do processo de localização da CLF e do processo de consulta da informação de associação a partir da CLF. Pode ser visto a partir das modalidades precedentes da presente invenção que o processo de localização da CLF e o processo de consulta da informação de associação a partir da CLF podem ser implementados empregando-se outros parâmetros, os quais não serão repetidos aqui.

[00171] Com referência às Figuras 7a e 7b, o método de autenticação de acordo com a quinta modalidade é conforme se segue:

[00172] Bloco **501**: O UE envia uma mensagem Register para a P-CSCF.

[00173] Bloco **502**: A P-CSCF localiza a CLF de acordo com o endereço de IP de origem da mensagem Register e a relação correspondente entre a CLF e o endereço de IP de origem da mensagem Register.

[00174] Bloco **503**: A P-CSCF consulta a CLF sobre a identidade de usuário de acesso do usuário de acordo com o endereço de IP de origem da mensagem Register. A CLF pré-armazena um registro de dados da informação de anexação do UE correspondente ao endereço

de IP de origem; e a informação de anexação inclui pelo menos a informação de associação a qual é a identidade de usuário de acesso aqui. Se a CLF não tiver um registro de dados correspondente ao endereço de IP de origem, a CLF retornará uma mensagem de falha de consulta.

[00175] Bloco **504**: A P-CSCF envia a mensagem Register portando o resultado de consulta do bloco **503** para a I-CSCF. Caso a consulta seja bem-sucedida, a P-CSCF toma a identidade de usuário de acesso como o resultado de consulta para enviar para a I-CSCF; caso a consulta tenha falhado, a P-CSCF reporta uma mensagem de falha de consulta para a I-CSCF como o resultado de consulta.

[00176] Bloco **505**: A I-CSCF seleciona uma S-CSCF correspondente ao interagir com a UPSF ou o HSS através de uma mensagem Cx-Selection-Info, isto é, a I-CSCF envia a requisição para a UPSF ou o HSS para buscar um perfil de usuário do UE na UPSF ou no HSS para selecionar e S-CSCF para processamento da mensagem Register.

[00177] Bloco **506**: A I-CSCF encaminha a mensagem Register incluindo o resultado de consulta para a S-CSCF selecionada no Bloco **505**. Caso a consulta seja bem-sucedida, o resultado de consulta é a identidade de usuário de acesso, caso a consulta tenha falhado, o resultado de consulta é a mensagem de falha de consulta reportada.

[00178] Bloco **507**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[00179] Bloco **508**: A S-CSCF envia uma mensagem AV-Req para a UPSF ou o HSS requisitando os dados de autenticação do usuário.

[00180] Bloco **509**: A UPSF ou o HSS checa o perfil de usuário para obter o mecanismo de autenticação o qual indica que a autenticação

de IMS é em feixe com NASS.

[00181] Bloco **510**: A UPSF ou o HSS envia uma mensagem AV-Req-Resp para a S-CSCF. Diferentemente dos dados de autenticação enviados na técnica relacionada, a informação do mecanismo de autenticação do usuário e a informação de auditoria são emitidas para a S-CSCF neste bloco.

[00182] Bloco **511**: caso o resultado de consulta seja a identidade de usuário de acesso, a S-CSCF determina se a identidade de usuário de acesso consultada a partir da CLF é consistente com a informação de auditoria emitida pela UPSF ou pelo HSS. Caso a informação de auditoria consultada a partir da CLF seja consistente com a informação de auditoria emitida pela UPSF ou pelo HSS, isto significa que a autenticação foi bem-sucedida, prossegue-se para o Bloco **512**, isto é, envia-se uma mensagem de sucesso de autenticação para o UE; caso a informação de auditoria consultada a partir da CLF não seja consistente com a identidade de usuário de acesso emitida pela UPSF ou pelo HSS, isto significa que a autenticação falhou, prossegue-se para o Bloco **521**, isto é, envia-se uma mensagem de falha de autenticação para o UE.

[00183] Caso o resultado de consulta acima seja a mensagem de falha de consulta reportada, isto também significa que a autenticação falhou, prossegue-se para o Bloco **521**, isto é, envia-se a mensagem de falha de autenticação para o UE.

[00184] Bloco **512**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[00185] Bloco **513**: A S-CSCF consulta o perfil de usuário a partir da UPSF ou do HSS através de uma mensagem Cx-Pull.

[00186] Bloco **514**: A S-CSCF envia uma mensagem 2xx Auth_OK

para a I-CSCF indicando que a autenticação foi bem-sucedida;

[00187] Bloco **515**: A I-CSCF encaminha a mensagem 2xx Auth_OK para a P-CSCF.

[00188] Bloco **516**: após receber a mensagem 2xx Auth_OK, a P-CSCF determina que ela não recebeu uma mensagem 4xx Auth_Challenge antes; portanto, a P-CSCF não precisa estabelecer uma associação de segurança com o UE. A P-CSCF encaminha a mensagem 2xx Auth_OK para o UE. Após receber a mensagem 2xx Auth_OK, o UE determina que ele não recebeu a mensagem 4xx Auth_Challenge antes; portanto, o UE não precisa estabelecer uma associação de segurança com a P-CSCF.

[00189] Bloco **521**, conforme mostrado na Figura 7b: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[00190] Bloco **522**: A S-CSCF transfere (via download) o perfil de usuário a partir da UPSF ou do HSS através de uma mensagem Cx-Pull.

[00191] Bloco **523**: A S-CSCF envia uma mensagem de falha de autenticação para a I-CSCF indicando que a autenticação falhou.

[00192] Bloco **524**: A I-CSCF encaminha uma mensagem de falha de autenticação para a P-CSCF.

[00193] Bloco **525**: A P-CSCF encaminha uma mensagem de falha de autenticação para o UE.

[00194] Nas modalidades acima, a UPSF ou o HSS armazena apenas um mecanismo de autenticação para um usuário, isto é, a autenticação de IMS em feixe com NASS. Nas modalidades acima, o usuário será rejeitado para acessar a rede, se a autenticação de IMS em feixe com NASS falhar, o que restringe a autenticação e o uso de

serviços de rede, quando o usuário estiver fora de sua área doméstica (em roaming). Roaming significa que o usuário pode mudar seu ponto de acesso quando em movimento, mas a sessão em andamento é completamente interrompida e precisa ser reiniciada.

[00195] Por exemplo, o usuário pode desejar usar um terminal tradicional para acessar a rede em uma localização fixa, neste momento, a autenticação de IMS em feixe com NASS é adotada. Quando em roaming para um outro lugar, o usuário pode desejar usar um outro terminal para acessar a rede. Uma vez que a informação de localização do usuário é mudada, se ainda estiver usando a autenticação de IMS em feixe com NASS para autenticação do usuário, a autenticação falhará, o que afeta o usuário quanto ao uso da rede. Portanto, um mecanismo de autenticação de Compilação de Protocolo de Transmissão de Hipertexto (HTTP DIGEST) ou o mecanismo de autenticação de AKA de IMS pode ser adotado, após o mecanismo de autenticação de IMS em feixe com NASS falhar, desse modo se provendo uma autenticação flexível para o usuário.

[00196] Com referência à Figura 8, o processo de mecanismo de autenticação de HTTP DIGEST inclui principalmente:

[00197] Bloco **s301**: O UE envia uma mensagem Register para a P-CSCF.

[00198] Bloco **s302**: A P-CSCF encaminha a mensagem Register do UE para a I-CSCF.

[00199] Bloco **s303**: A I-CSCF seleciona uma S-CSCF correspondente ao interagir com a HSS através de uma mensagem Cx-Selection-Info, isto é, a I-CSCF envia uma requisição para o HSS para buscar o perfil de usuário no HSS para seleção da S-CSCF para processamento da mensagem Register.

[00200] Bloco **s304**: A I-CSCF encaminha a mensagem Register do UE para a S-CSCF selecionada no Bloco s303.

[00201] Bloco **s305**: A S-CSCF envia uma mensagem Cx-Put para o HSS para atualização da informação de indicação de S-CSCF e notificar ao HSS que ele foi atribuído para servir a este usuário.

[00202] Bloco **s306**: A S-CSCF envia uma mensagem AV-Req para o HSS requisitando os dados de autenticação do usuário.

[00203] Bloco **s307**: O HSS checa o perfil de usuário e determina que o mecanismo de autenticação do usuário é a HTTP DIGEST, e gera parâmetros de autenticação tais como nonce (número ou cadeia de bits usado apenas uma vez) e resposta de expectativa (XRES), etc.

[00204] O HSS envia uma mensagem AV-Req-Resp portando uma indicação do mecanismo de autenticação, HTTP DIGEST, e os parâmetros de autenticação tais como nonce, XRES para a S-CSCF.

[00205] Bloco **s308**: A S-CSCF obtém a indicação do mecanismo de autenticação e armazena a XRES, então, envia a mensagem 4xx Auth_Challenge para a I-CSCF.

[00206] Bloco **s309**: A I-CSCF encaminha a mensagem 4xx Auth_Challenge para a P-CSCF.

[00207] Bloco **s310**: após receber a mensagem 4xx Auth_Challenge, a P-CSCF determina que o parâmetro “algorithm” no cabeçalho WWW-Authenticate da mensagem 4xx Auth_Challenge indica que o mecanismo de autenticação do usuário é o HTTP DIGEST; portanto, a P-CSCF não precisa estabelecer uma associação de segurança com o UE. A P-CSCF envia a mensagem 4xx Auth_Challenge sem o cabeçalho Security-Server para o UE.

[00208] Bloco **s311**: após receber a mensagem 4xx Auth_Challenge, o UE determina que o parâmetro “algorithm” indica que o mecanismo de autenticação do usuário é o HTTP DIGEST, portanto, o UE não precisa estabelecer a associação de segurança com a P-CSCF; e o UE envia uma mensagem Register portando uma resposta (RES) para a P-CSCF de novo.

[00209] Bloco **s312**: A P-CSCF encaminha a mensagem Register portando a RES para a I-CSCF.

[00210] Bloco **s313**: A I-CSCF envia a mensagem Cx-Query para o HSS para determinar a S-CSCF para processamento da mensagem Register, isto é, a I-CSCF consulta a UPSF ou o HSS sobre a S-CSCF a qual foi atribuída para servir a este usuário. O HSS retorna o nome de S-CSCF o qual foi previamente selecionado no bloco **s303** para a I-CSCF de acordo com a informação de indicação de S-CSCF armazenada no HSS.

[00211] Bloco **s314**: A I-CSCF encaminha a mensagem Register para a S-CSCF determinada no Bloco **s313**.

[00212] A S-CSCF compara a XRES obtida a partir do HSS com a RES enviada pelo UE; caso a XRES obtida a partir do HSS seja consistente com a RES enviada pelo UE, isto significa que a autenticação foi bem-sucedida; caso contrário, isto significa que a autenticação falhou.

[00213] Bloco **s315**: A S-CSCF envia uma mensagem Cx-Put para o HSS para atualização da informação de indicação de S-CSCF no HSS e notificar o HSS que ele foi atribuído para servir a este usuário.

[00214] Bloco **s316**: A S-CSCF transfere (via download) o perfil de usuário a partir do HSS através de uma mensagem Cx-Pull.

[00215] Bloco **s317**: A S-CSCF envia a mensagem 200 indicando que a autenticação foi bem-sucedida para a I-CSCF, ou uma mensagem 403 Forbidden indicando que a autenticação falhou para a I-CSCF. Para fins ilustrativos, apenas a mensagem 200 enviada quando a autenticação é bem-sucedida é mostrada na Figura 8.

[00216] Bloco **s318**: A I-CSCF encaminha a mensagem 200 ou a mensagem 403 Forbidden para a P-CSCF.

[00217] Bloco **s319**: A P-CSCF encaminha a mensagem 200 ou a mensagem 403 Forbidden para o UE.

[00218] De acordo com da primeira à quinta modalidade, os dados de autenticação pré-armazenados na UPSF ou no HSS são configurados como o mecanismo de autenticação HTTP DIGEST ou o AKA de IMS além da autenticação de IMS em feixe com NASS.

[00219] A sexta modalidade, mostrada nas Figura 9a e 9b, é com respeito à terceira modalidade. Na sexta modalidade, o mecanismo de autenticação é adotado após a autenticação de IMS em feixe com NASS ter falhado.

[00220] Com referência às Figuras 9a e 9b, o método de autenticação de acordo com sexta modalidade da presente invenção inclui:

[00221] Bloco **601**: O UE envia uma mensagem Register portando a identidade de rede de acesso e a informação de associação para a P-CSCF.

[00222] Bloco **602**: A P-CSCF localiza a CLF de acordo com a identidade de rede de acesso na mensagem Register e a relação correspondente pré-regulada entre a CLF e a identidade de rede de acesso.

[00223] Bloco **603**: A P-CSCF consulta a CLF localizada no bloco 602 sobre a informação de anexação do UE na camada de acesso de acordo com a informação de associação na mensagem Register. A CLF pré-armazena o registro dados da informação de anexação correspondente à informação de associação, onde a informação de anexação inclui uma informação de endereço de IP, uma informação de localização, etc., mas não uma indicação em feixe na técnica relacionada. Caso não haja um registro de dados correspondente à informação de associação, a CLF retorna uma mensagem de falha de consulta para a P-CSCF.

[00224] Bloco **604**: A P-CSCF envia para a I-CSCF a mensagem Register portando o resultado de consulta no bloco **603** e o endereço

de IP de origem da mensagem Register recebida pela P-CSCF; se a consulta no bloco **603** for bem-sucedida, a P-CSCF enviará a informação de anexação consultada para a I-CSCF; caso contrário, a P-CSCF reportará uma mensagem de falha de consulta para a I-CSCF.

[00225] Bloco **605**: A I-CSCF interage com a UPSF ou o HSS através de uma mensagem Cx-Selection-Info para selecionar a S-CSCF correspondente, isto é, a I-CSCF envia uma requisição para a UPSF ou o HSS para buscar o perfil de usuário na UPSF ou no HSS para determinar a S-CSCF para processamento da mensagem Register.

[00226] Bloco **606**: A I-CSCF encaminha a mensagem Register portando o resultado de consulta e o endereço de IP de origem da mensagem Register recebida pela P-CSCF para a S-CSCF determinada no Bloco **605**. Caso a consulta seja bem-sucedida, o resultado de consulta é a informação de anexação consultada; caso contrário, o resultado de consulta é a mensagem de falha de consulta reportada.

[00227] Bloco **607**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[00228] Bloco **608**: A S-CSCF envia uma mensagem AV-Req para a UPSF ou o HSS requisitando os dados de autenticação do usuário.

[00229] Bloco **609**: A UPSF ou o HSS checa o perfil de usuário e descobre que os dados de autenticação são configurados como os mecanismos de NBA e o HTTP DIGEST.

[00230] Bloco **610**: A UPSF ou o HSS envia uma mensagem AV-Req-Resp para a S-CSCF para enviar os dados de autenticação do usuário para a S-CSCF.

[00231] Bloco **611**: A S-CSCF armazena todos os mecanismos de autenticação e os dados de autenticação correspondentes aos mecanismos de autenticação. Caso o resultado de consulta seja a informação de anexação, a S-CSCF compara o endereço de IP de origem da mensagem Register recebida pela P-CSCF com o endereço de IP na informação de anexação consultada a partir da CLF. Caso o endereço de IP de origem da mensagem Register recebida pela P-CSCF seja consistente com o endereço de IP na informação de anexação consultada a partir da CLF, isto significa que a autenticação é bem-sucedida, prossegue-se para o Bloco **612**, isto é, enviar uma mensagem de sucesso de autenticação para o UE. Caso o endereço de IP de origem da mensagem Register recebido pela P-CSCF não seja consistente com o endereço de IP na informação de anexação consultada a partir da CLF, isto significa que a autenticação falhou, prossegue-se para o Bloco **621**, isto é, autentica-se o usuário pelo mecanismo de autenticação HTTP DIGEST.

[00232] Caso o resultado de consulta acima seja a mensagem de falha de consulta reportada, isto também significa que a autenticação falhou, prossegue-se para o Bloco **621**, isto é, autentica-se o usuário pelo mecanismo de autenticação HTTP DIGEST.

[00233] Bloco **612**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[00234] Bloco **613**: A S-CSCF transfere (via download) o perfil de usuário a partir da UPSF ou do HSS através de uma mensagem Cx-Pull.

[00235] Bloco **614**: A S-CSCF envia uma mensagem 2xx Auth_OK para a I-CSCF para indicar que a autenticação é bem-sucedida.

[00236] Bloco **615**: A I-CSCF encaminha a mensagem 2xx Auth_OK

para a P-CSCF.

[00237] Bloco **616**: após receber a mensagem 2xx Auth_OK, a P-CSCF determina que ela não recebeu uma mensagem 4xx Auth_Challenge antes, portanto, P-CSCF não precisa estabelecer uma associação de segurança com o UE; a P-CSCF encaminha a mensagem 2xx Auth_OK para o UE; e após receber a mensagem 2xx Auth_OK, o UE determina que ele não recebeu a 4xx Auth_Challenge antes, então, o UE não precisa estabelecer uma associação de segurança com a P-CSCF.

[00238] Bloco **621**, conforme mostrado na Figura 9b: uma vez que a S-CSCF armazenou os dados de autenticação obtidos a partir da UPSF ou do HSS no Bloco **611** correspondente ao mecanismo de autenticação HTTP DIGEST, a S-CSCF envia a mensagem 4xx Auth_Challenge incluindo a informação de autenticação do HTTP DIGEST para a I-CSCF.

[00239] Bloco **622**: A I-CSCF encaminha a mensagem 4xx Auth_Challenge para a P-CSCF.

[00240] Bloco **623**: após receber a mensagem 4xx Auth_Challenge, a P-CSCF determina que um parâmetro “algorithm” em um cabeçalho WWW-Authenticate da mensagem 4xx Auth_Challenge indica que o mecanismo de autenticação é o HTTP DIGEST, portanto, a P-CSCF não precisa estabelecer uma associação de segurança com o UE; a P-CSCF envia a mensagem 4xx Auth_Challenge sem o cabeçalho Security-Server para o UE.

[00241] Bloco **624**: após receber a mensagem 4xx Auth_Challenge, o UE determina que o parâmetro “algorithm” indica que o mecanismo de autenticação é o HTTP DIGEST, portanto, UE não precisa estabelecer uma associação de segurança com a P-CSCF; e o UE envia uma mensagem Register portando um parâmetro de autenticação para a P-CSCF de novo.

[00242] Bloco **625**: A P-CSCF encaminha a mensagem Register portando o parâmetro de autenticação para a I-CSCF.

[00243] Bloco **626**: A I-CSCF envia uma mensagem Cx-Query para a UPSF ou o HSS para determinar a S-CSCF para processamento da mensagem Register, isto é, a I-CSCF consulta a UPSF ou o HSS sobre a S-CSCF a qual foi atribuída para servir a este usuário. A UPSF ou o HSS retorna o nome de S-CSCF, o qual foi previamente selecionado no bloco 603 para a I-CSCF de acordo com a informação de indicação de S-CSCF armazenada no HSS.

[00244] Bloco **627**: A I-CSCF encaminha a mensagem Register para a S-CSCF determinada no Bloco 626.

[00245] A S-CSCF compara o parâmetro de autenticação obtido a partir da UPSF ou do HSS com o parâmetro de autenticação enviado pelo UE; caso o parâmetro de autenticação obtido a partir da UPSF ou do HSS seja consistente com o parâmetro de autenticação enviado pelo UE, isto significa que a autenticação foi bem-sucedida; caso contrário, isto significa que a autenticação falhou.

[00246] Bloco **628**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[00247] Bloco **629**: A S-CSCF transfere (via download) o perfil de usuário a partir da UPSF ou do HSS através de uma mensagem Cx-Pull.

[00248] Bloco **630**: A S-CSCF envia a mensagem 200 indicando que a autenticação foi bem-sucedida para a I-CSCF, ou uma mensagem 403 Forbidden indicando que a autenticação falhou para a I-CSCF. Para fins ilustrativos, apenas a mensagem 200 enviada quando a autenticação é bem-sucedida é mostrada na Figura 9b.

[00249] Bloco **631**: A I-CSCF encaminha a mensagem 200 ou a

mensagem 403 Forbidden para a P-CSCF.

[00250] Bloco **632**: A P-CSCF encaminha a mensagem 200 ou a mensagem 403 Forbidden para o UE.

[00251] Com respeito à quarta ou à quinta modalidade, a sexta modalidade pode ser modificada de acordo com as diferenças entre a quarta ou a quinta modalidade e a terceira modalidade, as quais não serão repetidas aqui.

[00252] A sétima modalidade, conforme mostrado nas Figura 10a e 10b, na qual o mecanismo de autenticação de AKA de IMS é adotado após o mecanismo de autenticação de IMS em feixe com NASS ter falhado.

[00253] Com referência às Figuras 10a e 10b, o método da sétima modalidade de acordo com a presente invenção inclui:

[00254] Bloco **701**: O UE envia uma mensagem Register portando a identidade de rede de acesso e a informação de associação para a P-CSCF.

[00255] Bloco **702**: A P-CSCF localiza a CLF de acordo com a identidade de rede de acesso na mensagem Register e a relação correspondente pré-regulada entre a CLF e a identidade de rede de acesso.

[00256] Bloco **703**: A P-CSCF consulta a CLF localizada no bloco **702** sobre a informação de anexação do UE na camada de acesso de acordo com a informação de associação na mensagem Register. A CLF pré-armazena o registro dados da informação de anexação correspondente à informação de associação, onde a informação de anexação inclui uma informação de endereço de IP, uma informação de localização, etc., mas não uma indicação em feixe na técnica relacionada. Caso não haja um registro de dados correspondente à informação de associação, a CLF retorna uma mensagem de falha de consulta para a P-CSCF.

[00257] Bloco **704**: A P-CSCF envia para a I-CSCF a mensagem Register portando o resultado de consulta no bloco **703** e o endereço de IP de origem da mensagem Register recebida pela P-CSCF; se a consulta no bloco **703** for bem-sucedida, a P-CSCF enviará a informação de anexação para a I-CSCF; caso contrário, a P-CSCF reportará uma mensagem de falha de consulta para a I-CSCF.

[00258] Bloco **705**: A I-CSCF interage com a UPSF ou o HSS através de uma mensagem Cx-Selection-Info para selecionar a S-CSCF correspondente, isto é, a I-CSCF envia uma requisição para UPSF ou o HSS para buscar o perfil de usuário na UPSF ou no HSS para selecionar a S-CSCF para processamento da mensagem Register.

[00259] Bloco **706**: A I-CSCF encaminha a mensagem Register portando o resultado de consulta e o endereço de IP de origem da mensagem Register recebida pela P-CSCF para a S-CSCF selecionada no Bloco **705**. Se a consulta for bem-sucedida, o resultado de consulta será a informação de anexação; caso contrário, o resultado de consulta será a mensagem de falha de consulta reportada.

[00260] Bloco **707**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[00261] Bloco **708**: A S-CSCF envia uma mensagem AV-Req para a UPSF ou o HSS requisitando os dados de autenticação do usuário.

[00262] Bloco **709**: A UPSF ou o HSS detecta que os dados de autenticação são configurados como o mecanismo de autenticação de NBA e AKA de IMS.

[00263] Bloco **710**: A UPSF ou o HSS envia uma mensagem AV-Req-Resp para a S-CSCF para enviar os dados de autenticação do

usuário para a S-CSCF.

[00264] Bloco **711**: A S-CSCF armazena todos os mecanismos de autenticação e os dados de autenticação correspondentes aos mecanismos de autenticação. Caso o resultado de consulta seja a informação de anexação, a S-CSCF compara o endereço de IP de origem da mensagem Register recebida pela P-CSCF com o endereço de IP na informação de anexação consultada a partir da CLF. Caso o endereço de IP de origem da mensagem Register recebida pela P-CSCF seja consistente com o endereço de IP na informação de anexação consultada a partir da CLF, isto significa que a autenticação é bem-sucedida, prossegue-se para o Bloco **712**, isto é, enviar uma mensagem de sucesso de autenticação para o UE. Caso o endereço de IP de origem da mensagem Register recebido pela P-CSCF não seja consistente com o endereço de IP na informação de anexação consultada a partir da CLF, isto significa que a autenticação falhou, prossegue-se para o Bloco **721**, isto é, autenticar o usuário pelo mecanismo de autenticação de AKA de IMS.

[00265] Caso o resultado de consulta acima seja a mensagem de falha de consulta reportada, isto também significa que a autenticação falhou, prossegue-se para o Bloco **721**, isto é, autenticar o usuário pelo mecanismo de autenticação de AKA de IMS.

[00266] Bloco **712**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[00267] Bloco **713**: A S-CSCF transfere (via download) o perfil de usuário a partir da UPSF ou do HSS através de uma mensagem Cx-Pull.

[00268] Bloco **714**: A S-CSCF envia uma mensagem 2xx Auth_OK para a I-CSCF indicando que a autenticação foi bem-sucedida.

[00269] Bloco **715**: A I-CSCF encaminha a mensagem 2xx Auth_OK para a P-CSCF.

[00270] Bloco **716**: após receber a mensagem 2xx Auth_OK, a P-CSCF determina que ela não recebeu uma mensagem 4xx Auth_Challenge antes, portanto, a P-CSCF não precisa estabelecer uma associação de segurança com o UE; a P-CSCF encaminha a mensagem 2xx Auth_OK para o UE; e, após receber a mensagem 2xx Auth_OK, o UE determina que ele não recebeu a mensagem 4xx Auth_Challenge antes, portanto, o UE precisa estabelecer uma associação de segurança com a P-CSCF.

[00271] Bloco **721**, conforme mostrado na Figura 10b: uma vez que a S-CSCF armazenou os dados de autenticação obtidos a partir da UPSF ou do HSS no Bloco **711** correspondente ao mecanismo de autenticação de AKA de IMS, a S-CSCF envia a mensagem 4xx Auth_Challenge portando a informação de autenticação do mecanismo de autenticação de AKA de IMS para a I-CSCF.

[00272] Bloco **722**: A I-CSCF encaminha a mensagem 4xx Auth_Challenge para a P-CSCF.

[00273] Bloco **723**: após receber a mensagem 4xx Auth_Challenge, a P-CSCF determina que um parâmetro “algorithm” no cabeçalho de WWW-Authenticate de uma mensagem 4xx Auth_Challenge indica que o mecanismo de autenticação é o IMS AKA, portanto, a P-CSCF não precisa estabelecer uma associação de segurança com o UE; a P-CSCF encaminha a mensagem 4xx Auth_Challenge para o UE.

[00274] Bloco **724**: após receber a mensagem 4xx Auth_Challenge, o UE determina que o parâmetro “algorithm” no cabeçalho WWW-Authenticate da mensagem 4xx Auth_Challenge indica que o mecanismo de autenticação é o IMS AKA, portanto, o UE precisa estabelecer uma associação de segurança com a P-CSCF; o UE envia uma mensagem Register portando o parâmetro de autenticação para a

P-CSCF de novo.

[00275] Bloco **725**: A P-CSCF encaminha a mensagem Register do UE para a I-CSCF.

[00276] Bloco **726**: A I-CSCF envia uma mensagem Cx-Query para a UPSF ou o HSS para determinar a S-CSCF para processamento da mensagem Register, isto é, a I-CSCF consulta a UPSF ou o HSS sobre a S-CSCF a qual foi atribuída para servir a este usuário. A UPSF ou o HSS retorna o nome de S-CSCF, o qual foi previamente selecionado no bloco 703 para a I-CSCF de acordo com a informação de indicação de S-CSCF armazenada no HSS.

[00277] Bloco **727**: A I-CSCF encaminha a mensagem Register para a S-CSCF determinada no Bloco **726**.

[00278] A S-CSCF compara o parâmetro de autenticação obtido a partir da UPSF ou do HSS com o parâmetro de autenticação enviado pelo; caso o parâmetro de autenticação obtido a partir da UPSF ou do HSS seja consistente com o parâmetro de autenticação enviado pelo UE, isto significa que a autenticação foi bem-sucedida; caso contrário, isto significa que a autenticação falhou.

[00279] Bloco **728**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar o HSS que ele foi atribuído para servir a este usuário.

[00280] Bloco **729**: A S-CSCF transfere (via download) o perfil de usuário a partir do HSS através de uma mensagem Cx-Pull.

[00281] Bloco **730**: caso a autenticação seja bem-sucedida, a S-CSCF envia uma mensagem 2xx Auth_OK para a I-CSCF indicando que o registro é bem-sucedido, onde 2xx indica que a mensagem é relevante para sucesso, e xx é um número em 00~99; caso a autenticação tenha falhado, a S-CSCF envia uma mensagem de falha de autenticação para a I-CSCF.

[00282] Bloco **731**: A I-CSCF encaminha a mensagem 2xx Auth_OK ou a mensagem de falha de autenticação para a P-CSCF.

[00283] Bloco **732**: A P-CSCF encaminha a mensagem 2xx Auth_OK ou a mensagem de falha de autenticação para o UE.

[00284] Com respeito à quarta ou à quinta modalidade, o método da sétima modalidade pode ser modificado de forma correspondente de acordo com a diferença entre a quarta modalidade e a terceira modalidade, ou a diferença entre a quinta modalidade e a terceira modalidade, o que não será repetido aqui.

[00285] A oitava modalidade, conforme mostrado nas Figura 11a e 11b, é com respeito à primeira modalidade. Na oitava modalidade, o mecanismo de autenticação de HTTP DIGEST é adotado após a autenticação de IMS em feixe com NASS ter falhado.

[00286] Com referência às Figuras 11a e 11b, o método da oitava modalidade inclui:

[00287] Bloco **801**: O UE envia uma mensagem Register para a P-CSCF.

[00288] Bloco **802**: A P-CSCF encaminha a mensagem Register do UE para a I-CSCF.

[00289] Bloco **803**: A I-CSCF interage com a UPSF ou o HSS através de uma mensagem Cx-Selection-Info para selecionar a S-CSCF correspondente, isto é, a I-CSCF envia uma requisição para UPSF ou o HSS para buscar o perfil de usuário na UPSF ou no HSS para selecionar a S-CSCF para processamento da mensagem Register.

[00290] Bloco **804**: A I-CSCF encaminha a mensagem Register do UE para a S-CSCF selecionada no Bloco **803**.

[00291] Bloco **805**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi

atribuída(o) para servir a este usuário.

[00292] Bloco **806**: A S-CSCF envia uma mensagem AV-Req para a UPSF ou o HSS requisitando os dados de autenticação do usuário.

[00293] Bloco **807**: A UPSF ou o HSS detecta que os dados de autenticação são configurados como os mecanismos de autenticação de NBA de HTTP DIGEST.

[00294] Bloco **808**: A UPSF ou o HSS envia uma mensagem AV-Req-Resp para enviar os dados de autenticação do usuário para a S-CSCF. Os dados de autenticação incluem pelo menos o mecanismo de autenticação de IMS em feixe com NASS e os dados correspondentes ao mecanismo de autenticação de IMS em feixe com NASS, o mecanismo de autenticação de HTTP DIGEST e os dados de autenticação correspondentes ao mecanismo de autenticação de HTTP DIGEST.

[00295] Bloco **809**: A S-CSCF armazena todos os mecanismos de autenticação e os dados de autenticação correspondentes aos mecanismos de autenticação. O mecanismo de autenticação padrão é a autenticação de IMS em feixe com NASS, e o HTTP DIGEST é usado após o mecanismo de autenticação padrão ter falhado. A S-CSCF envia a mensagem 4xx Auth_Challenge para a I-CSCF, onde o cabeçalho de autenticação depositado da mensagem 4xx Auth_Challenge indica que o mecanismo de autenticação é a autenticação de IMS em feixe com NASS, isto é, porta uma indicação do mecanismo de autenticação.

[00296] Bloco **810**: A I-CSCF encaminha a mensagem 4xx Auth_Challenge para a P-CSCF.

[00297] Bloco **811**: após receber a mensagem 4xx Auth_Challenge, a P-CSCF determina que um “algorithm” em um cabeçalho WWW-Authenticate da mensagem 4xx Auth_Challenge indica que o mecanismo de autenticação do usuário é a autenticação de IMS em

feixe com NASS. Portanto, a P-CSCF não precisa estabelecer uma associação de segurança com o UE; a P-CSCF encaminha a mensagem 4xx portando a indicação em feixe, mas nenhum cabeçalho de Security-Server para o UE.

[00298] Bloco **812**: após receber a mensagem 4xx Auth_Challenge, o UE determina que o parâmetro “algorithm” no cabeçalho WWW-Authenticate da mensagem 4xx Auth_Challenge indica que o mecanismo de autenticação do usuário é autenticação de IMS em feixe com NASS. Portanto, o UE não precisa estabelecer uma associação de segurança com a P-CSCF; e envia para a P-CSCF uma outra mensagem Register portando uma identidade de rede de acesso e a informação de associação.

[00299] Bloco **813**: A P-CSCF localiza a CLF de acordo com a identidade de rede de acesso na mensagem Register e a relação correspondente pré-regulada entre a CLF e a identidade de rede de acesso.

[00300] Bloco **814**: A P-CSCF consulta a CLF localizada no bloco **813** sobre a informação de anexação do UE na camada de acesso de acordo com a informação de associação na mensagem Register. Diferentemente da técnica relacionada, a CLF pré-armazena o registro de dados da informação de anexação correspondente à informação de associação, onde a informação de anexação inclui uma informação de endereço de IP, uma informação de localização, etc., mas não uma indicação em feixe na técnica relacionada. Caso não haja um registro de dados correspondente à informação de associação, a CLF retorna uma mensagem de falha de consulta para a P-CSCF.

[00301] Bloco **815**: A P-CSCF envia para a I-CSCF a mensagem Register portando o resultado de consulta no bloco **814** e o endereço de IP de origem da mensagem Register recebida pela P-CSCF; se a consulta no bloco **814** for bem-sucedida, a P-CSCF enviará a

informação de anexação para a I-CSCF; caso contrário, a P-CSCF reportará uma mensagem de falha de consulta para a I-CSCF.

[00302] Bloco **816**: A I-CSCF envia uma mensagem Cx-Query para a UPSF ou o HSS para determinar a S-CSCF para processamento da mensagem Register, isto é, a I-CSCF consulta a UPSF ou o HSS sobre a S-CSCF a qual foi atribuída para servir a este usuário. A UPSF ou o HSS retorna o nome de S-CSCF, o qual foi previamente selecionado no bloco 703 para a I-CSCF de acordo com a informação de indicação de S-CSCF armazenada no HSS.

[00303] Bloco **817**: A I-CSCF encaminha a mensagem Register portando o resultado de consulta e o endereço de IP de origem da mensagem Register recebida pela P-CSCF para a S-CSCF determinada no Bloco **816**. Se a consulta for bem-sucedida, o resultado de consulta será a informação de anexação; caso contrário, o resultado de consulta será a mensagem de falha de consulta reportada.

[00304] Bloco **818**: Caso o resultado de consulta seja a informação de anexação, a S-CSCF compara o endereço de IP de origem da mensagem Register recebida pela P-CSCF com o endereço de IP na informação de anexação consultada a partir da CLF. Caso o endereço de IP de origem da mensagem Register recebida pela P-CSCF seja consistente com o endereço de IP na informação de anexação consultada a partir da CLF, isto significa que a autenticação é bem-sucedida, prossegue-se para o Bloco **819**, isto é, envia-se uma mensagem de sucesso de autenticação para o UE; caso contrário, isto significa que a autenticação falhou, prossegue-se para o Bloco **831**, isto é, envia-se uma mensagem de falha de autenticação para o UE.

[00305] Caso o resultado de consulta seja a mensagem de falha de consulta reportada, isto também significa que a autenticação falhou, prossegue-se para o Bloco **831**, isto é, envia-se a mensagem de falha

de autenticação para o UE.

[00306] Bloco **819**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[00307] Bloco **820**: A S-CSCF transfere (via download) o perfil de usuário a partir da UPSF ou do HSS através de uma mensagem Cx-Pull.

[00308] Bloco **821**: A S-CSCF envia uma mensagem 2xx Auth_OK para a I-CSCF indicando que a autenticação foi bem-sucedida.

[00309] Bloco **822**: A I-CSCF encaminha a mensagem 2xx Auth_OK para a P-CSCF.

[00310] Bloco **823**: A P-CSCF encaminha a mensagem 2xx Auth_OK para o UE.

[00311] Bloco **831**, conforme mostrado na Figura 11b: uma vez que a S-CSCF armazenou os dados de autenticação obtidos a partir da UPSF ou do HSS no Bloco **809** correspondente ao mecanismo de autenticação HTTP DIGEST, a S-CSCF envia a mensagem 4xx Auth_Challenge portando a informação de autenticação de HTTP DIGEST para a I-CSCF.

[00312] Bloco **832**: A I-CSCF encaminha a mensagem 4xx Auth_Challenge para a P-CSCF.

[00313] Bloco **833**: após receber a mensagem 4xx Auth_Challenge, a P-CSCF determina que o parâmetro “algorithm” em um cabeçalho de WWW-Authenticate da mensagem 4xx Auth_Challenge indica que o mecanismo de autenticação é o HTTP DIGEST, portanto, a P-CSCF não precisa estabelecer uma associação de segurança com o UE; e a P-CSCF envia a mensagem 4xx Auth_Challenge sem o cabeçalho Security-Server para o UE.

[00314] Bloco **834**: após receber a mensagem 4xx Auth_Challenge,

o UE determina que o parâmetro “algorithm” indica que o mecanismo de autenticação é o HTTP DIGEST, portanto, o UE não precisa estabelecer uma associação com P-CSCF; e o UE envia uma mensagem Register portando um parâmetro de autenticação para a P-CSCF de novo.

[00315] Bloco **835**: A P-CSCF encaminha a mensagem Register portando o parâmetro de autenticação para a I-CSCF.

[00316] Bloco **836**: A I-CSCF envia uma mensagem Cx-Query para a UPSF ou o HSS para determinar a S-CSCF para processamento da mensagem Register, isto é, a I-CSCF consulta a UPSF ou o HSS sobre a S-CSCF a qual foi atribuída para servir a este usuário. A UPSF ou o HSS retorna o nome de S-CSCF, o qual foi previamente selecionado no bloco 803 para a I-CSCF de acordo com a informação de indicação de S-CSCF armazenada no HSS.

[00317] Bloco **837**: A I-CSCF encaminha a mensagem Register para a S-CSCF determinada no Bloco 836.

[00318] A S-CSCF compara o parâmetro de autenticação obtido a partir da UPSF ou do HSS com o parâmetro de autenticação enviado pelo; caso o parâmetro de autenticação obtido a partir da UPSF ou do HSS seja consistente com o parâmetro de autenticação enviado pelo UE, isto significa que a autenticação foi bem-sucedida; caso contrário, isto significa que a autenticação falhou.

[00319] Bloco **838**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[00320] Bloco **839**: A S-CSCF transfere (via download) o perfil de usuário a partir da UPSF ou do HSS através de uma mensagem Cx-Pull.

[00321] Bloco **840**: A S-CSCF envia a mensagem 200 indicando

que a autenticação foi bem-sucedida para a I-CSCF, ou uma mensagem 403 Forbidden indicando que a autenticação falhou para a I-CSCF. Para fins ilustrativos, apenas a mensagem 200 enviada quando a autenticação é bem-sucedida é mostrada na Figura 10b.

[00322] Bloco **841**: A I-CSCF encaminha a mensagem 200 ou a mensagem 403 Forbidden para a P-CSCF.

[00323] Bloco **842**: A P-CSCF encaminha a mensagem 200 ou a mensagem 403 Forbidden para o UE.

[00324] Com respeito à segunda modalidade, o método da oitava modalidade pode ser modificado correspondentemente de acordo com a diferença entre a segunda modalidade e a primeira modalidade, o que não será repetido aqui.

[00325] A nona modalidade, conforme mostrado nas Figura 12a e 12b, é com respeito à primeira modalidade. Na nona modalidade, o mecanismo de autenticação de AKA de IMS é adotado após a autenticação de IMS em feixe com NASS ter falhado.

[00326] Com referência às Figuras 12a e 12b, o método da nona modalidade inclui:

[00327] Bloco **901**: O UE envia uma mensagem Register para a P-CSCF.

[00328] Bloco **902**: A P-CSCF encaminha a mensagem Register do UE para a I-CSCF.

[00329] Bloco **903**: A I-CSCF interage com a UPSF ou o HSS através de uma mensagem Cx-Selection-Info para selecionar a S-CSCF correspondente, isto é, a I-CSCF envia uma requisição para a UPSF ou o HSS para buscar o perfil de usuário na UPSF ou no HSS para selecionar qual S-CSCF processará a mensagem Register.

[00330] Bloco **904**: A I-CSCF encaminha a mensagem Register do UE para a S-CSCF selecionada no Bloco 903.

[00331] Bloco **905**: A S-CSCF envia uma mensagem Cx-Put para a

UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[00332] Bloco **906**: A S-CSCF envia uma mensagem AV-Req para a UPSF ou o HSS requisitando os dados de autenticação do usuário.

[00333] Bloco **907**: A UPSF ou o HSS checa o perfil de usuário e determina que os dados de autenticação são configurados como os mecanismos de autenticação de NBA e de AKA de IMS.

[00334] Bloco **908**: A UPSF ou o HSS envia uma mensagem AV-Req-Resp para enviar os dados de autenticação do usuário para a S-CSCF. Os dados de autenticação incluem pelo menos o mecanismo de autenticação de IMS em feixe com NASS e os dados de autenticação correspondentes ao mecanismo de autenticação de IMS em feixe com NASS, ao mecanismo de autenticação de AKA de IMS e os dados de autenticação correspondentes ao mecanismo de autenticação de AKA de IMS.

[00335] Bloco **909**: A S-CSCF armazena todos os mecanismos de autenticação e os dados de autenticação correspondentes aos mecanismos de autenticação. O mecanismo de autenticação padrão do usuário é o mecanismo de autenticação de IMS em feixe com NASS, após o mecanismo de autenticação padrão ter falhado, o AKA de IMS é usado. A S-CSCF envia a mensagem 4xx Auth_Challenge para a I-CSCF, onde o cabeçalho de autenticação depositado da mensagem 4xx Auth_Challenge indica que o mecanismo de autenticação é a autenticação de IMS em feixe com NASS, isto é, porta a indicação do mecanismo de autenticação.

[00336] Bloco **910**: A I-CSCF encaminha a mensagem 4xx Auth_Challenge para a P-CSCF.

[00337] Bloco **911**: após receber a 4xx Auth_Challenge, a P-CSCF determina que o parâmetro “algorithm” no cabeçalho WWW-

Authenticate da 4xx Auth_Challenge indica que o mecanismo de autenticação do usuário é autenticação de IMS em feixe com NASS. Portanto, a P-CSCF não precisa estabelecer uma associação de segurança com o UE, e encaminha a mensagem 4xx portando a indicação em feixe, mas nenhum cabeçalho de Security-Server para o UE.

[00338] Bloco **912**: após receber a mensagem 4xx Auth_Challenge, o UE determina que o parâmetro “algorithm” no cabeçalho WWW-Authenticate da mensagem 4xx Auth_Challenge indica que o mecanismo de autenticação do usuário é autenticação de IMS em feixe com NASS. Portanto, o UE não precisa estabelecer a associação de segurança com a P-CSCF; e envia para a P-CSCF uma outra mensagem Register portando a identidade de rede de acesso e a informação de associação.

[00339] Bloco **913**: A P-CSCF localiza a CLF de acordo com a identidade de rede de acesso na mensagem Register e a relação correspondente pré-regulada entre a CLF e a identidade de rede de acesso.

[00340] Bloco **914**: A P-CSCF consulta a CLF localizada no bloco **913** sobre a informação de anexação do UE na camada de acesso de acordo com a informação de associação na mensagem Register. Diferentemente da técnica relacionada, a CLF pré-armazena o registro de dados da informação de anexação correspondente à informação de associação, onde a informação de anexação inclui uma informação de endereço de IP, uma informação de localização, etc., mas não uma indicação em feixe na técnica relacionada. Caso não haja um registro de dados correspondente à informação de associação, a CLF retorna uma mensagem de falha de consulta para a P-CSCF.

[00341] Bloco **915**: A P-CSCF envia para a I-CSCF a mensagem Register portando o resultado de consulta no bloco **914** e o endereço

de IP de origem da mensagem Register recebida pela P-CSCF; se a consulta no bloco **914** for bem-sucedida, a P-CSCF enviará a informação de anexação para a I-CSCF; caso contrário, a P-CSCF reportará uma mensagem de falha de consulta para a I-CSCF.

[00342] Bloco **916**: A I-CSCF envia uma mensagem Cx-Query para a UPSF ou o HSS para determinar a S-CSCF para processamento da mensagem Register, isto é, a I-CSCF consulta a UPSF ou o HSS sobre a S-CSCF a qual foi atribuída para servir a este usuário. A UPSF ou o HSS retorna o nome de S-CSCF, o qual foi previamente selecionado no bloco **903** para a I-CSCF de acordo com a informação de indicação de S-CSCF armazenada no HSS.

[00343] Bloco **917**: A I-CSCF encaminha a mensagem Register portando o resultado de consulta e o endereço de IP de origem da mensagem Register recebida pela P-CSCF para a S-CSCF determinada no Bloco **916**. Se a consulta for bem-sucedida, o resultado de consulta será a informação de anexação; caso contrário, o resultado de consulta será a mensagem de falha de consulta reportada.

[00344] Bloco **918**: Caso o resultado de consulta seja a informação de anexação, a S-CSCF compara o endereço de IP de origem da mensagem Register recebida pela P-CSCF com o endereço de IP na informação de anexação consultada a partir da CLF. Caso o endereço de IP de origem da mensagem Register recebida pela P-CSCF seja consistente com o endereço de IP na informação de anexação consultada a partir da CLF, isto significa que a autenticação é bem-sucedida, prossegue-se para o Bloco **919**, isto é, envia-se uma mensagem de sucesso de autenticação para o UE; caso contrário, isto significa que a autenticação falhou, prossegue-se para o Bloco **931**, isto é, envia-se uma mensagem de falha de autenticação para o UE.

[00345] Caso o resultado de consulta seja a mensagem de falha de

consulta reportada, isto também significa que a autenticação falhou, prossegue-se para o Bloco **931**, isto é, envia-se a mensagem de falha de autenticação para o UE.

[00346] Bloco **919**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualização da informação de indicação de S-CSCF na UPSF ou no HSS e notificar a UPSF ou o HSS que ela(e) foi atribuída(o) para servir a este usuário.

[00347] Bloco **920**: A S-CSCF transfere (via download) o perfil de usuário a partir da UPSF ou do HSS através de uma mensagem Cx-Pull.

[00348] Bloco **921**: A S-CSCF envia uma mensagem 2xx Auth_OK para a I-CSCF indicando que a autenticação foi bem-sucedida.

[00349] Bloco **922**: A I-CSCF encaminha a mensagem 2xx Auth_OK para a P-CSCF.

[00350] Bloco **923**: A P-CSCF encaminha a mensagem 2xx Auth_OK para o UE.

[00351] Bloco **931**, conforme mostrado na Figura 12b, uma vez que a S-CSCF armazenou os dados de autenticação obtidos a partir da UPSF ou do HSS no Bloco 909 correspondente ao mecanismo de autenticação de AKA de IMS, a S-CSCF envia a mensagem 4xx Auth_Challenge portando a informação relacionada à autenticação de AKA de IMS para a I-CSCF.

[00352] Bloco **932**: A I-CSCF encaminha a mensagem 4xx Auth_Challenge para a P-CSCF.

[00353] Bloco **933**: após receber a mensagem 4xx Auth_Challenge, a P-CSCF determina que o parâmetro “algorithm” no cabeçalho WWW-Authenticate da mensagem 4xx Auth_Challenge indica que o mecanismo de autenticação é o IMS AKA, portanto, a P-CSCF não precisa estabelecer uma associação de segurança com o UE; a P-CSCF encaminha a mensagem 4xx Auth_Challenge para o UE.

[00354] Bloco **934**: após receber a mensagem 4xx Auth_Challenge, o UE determina que o parâmetro “algorithm” no cabeçalho WWW-Authenticate da mensagem 4xx Auth_Challenge indica que o mecanismo de autenticação é o IMS AKA, portanto, o UE precisa estabelecer uma associação de segurança com a P-CSCF; o UE envia uma mensagem Register portando o parâmetro de autenticação para a P-CSCF de novo.

[00355] Bloco **935**: A P-CSCF encaminha a mensagem Register do UE para a I-CSCF.

[00356] Bloco **936**: A I-CSCF envia uma mensagem Cx-Query para a UPSF ou o HSS para determinar a S-CSCF para processamento da mensagem Register, isto é, a I-CSCF consulta a UPSF ou o HSS sobre a S-CSCF a qual foi atribuída para servir a este usuário. A UPSF ou o HSS retorna o nome de S-CSCF, o qual foi previamente selecionado no bloco 903 para a I-CSCF de acordo com a informação de indicação de S-CSCF armazenada no HSS.

[00357] Bloco **937**: A I-CSCF encaminha a mensagem Register para a S-CSCF determinada no Bloco **926**.

[00358] A S-CSCF compara o parâmetro de autenticação obtido a partir da UPSF ou do HSS com o parâmetro de autenticação enviado pelo; caso o parâmetro de autenticação obtido a partir da UPSF ou do HSS seja consistente com o parâmetro de autenticação enviado pelo UE, isto significa que a autenticação foi bem-sucedida; caso contrário, isto significa que a autenticação falhou.

[00359] Bloco **938**: A S-CSCF envia uma mensagem Cx-Put para a UPSF ou o HSS para atualizar a informação de indicação de S-CSCF na UPSF ou no HSS e notificar o HSS que ele foi atribuído para servir a este usuário.

[00360] Bloco **939**: A S-CSCF transfere (via download) o perfil de usuário a partir da UPSF ou do HSS através de uma mensagem Cx-

Pull.

[00361] Bloco **940**: caso a autenticação seja bem-sucedida, a S-CSCF envia uma mensagem 2xx Auth_OK para a I-CSCF indicando que o registro é bem-sucedido, onde 2xx indica que a mensagem é relevante para sucesso, e xx é um número em 00~99; caso a autenticação tenha falhado, a S-CSCF envia uma mensagem de falha de autenticação a I-CSCF.

[00362] Bloco **941**: A I-CSCF encaminha a mensagem 2xx Auth_OK ou a mensagem de falha de autenticação para a P-CSCF.

[00363] Bloco **942**: A P-CSCF encaminha a mensagem 2xx Auth_OK ou a mensagem de falha de autenticação para o UE.

[00364] Com respeito à segunda modalidade, o método da nona modalidade pode ser modificado correspondentemente de acordo com a diferença entre a segunda modalidade e a primeira modalidade, o que não será repetido aqui.

[00365] A descrição precedente é apenas das modalidades preferidas da presente invenção e não é para uso na limitação do escopo de proteção da mesma. Todas as modificações, substituições equivalentes ou melhoramentos no escopo do espírito e nos princípios da presente invenção devem ser incluídos no escopo de proteção da presente invenção.

REIVINDICAÇÕES

1. Método de autenticação em um Subsistema Multimídia IP (IMS) que compreende:

após receber uma mensagem de Registro do Equipamento do Usuário (EU), localizar, através de uma Função de Controle de Sessão Proxy-Chamada (P-CSCF), uma Função de Localização de Conexão (CLF) de acordo com informação contida na mensagem de Registro e uma relação pré-configurada correspondente entre a informação contida na mensagem de Registro e o CLF, **caracterizado pelo fato de que** ainda compreende:

obter, através da P-CSCF, um resultado inquirido através da inquirição do CLF sobre informação de anexo do UE em uma rede de acesso, e enviar a mensagem de Registro transportando o resultado inquirido para uma Função de Controle de Sessão de Interrogação-Chamada (I-CSCF);

encaminhar, através da I-CSCF, a mensagem de Registro transportando o resultado inquirido para uma Função de Controle de Sessão de Serviço-Chamada (S-CSCF);

autenticar, através da S-CSCF, o UE de acordo com o resultado inquirido e um mecanismo de autenticação obtido a partir de um Servidor do Assinante (HSS), e enviar um resultado de autenticação para o UE.

2. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** a informação contida na mensagem de Registro é uma identidade de rede de acesso ou um endereço IP de origem da mensagem de Registro.

3. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** a mensagem de Registro compreende informação de associação do UE na rede de acesso; e a CLF pré-armazena a informação de conexão do UE na rede de acesso correspondente à

informação de associação;

inquirir a CLF sobre a informação de conexão NASS do UE em uma rede de acesso para obter um resultado inquirido que compreende:

inquirir, através da P-CSCF, a CLF sobre a informação de conexão do UE na rede de acesso de acordo com a informação de associação;

se existe informação de conexão do UE na rede de acesso que contem um endereço IP correspondente à informação de associação, retornar, através da CLF, o resultado inquirido que compreende o endereço IP para a P-CSCF; se não, retornar o resultado inquirido indicando que a inquirição falhou para a P-CSCF.

4. Método, de acordo com a reivindicação 1 ou 3, **caracterizado pelo fato de** que enviar a mensagem de Registro transportando o resultado inquirido para uma I-CSCF ainda compreende:

enviar, através da P-CSCF, um endereço IP de origem da mensagem de Registro para a I-CSCF;

encaminhar a mensagem de Registro transportando o resultado inquirido para uma S-CSCF ainda compreende:

encaminhar, através da I-CSCF, o endereço IP de origem da mensagem de registro para a S-CSCF;

autenticar o UE de acordo com um mecanismo de autenticação obtido do HSS que compreende:

se o resultado inquirido compreende um endereço IP, comparar, através da S-CSCF, o endereço IP de origem da mensagem de Registro recebida pela P-CSCF com o endereço IP no resultado inquirido; se o endereço IP de origem da mensagem de registro recebida pela P-CSCF é coerente com o endereço IP no resultado inquirido, indica que a autenticação obteve sucesso; se não, indica que

a autenticação falhou.

5. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** a informação de associação do UE na rede de acesso correspondente à um endereço IP de origem da mensagem de Registro é pré-armazenada na CLF; e

inquirir a CLF sobre a informação de conexão do UE em uma rede de acesso para obter um resultado inquirido que compreende:

inquirir, através da P-CSCF, a CLF, sobre a informação de associação de acordo com o endereço IP de origem da mensagem de Registro;

se existe informação de associação correspondente ao endereço IP de origem da mensagem de Registro na CLF, retornar, através da CLF, o resultado inquirido compreendendo a informação de associação para a P-CSCF; se não, retornar através da CLF, o resultado inquirido indicando que a inquirição falhou para a P-CSCF.

6. Método, de acordo com a reivindicação 1 ou 5, **caracterizado pelo fato de que** ainda compreende:

antes de autenticar o UE de acordo com um mecanismo de autenticação obtido a partir do HSS, obter, através da S-CSCF, informação de associação pré-armazenada no HSS; e

autenticar o UE de acordo com um mecanismo de autenticação obtido a partir do HSS que compreende:

se o resultado inquirido compreende informação de associação do UE na rede de acesso, comparar, através da S-CSCF, a informação de associação obtida a partir do HSS com a informação de associação no resultado inquirido; se a informação de associação obtida a partir do HSS é coerente com a informação de associação no resultado inquirido, indica que a autenticação obteve sucesso; se não, indica que a autenticação falhou.

7. Método, de acordo com a reivindicação 6, **caracterizado pelo fato de que** a informação de associação é a identidade do usuário de acesso ou informação de localização.

8. Método, de acordo com a reivindicação 1, **caracterizado pelo fato de que** a autenticação de UE de acordo com um mecanismo de autenticação obtido a partir do HSS compreende:

armazenar, através da S-CSCF, um primeiro mecanismo de autenticação da autenticação IMS combinada com NASS e dados de autenticação correspondente obtidos a partir do HSS, e um segundo mecanismo de autenticação e dados de autenticação correspondente ao segundo mecanismo de autenticação; e

autenticar, através da S-CSCF, o UE através da autenticação IMS combinada com NASS para obter um primeiro resultado de autenticação; se a autenticação obtiver sucesso, enviar o primeiro resultado de autenticação para o UE; se não; autenticar, através da S-CSCF, o UE através do segundo mecanismo de autenticação para obter um segundo resultado de autenticação, e enviar o segundo resultado de autenticação para o UE.

9. Método, de acordo com a reivindicação 8, **caracterizado pelo fato de que** o mecanismo de autenticação obtido a partir do HSS compreende: a autenticação IMS combinada com NASS, e o segundo mecanismo de autenticação o qual é adotado quando a autenticação IMS combinada com NASS falha.

10. Método, de acordo com a reivindicação 8, **caracterizado pelo fato de que** o segundo mecanismo de autenticação é HTTP DIGEST.

11. Método, de acordo com a reivindicação 10, **caracterizado pelo fato de que** autenticar o UE de acordo com um mecanismo de autenticação obtido a partir do HSS e enviar um resultado de autenticação para o UE compreende:

enviar, através da S-CSCF, uma mensagem de contestação que compreende o mecanismo de autenticação HTTP DIGEST para o UE;

após receber a mensagem de contestação que compreende o mecanismo de autenticação HTTP DIGEST, enviar, através do UE, uma mensagem de registro que compreende um parâmetro de autenticação para a S-CSCF;

autenticar, através da S-CSCF, o UE através do mecanismo HTTP DIGEST; se o mecanismo de autenticação obtiver sucesso, enviar, através da S-CSCF, uma mensagem de sucesso de autenticação para o UE; se não, enviar através da S-CSCF uma mensagem de falha de autenticação para o UE.

12. Método, de acordo com a reivindicação 8, **caracterizado pelo fato de que** o segundo mecanismo de autenticação é IMS AKA.

13. Método, de acordo com a reivindicação 12, **caracterizado pelo fato de que** autenticar o UE de acordo com um mecanismo de autenticação obtido a partir do HSS e enviar um resultado de autenticação para o UE compreende:

enviar, através da S-CSCF, uma mensagem de contestação contendo o mecanismo de autenticação IMS AKA para o UE;

após receber a mensagem de contestação contendo o mecanismo de autenticação IMS AKA, enviar, através do UE, uma mensagem de Registro que compreende um parâmetro de autenticação para a S-CSCF;

autenticar, através da S-CSCF, o UE através do mecanismo de autenticação IMS AKA; se o mecanismo de autenticação obtiver sucesso, enviar, através da S-CSCF, uma mensagem de sucesso de autenticação para o UE; se não, enviar,

através da S-CSCF, uma mensagem de falha de autenticação para o UE.

14. Método, de acordo com a reivindicação 1 ou 8, **caracterizado pelo fato de que** ainda compreende:

antes de localizar uma CLF de acordo com informação contida na mensagem de Registro e uma relação pré-configurada correspondente entre a informação contida na mensagem de Registro e a CLF,

enviar, através do UE, uma mensagem de Registro para a S-CSCF;

requisitar, através da S-CSCF, dados de autenticação do UE a partir do HSS ;

enviar, através do HSS, o mecanismo de autenticação para a S-CSCF de acordo com o perfil de usuário pré-configurado;

enviar, através da S-CSCF, uma mensagem que compreende o mecanismo de autenticação para o UE;

após receber a mensagem que compreende o mecanismo de autenticação, enviar, através do UE, outra mensagem de Registro para a P-CSCF.

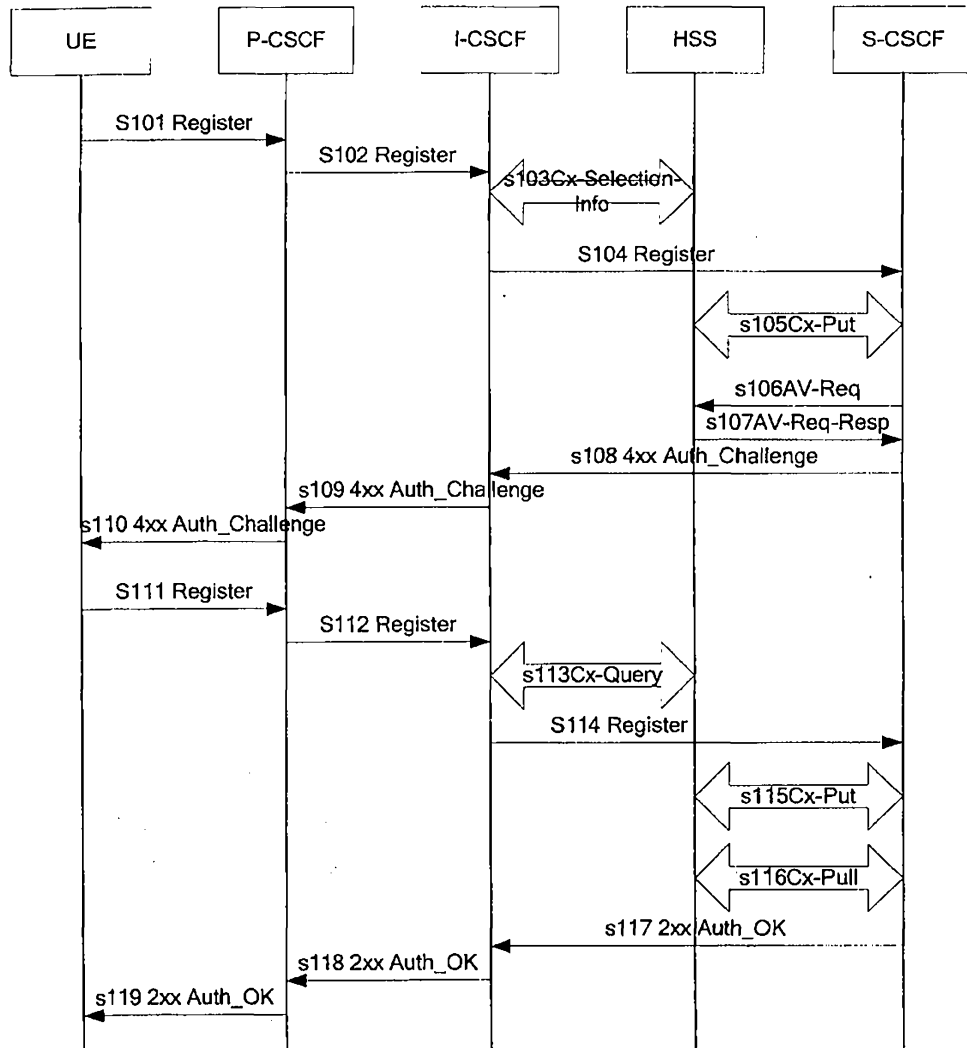


Fig. 1

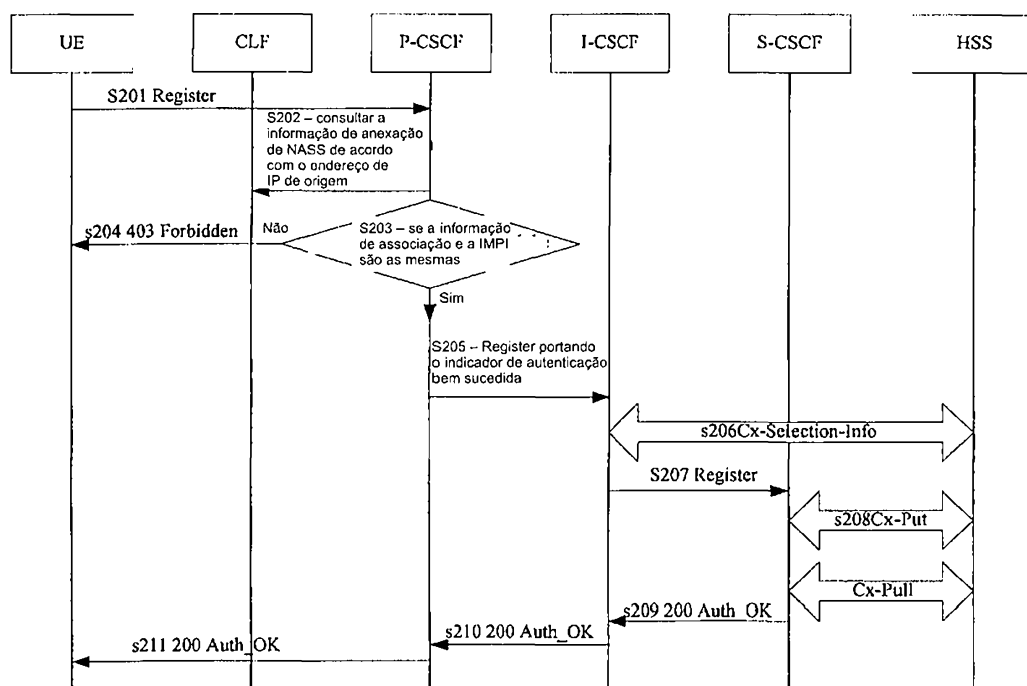


Fig. 2

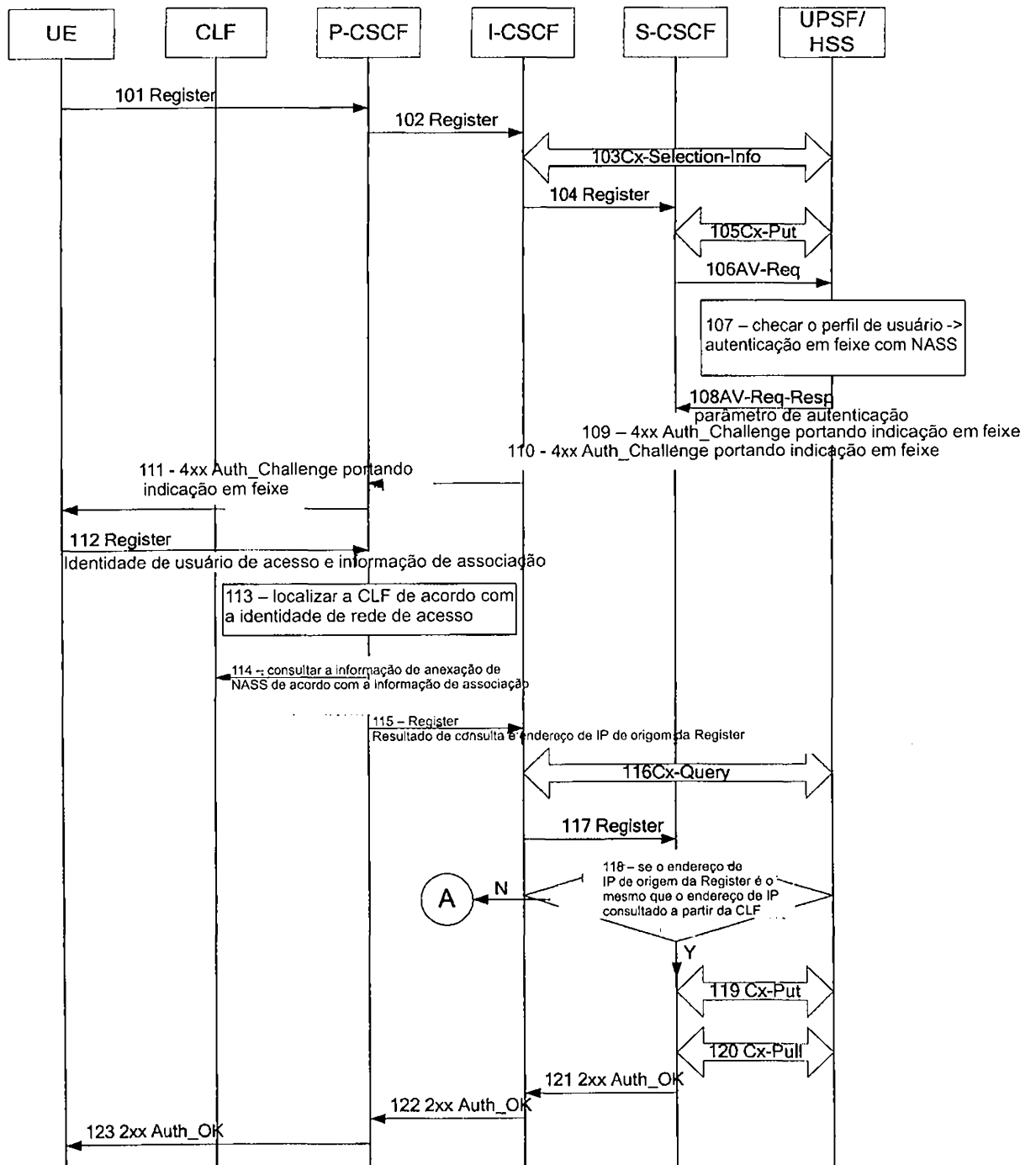


Fig. 3a

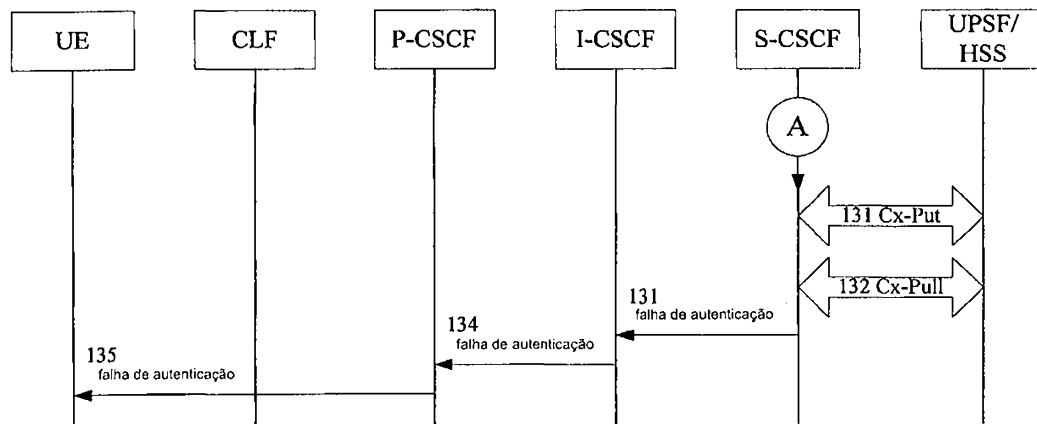


Fig. 3b

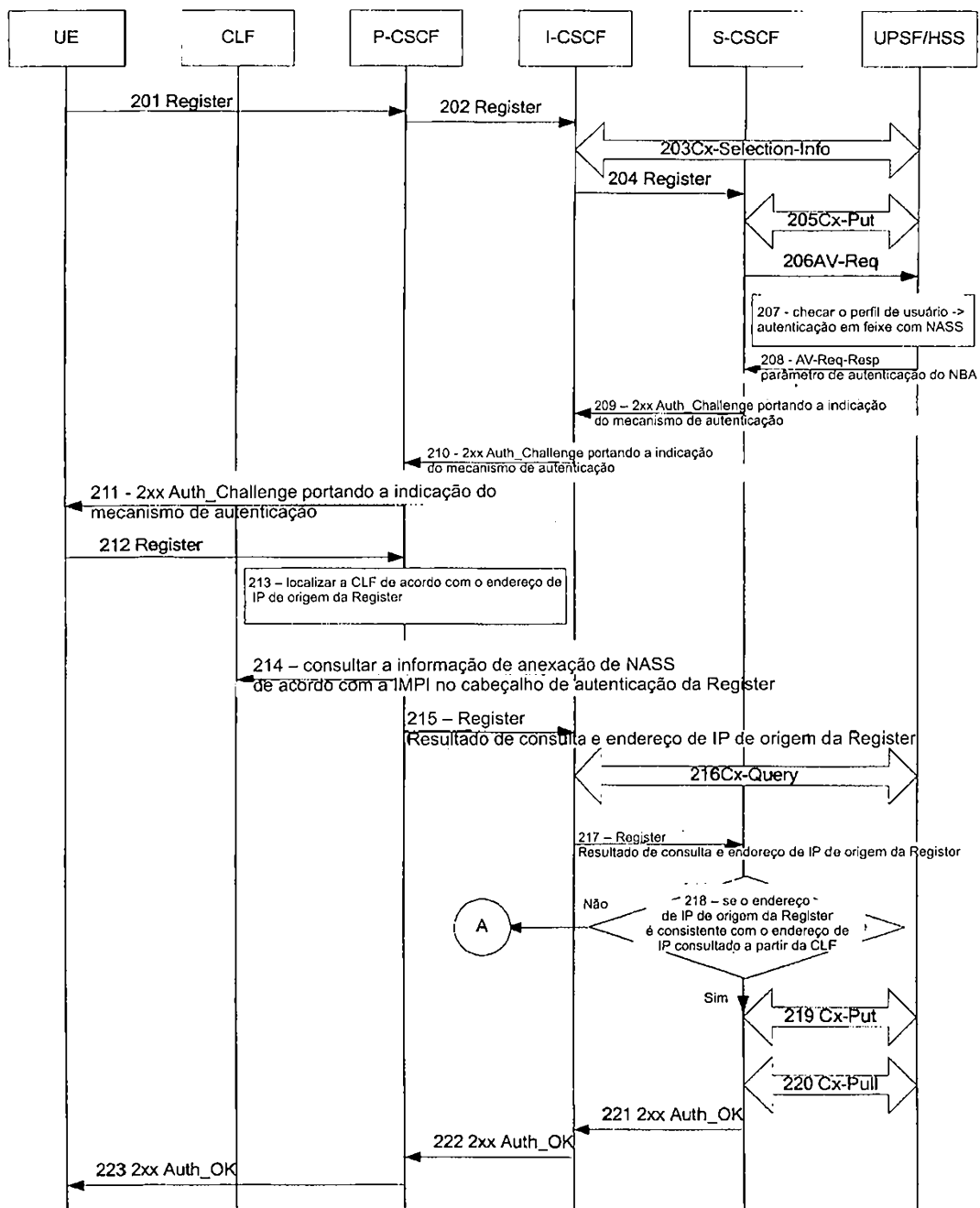


Fig. 4a

160

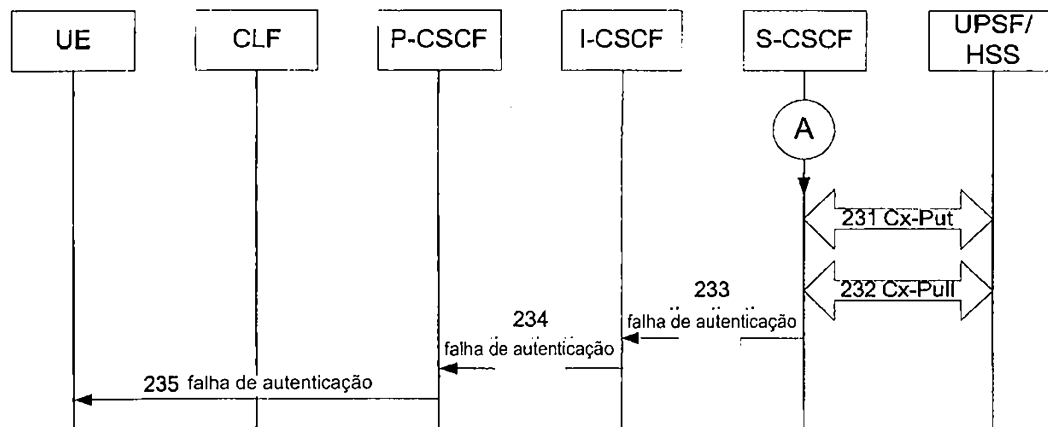


Fig. 4b

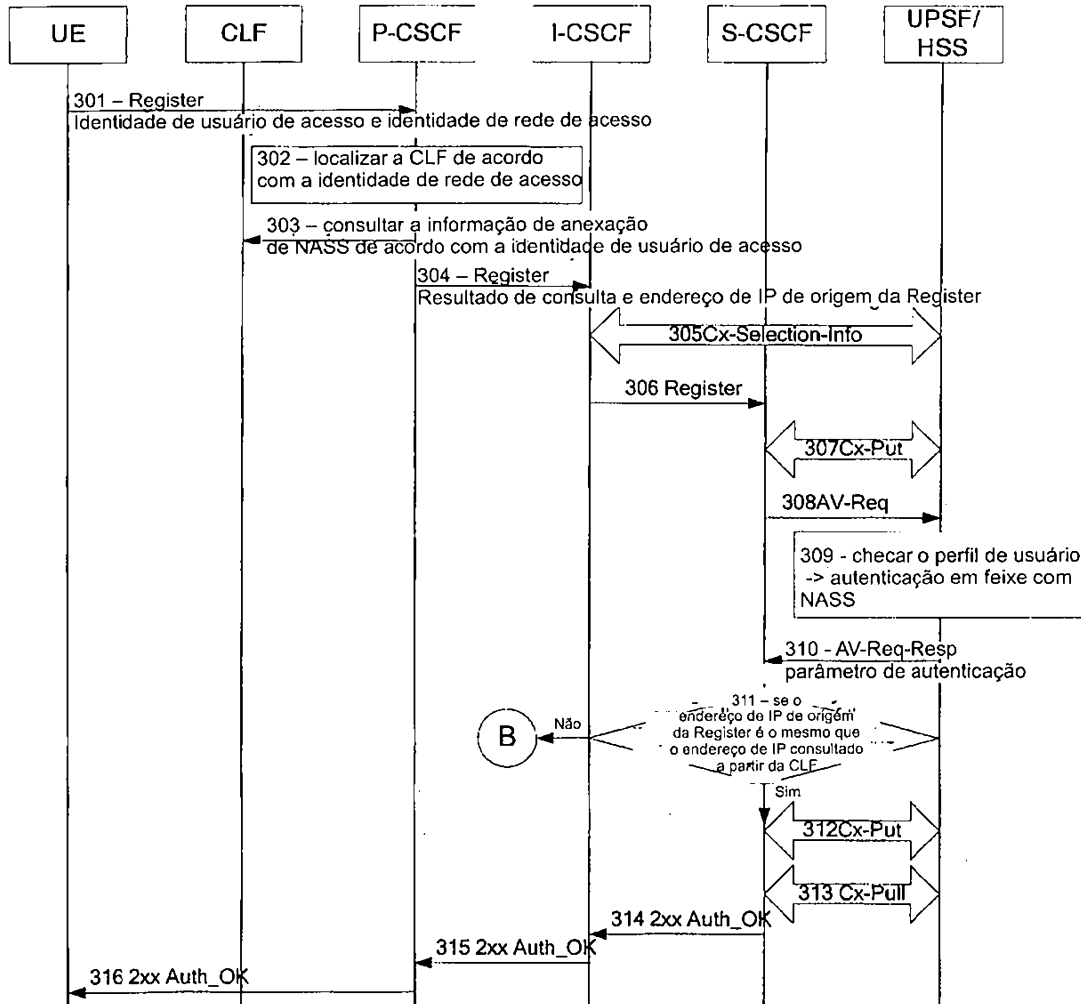


Fig. 5a

113
f

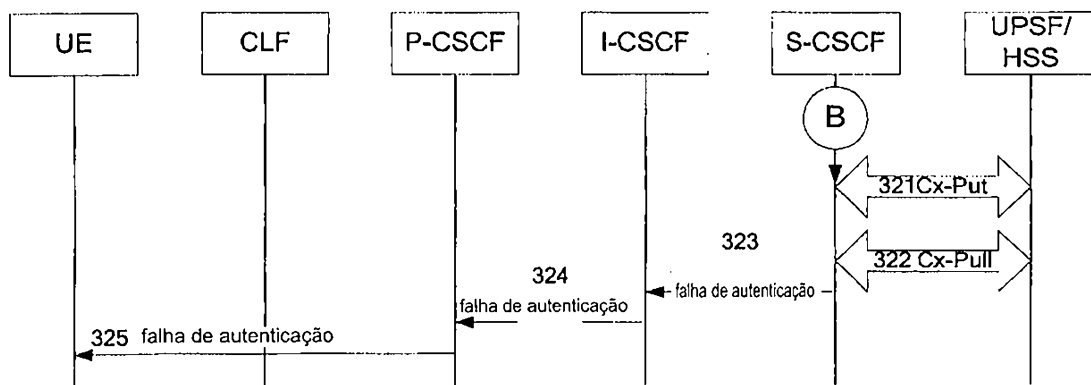


Fig. 5b

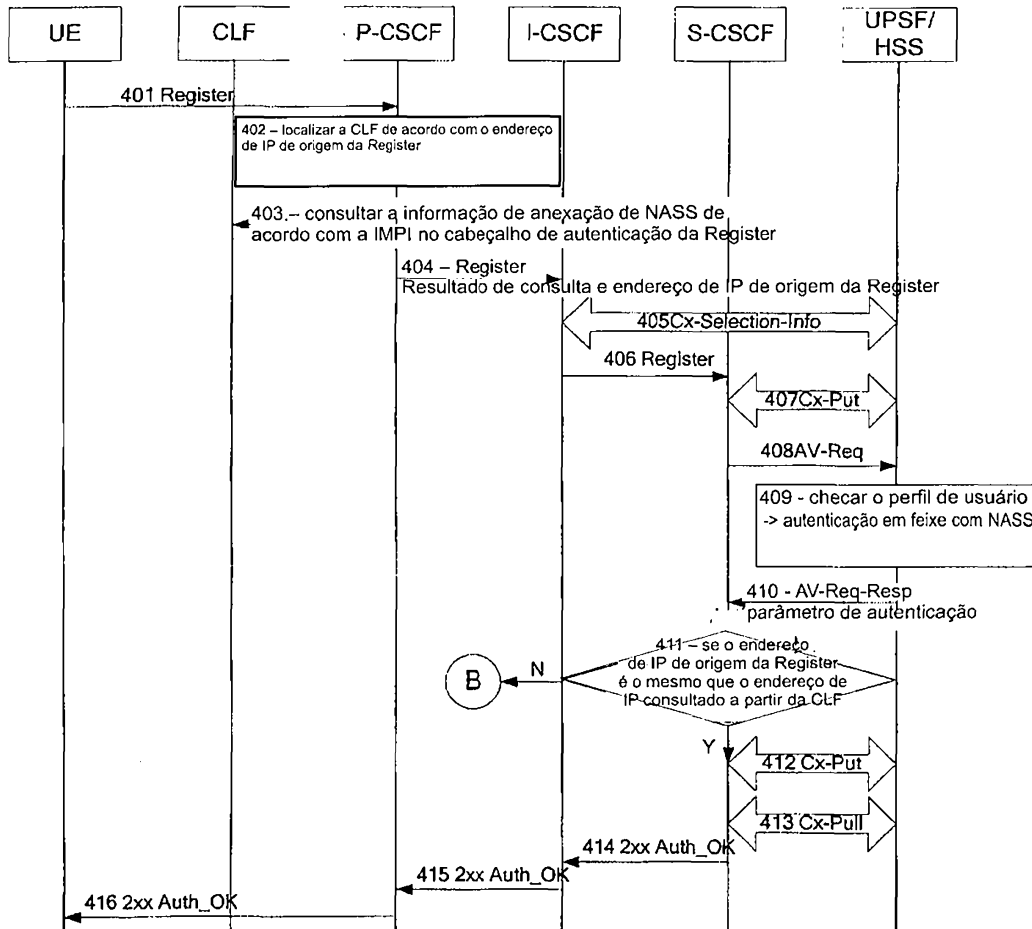


Fig. 6a

169.

10/21

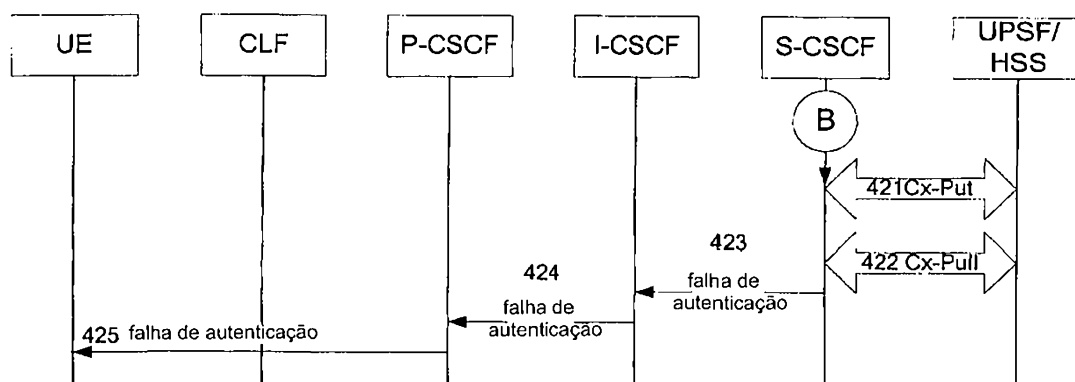


Fig. 6a

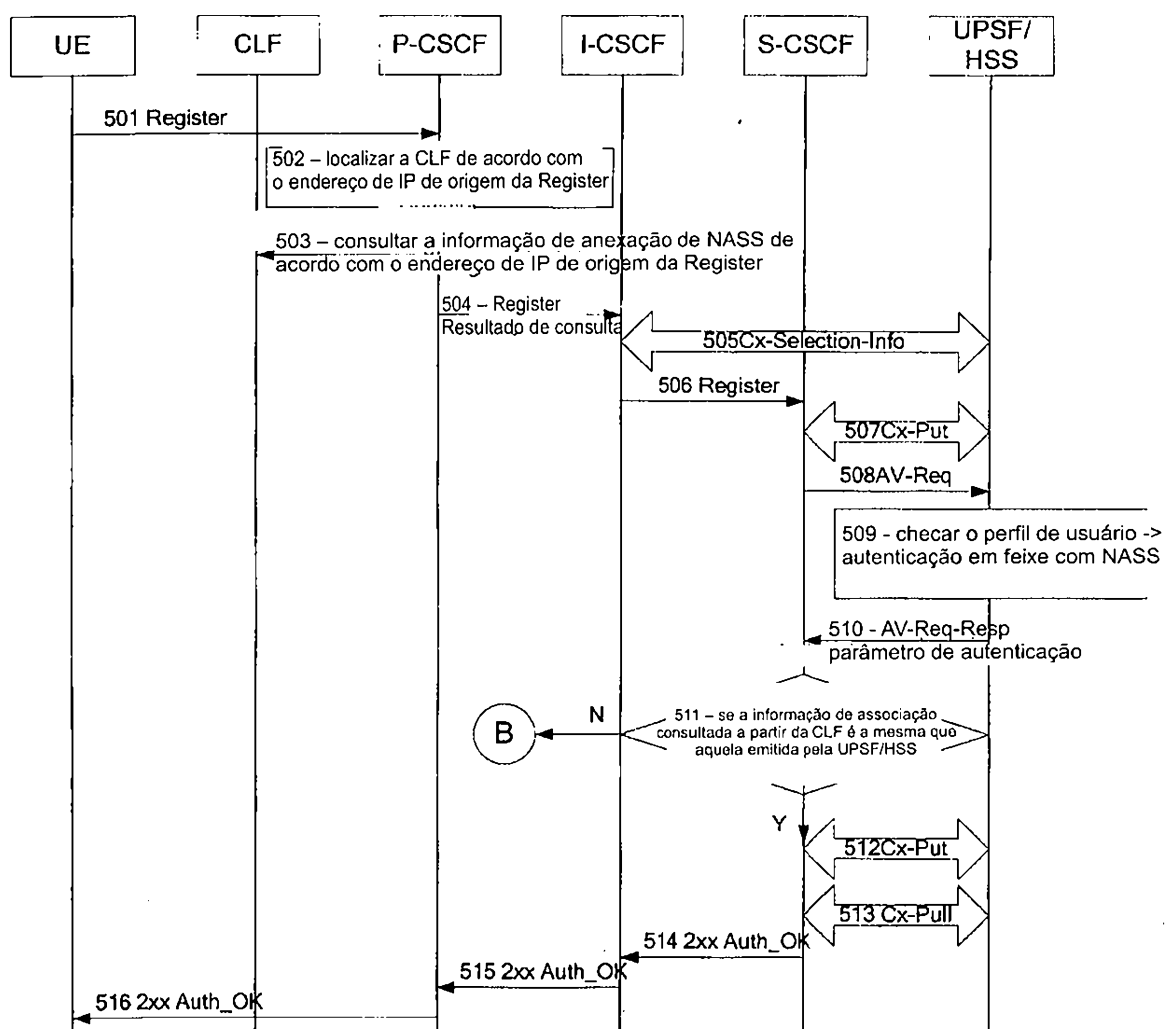


Fig. 7a

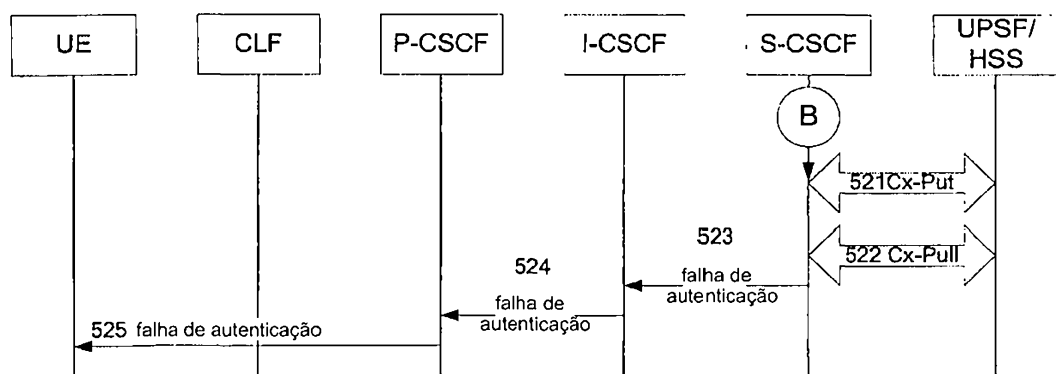


Fig. 7b

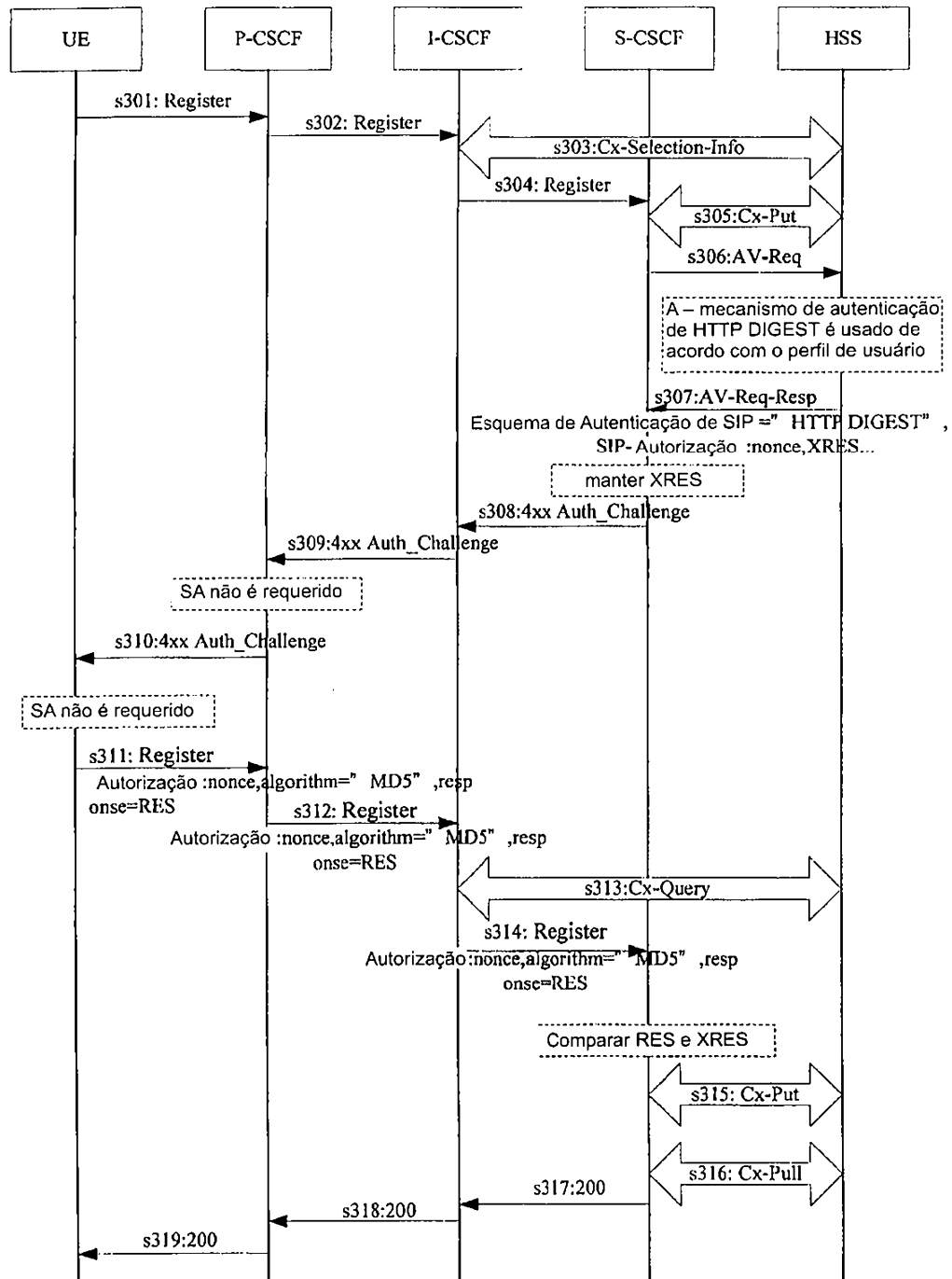


Fig. 8

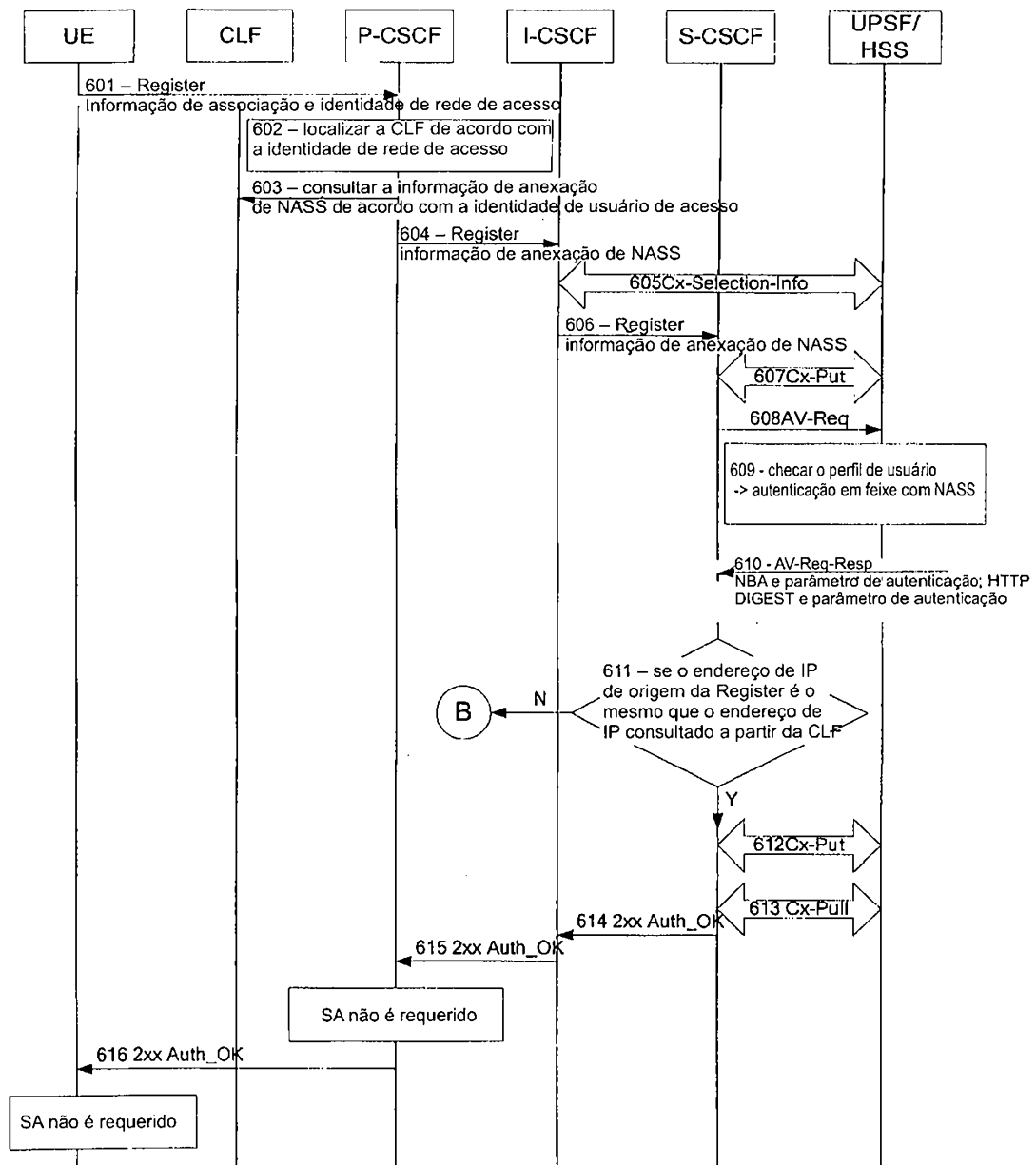


Fig. 9a

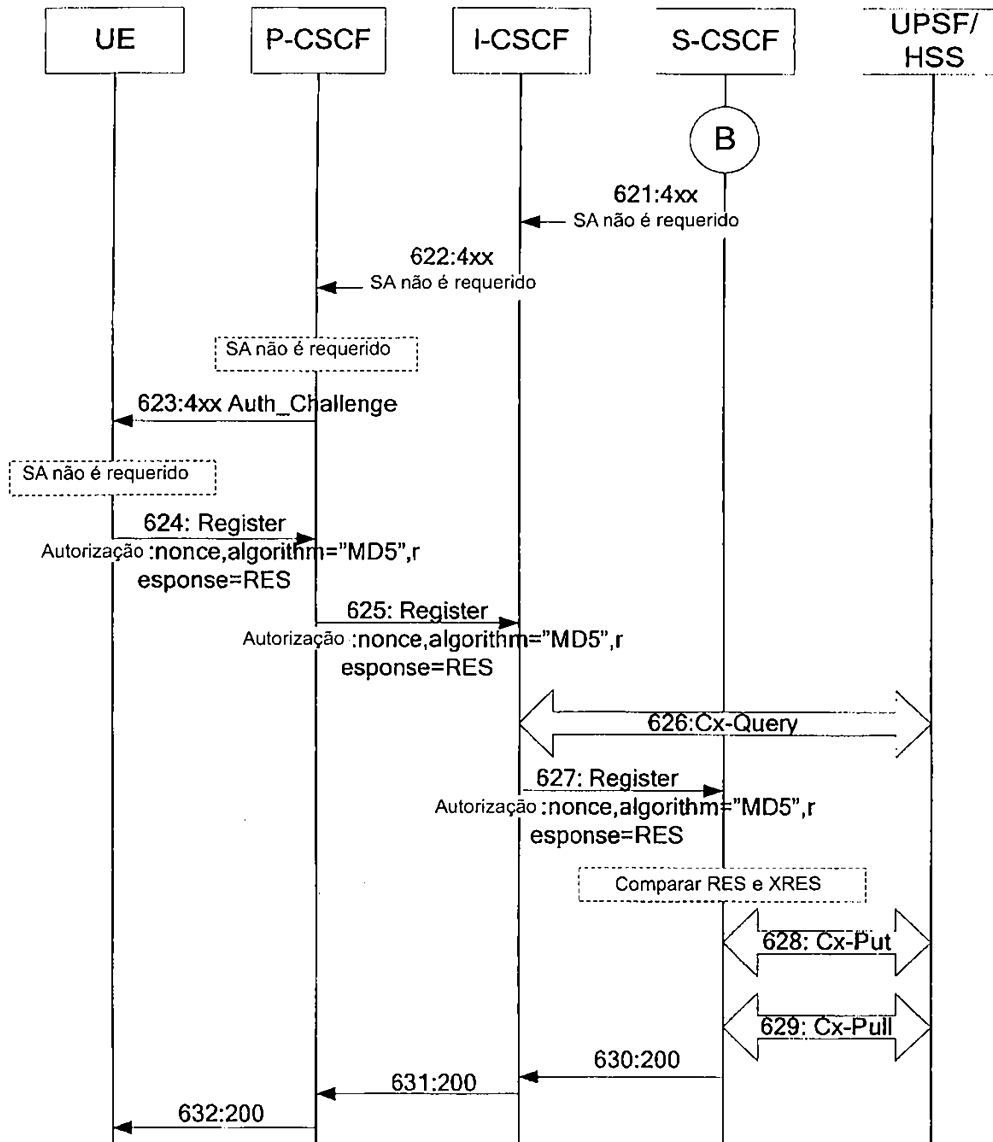


Fig. 9b

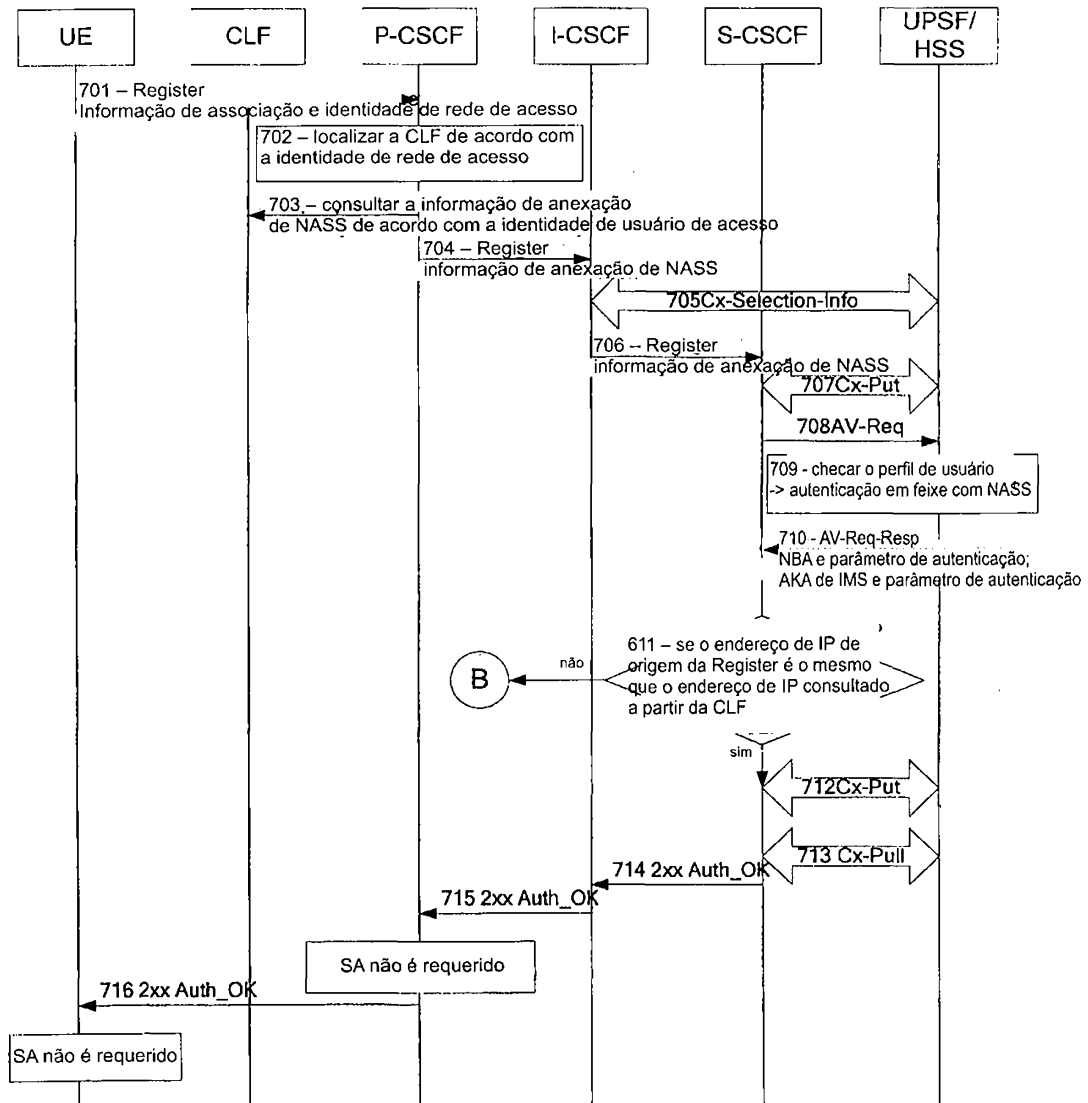


Fig. 10a

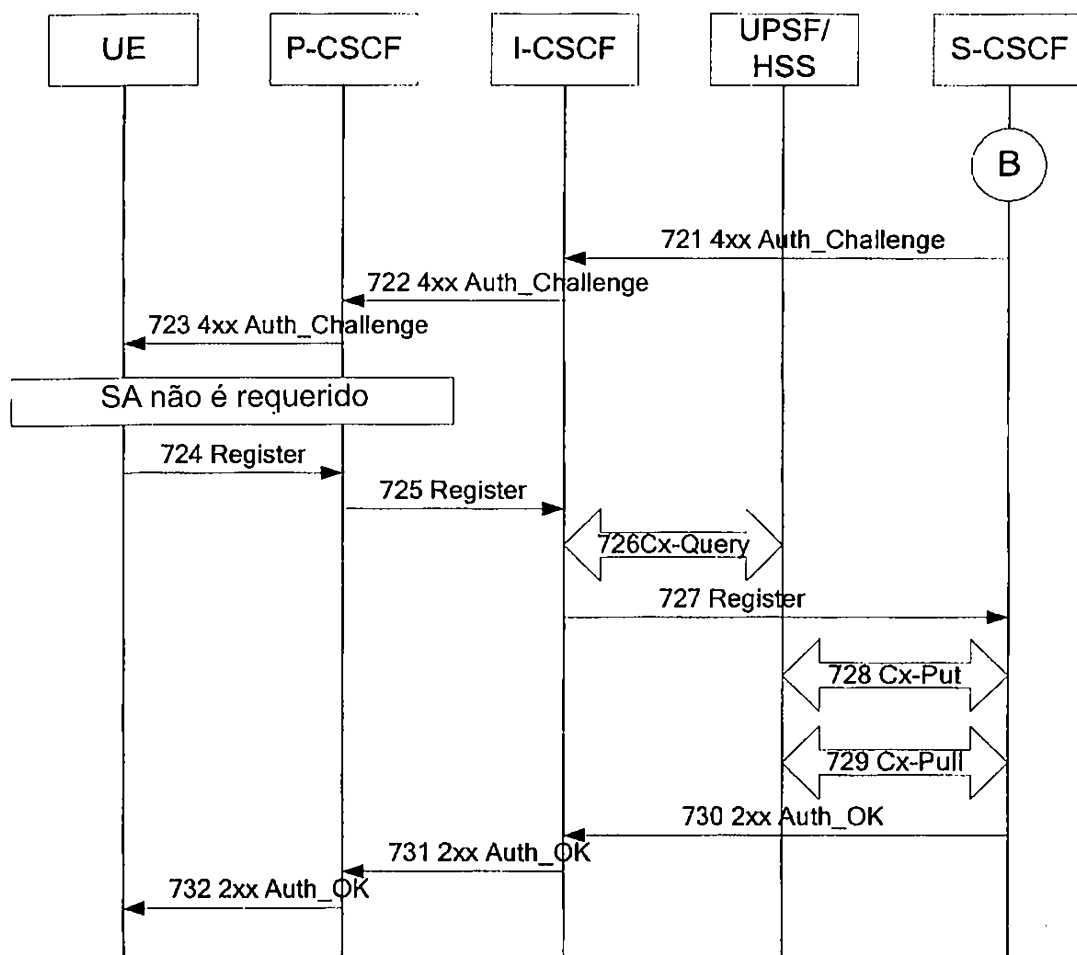
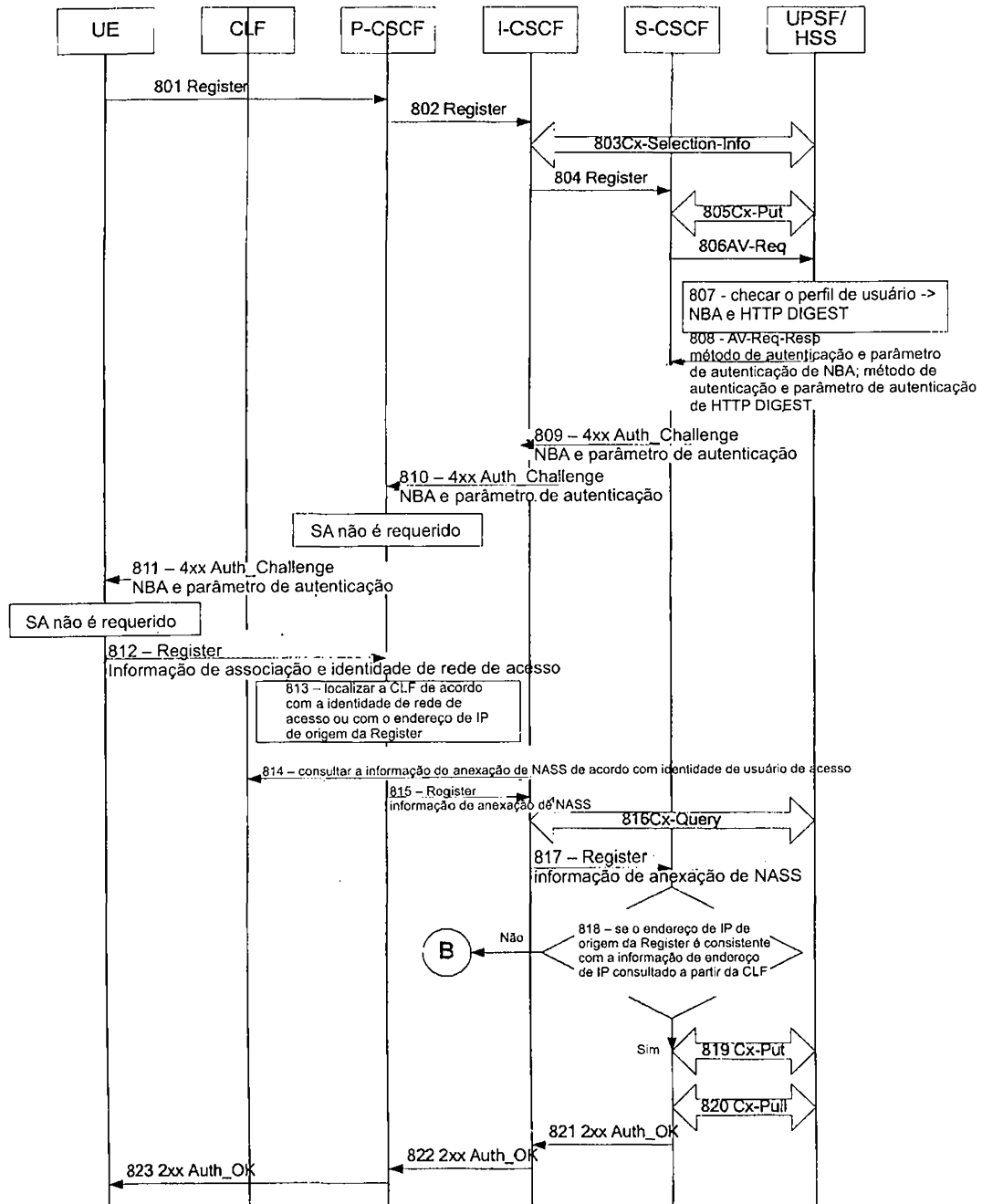


Fig. 10b



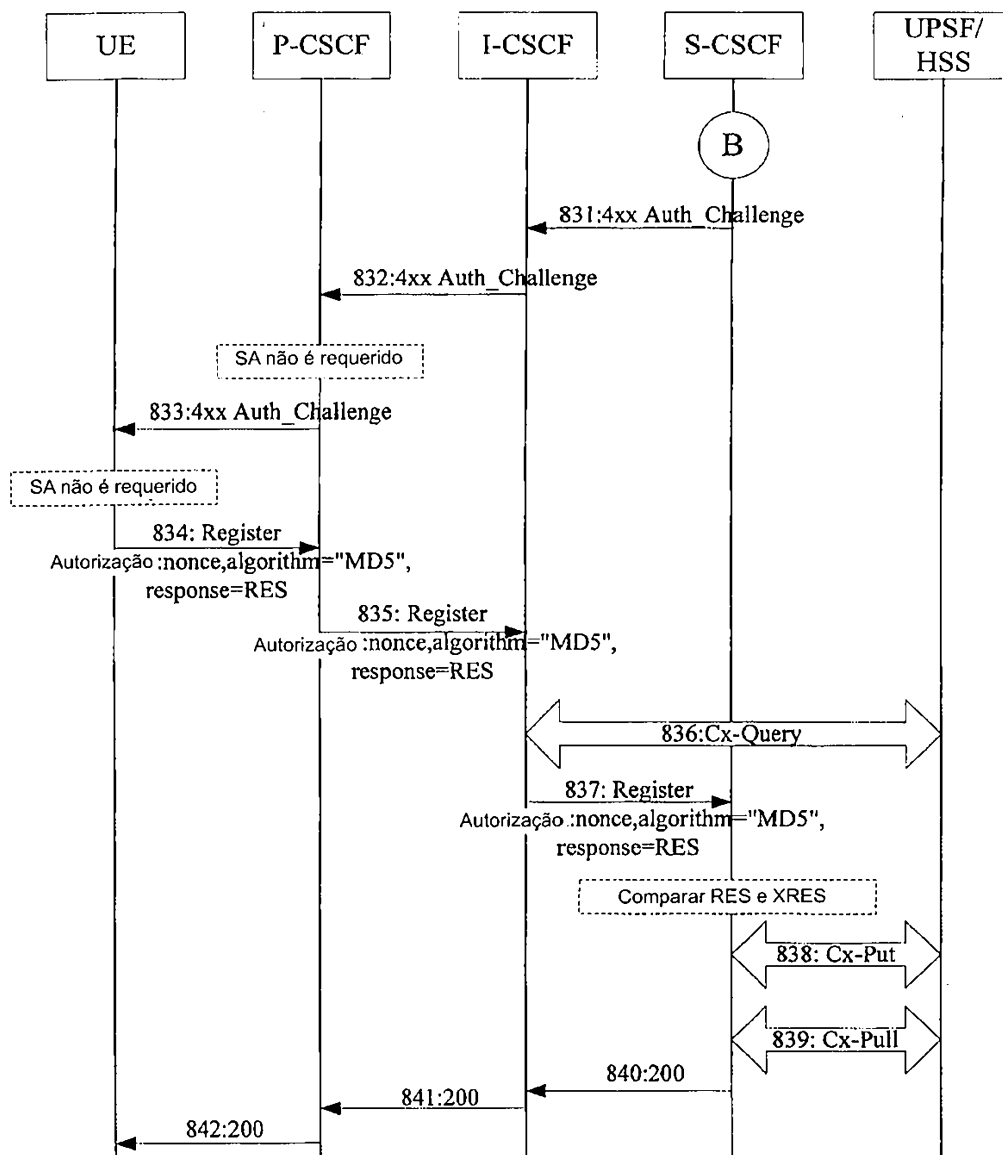


Fig. 11b

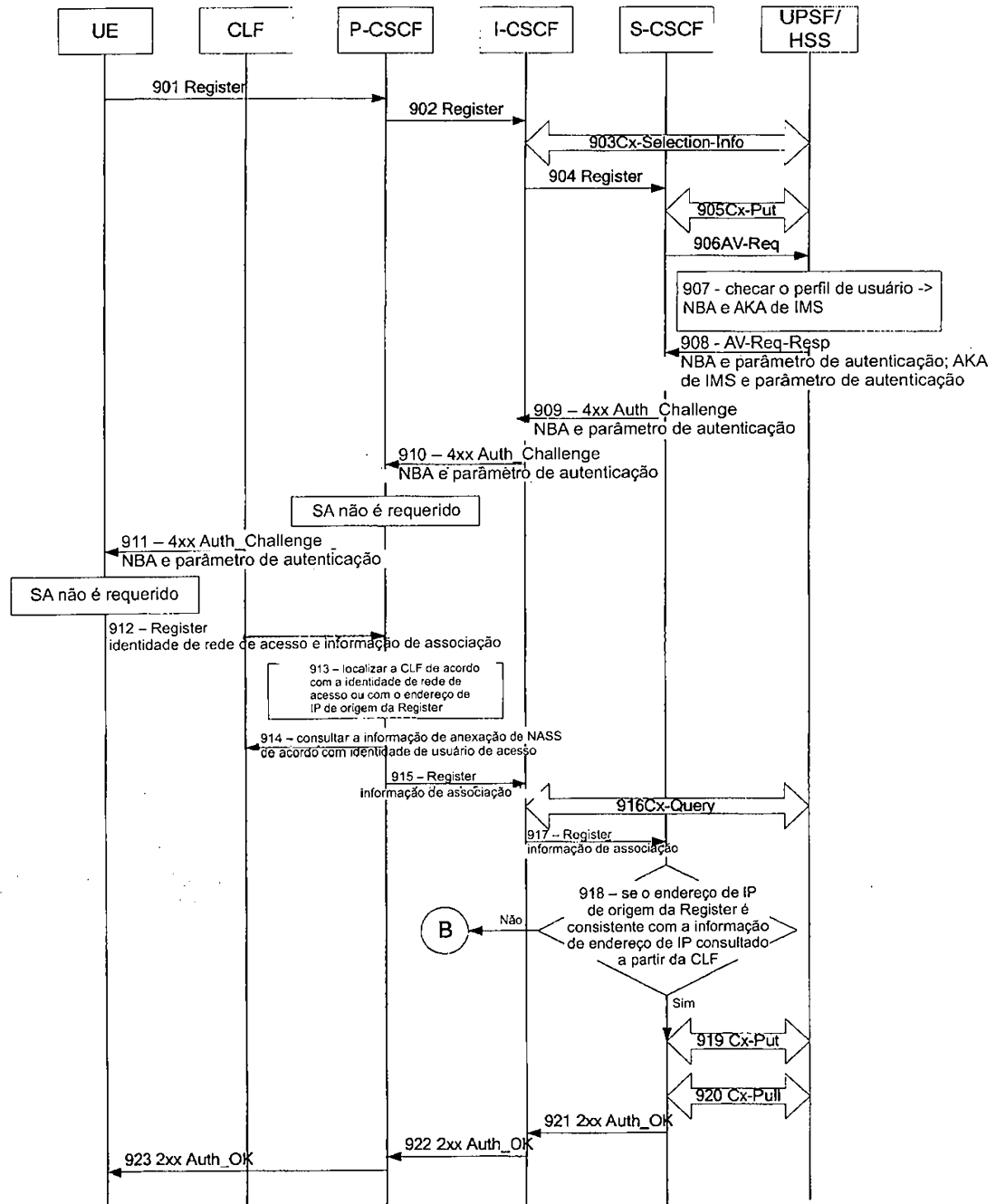


Fig. 12a

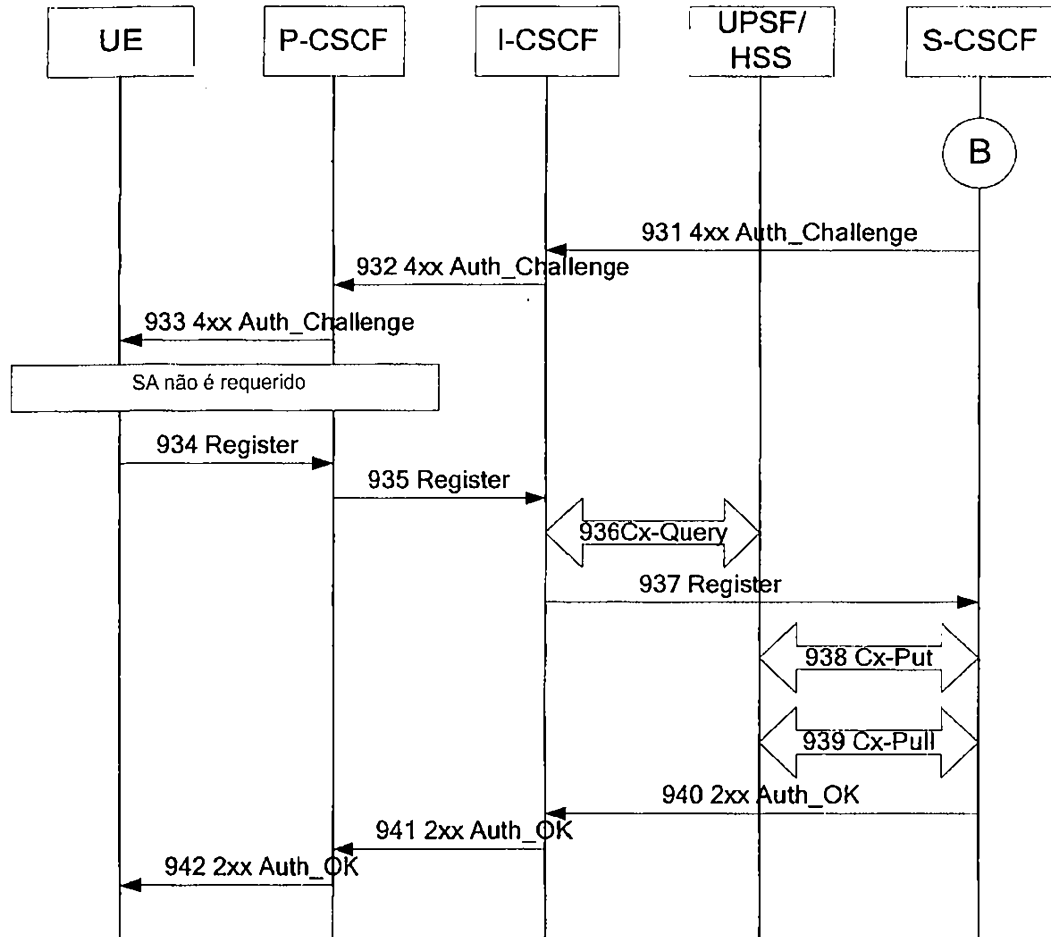


Fig. 12b