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

(21) **PI 0622025-8 A2**

*BRPI0622025A2*

(22) Data de Depósito: 26/09/2006
**(43) Data da Publicação: 20/12/2011**
**(RPI 2137)**

***(51) Int.Cl.:***
**H04L 12/24**
**H04W 12/08**
**H04W 8/08**

**(54) Título:** ARQUITETURA DE CONTROLE DE POLÍTICA, CONTROLADORES DE POLÍTICA INDEPENDENTE, DE POLÍTICA DE USUÁRIO, E DE POLÍTICA DE NEGÓCIO, MÉTODOS EM UM TERMINAL DE USUÁRIO DE LANÇAR O SERVIÇO EM UMA PRIMEIRA REDE DE ORIGEM E DE LANÇAR O MENCIONADO SERVIÇO EM UMA SEGUNDA REDE, E, MÉTODOS EM UM PROVEDOR DE IDENTIDADE INDEPENDENTE, EM UM CONTROLADOR DE POLÍTICA DE USUÁRIO, EM UM CONTROLADOR DE POLÍTICA DE NEGÓCIO, EM UM CONTROLADOR DE POLÍTICA DE SERVIÇO E EM UM CONTROLADOR DE POLÍTICA DE REDE

**(73) Titular(es):** Telefonaktiebolaget LM Ericsson

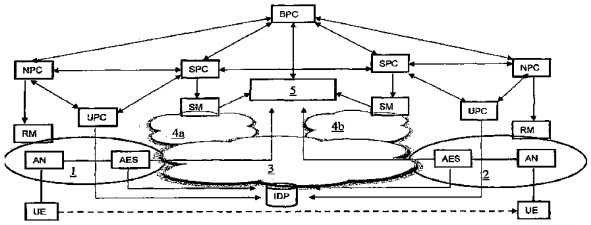
**(72) Inventor(es):** Wei Zhao

**(74) Procurador(es):** Momsen, Leonardos & Cia

**(86) Pedido Internacional:** PCT SE2006001093 de 26/09/2006

**(87) Publicação Internacional:** WO 2008/039114de 03/04/2008

**(57) Resumo:** ARQUITETURA DE CONTROLE DE POLÍTICA, CONTROLADORES DE POLÍTICA INDEPENDENTE, DE POLÍTICA DE USUARIO, E DE POLÍTICA DE NEGÓCIO, METODOS EM UM TERMINAL DE USUARIO DE LANÇAR O SERVIÇO EM UMA PRIMEIRA REDE DE ORIGEM E DE LANÇAR O MENCIONADO SERVIÇO EM UMA SEGUNDA REDE, E, METODOS EM UM PROVEDOR DE IDENTIDADE INDEPENDENTE, EM UM CONTROLADOR DE POLÍTICA DE USUARIO, EM UM CONTROLADOR DE POLÍTICA DE NEGÓCIO, EM UM CONTROLADOR DE POLÍTICA DE SERVIÇO E EM UM CONTROLADOR DE POLÍTICA DE REDE. Arquitetura de controle de política arranjada para tratar políticas em redes de comunicação, a arquitetura compreendendo um Provedor de Identidade independente (IDP) arranjado para gerar entradas de terminal de usuário do IDP para informação de controle de política. Ela ainda compreende ainda compreende controladores de política de modo lógico dividido em unidades de controle de política separadas incluindo um Controlador de Política de Usuário (UPC) arranjado para gerar entradas de terminal de usuário do UPC para subscrição de serviços e um controlador de política de Negócios (BPC) arranjado para aplicar políticas relacionadas ao negócios nos mencionados serviços.



"ARQUITETURA DE CONTROLE DE POLÍTICA, CONTROLADORES DE POLÍTICA INDEPENDENTE, DE POLÍTICA DE USUÁRIO, E DE POLÍTICA DE NEGÓCIO, MÉTODOS EM UM TERMINAL DE USUÁRIO DE LANÇAR O SERVIÇO EM UMA PRIMEIRA REDE DE ORIGEM E DE LANÇAR O MENCIONADO SERVIÇO EM UMA SEGUNDA REDE, E, MÉTODOS EM UM PROVEDOR DE IDENTIDADE INDEPENDENTE, EM UM CONTROLADOR DE POLÍTICA DE USUÁRIO, EM UM CONTROLADOR DE POLÍTICA DE NEGÓCIO, EM UM CONTROLADOR DE POLÍTICA DE SERVIÇO E EM UM CONTROLADOR DE POLÍTICA DE REDE"

CAMPO TÉCNICO

A presente invenção se refere à arquitetura de controle de política possibilitando descoberta de controlador de política entre diferentes tipos de redes de acesso, em particular para suportar deslocamento. A presente invenção também se refere à um Provedor de Identidade independente, um Controlador de Política de Usuário e um controlador de política de Negócios para a mencionada arquitetura de controle de política, assim como para métodos em um terminal de usuário, em um provedor de identidade, em um Controlador de Política de Usuário , em um controlador de política de Negócio, em um controlador de política de Serviço em um controlador de política de Rede dentro de tal Arquitetura de controle de política .

FUNDAMENTOS

A integração de tecnologias de linha com fio e sem fio de modo a criar uma base de rede de telecomunicação comum pode ser referida como Convergência Fixa e Móvel, FMC, possibilitando aos provedores de serviço de linha com fio e operadores de rede sem fio usarem a mesma infra-estrutura física, envolvendo várias vantagens para os usuários finais, assim como para os provedores de serviço e operadores. Um usuário final pode

acessar serviços de linhas com fio e sem fio através do mesmo terminal de usuário, tal como um telefone de comunicação móvel ou um computador pessoal, e serviços de comunicação móvel e fixa podem ser oferecidos ao usuário final em um pacote.

Dentro do campo técnico relacionado à FMC, a arquitetura de controle de política executa um papel vital, e. g. com relação à suporte de deslocamento e QoS (Qualidade of Serviço). Correntemente, um objeto de vários organismos de padronização, tal como o item de trabalho 3GPP PCC, o Tispan RACS, o WiMax Forum e o DSL Forum são para concordar com uma especificação de arquitetura de controle de política, fornecer Arquitetura de controle de política comum que seja aplicável independente do tipo de rede de acesso. Contudo, vários problemas tecnológicos ainda necessitam ser resolvidos, o mapeamento e alinhamento estão longe de estarem completos, e as organizações diferentes propõem soluções diferentes. O TISPAN e o DSL Forum (DSLF) ambos, têm um foco no lado de acesso fixo, que tipicamente é mais influenciado pelo assim chamado conceito de " igualdade de acesso ". Por conseguinte, eles propõem Arquitetura de controle de política distribuída, enquanto o 3GPP (3rd Generation Partnership Project) , que se refere à redes de acesso de rádio, preferem Arquitetura de controle de política mais fechada, já que os operadores de comunicação móvel/celular convencionalmente preferem dar serviços principalmente para seus próprios assinantes. Por exemplo, no DSLF, um PDP (ponto de decisão de política) é separado em três partes, um SPC (controlador de política de serviço), um NPC (controlador de política de rede) e a UPC (controlador de política de usuário) , enquanto as funções de controle da política normalmente são estreitamente acopladas no 3GPP, e. g. de acordo com as PCRF (Funções de Regras de Cobrança e Política combinadas), que permite regras de gerenciamento de resposta de fluxo de serviço, de passagem, QoS e fluxo baseado na cobrança independentemente da tecnologia

de acesso de assinante.

Contudo, de modo a permitir um usuário final se mover livremente de uma rede para uma outra, das quais uma das redes pode ser uma rede (com fio ou sem fio) fixa e o outro uma rede de acesso rádio, enquanto o usuário final pelo menos, parcialmente retém seus serviços subscritos , um controlador de política em uma rede precisa ser capaz de descobrir seu par de controlador de política na outra rede, e qualquer acordo de deslocamento entre as partes precisa ser detectado e recuperado. Esses objetos não são alcançados hoje por qualquer solução existente.

Deslocamento se refere a extensão de um serviço para uma localização diferente daquela localização de origem onde o serviço foi registrado, por meio de um acordo de deslocamento. Deslocamento ocorre quando um assinante para um operador de rede usa as facilidades de um outro operador, tal como e. g. quando um telefone de comunicação móvel foi realocado para uma outra região ou um outro país, onde seu operador de origem não tem cobertura.

Um processo de deslocamento convencional quando um telefone de comunicação móvel foi realocado para uma nova rede envolve o seguinte: Quando o telefone de comunicação móvel é ligado em uma nova rede, ou transferido através transferência sem interrupção para a nova rede, a rede nova visitada detecta o telefone, nota que ele não está registrado, e tenta identificar a rede de origem do telefone de comunicação móvel. Se não há acordo de deslocamento entre a rede de origem e a rede visitada , ao telefone de comunicação móvel serão negados serviços pela rede visitada . Ao contrário, a rede visitada contata a rede de origem e solicita informação de serviço considerando o telefone, a mencionada informação incluindo se o telefone de comunicação móvel está ou não permitido fazer deslocamento. Se a solicitação é sucedida, a rede visitada vai manter um registro do assinante temporário para o telefone, e a rede de origem vai atualizar sua informação

para indicar que o telefone foi realocado para a rede visitada, permitindo um encaminhamento correto da informação.

O 3GPP fornece descoberta de controlador de política entre redes de acesso de rádio diferentes, mas em redes de acesso fixo, e. g. no mundo de banda larga fixo, o princípio de igualdade de acesso conduz a um modelo e abordagem de negócio diferente daquele no 3GPP. Por exemplo, o DSL Forum propõe Arquitetura de controle de política composto de um número de controladores de política separada, do qual cada um pode pertencer a um provedor de serviço diferente. Contudo, no 3GPP, aquelas funções são efetuadas por somente um operador de rede.

Ainda de acordo com o 3GPP, a identidade de usuário é associada com um operador de rede específico, que não é o caso na banda larga fixa. Uma maneira de quebrar a ligação entre a identidade e um operador de rede é a introdução de uma entidade chamada Provedor de Identidade IDP, que pode ser totalmente independente de qualquer operador de rede, funcionando como uma terceira parte confiável. Por conseguinte, um assim chamado Provedor de Identidade independente não é associado com qualquer operador de rede, mas em vez disso, com qualquer outra organização adequada e independente, tal como e. g. um banco.

Assim sendo, quando um terminal de usuário, e. g. um telefone de comunicação móvel ou um computador pessoal, acessa tipos diferentes de redes, a descoberta de controladores de política e o deslocamento pode apresentar um problema.

SUMÁRIO

O objeto da presente invenção é endereçar os problemas esboçados acima, e fornecer Arquitetura de política melhorada permitindo a descoberta de controlador de política entre tipos diferentes de redes de acesso, assim como suporte de deslocamento, com igualdade de acesso. Este objeto e outros são alcançados pela arquitetura de controle de política, os nós

individuais da arquitetura de controle de política, e os métodos nos nós individuais da arquitetura de política de acordo com as reivindicações independentes anexas.

De acordo com um aspecto, a invenção fornece Arquitetura de controle de política para tratar políticas em redes de comunicação, assim como um Provedor de Identidade independente, um Controlador de Política de Usuário e um Controlador de Política de Negócio arranjado para funcionar como nós em tal Arquitetura de controle de política.

A arquitetura de controle de política compreende um Provedor de Identidade independente arranjado para entradas de terminal de usuário do IDP para informação de controle de política, e controladores de política de modo lógico dividido em unidades de controle de política. As unidades de controle de política incluem um Controlador de Política de Usuário arranjado para gerar entradas de terminal de usuário do UPC para subscrições de serviço.

A informação de controle de política na entrada de terminal de usuário de IDP do Provedor de Identidade pode compreender o endereço do Controlador de Política de Usuário em uma rede de origem do terminal de usuário, e as unidades de controle de política divididas de forma lógica podem ainda incluir um Controlador de Política de Negócio arranjado para aplicar política relacionada à negócio sobre subscrições de serviço. Às políticas relacionadas ao negócio do Controlador de Política de Negócio podem compreender acordos de deslocamento.

As unidades de controle de política divididas de forma lógica podem ainda incluir um controlador de política de Serviço arranjado para aplicar políticas relacionadas à serviço, e um controlador de política de Rede arranjado para mapear políticas de serviço em políticas dependentes da rede, que podem ser arranjadas para criar políticas relacionadas de rede com base no estado da rede.

De acordo com um outro aspecto, um método é fornecido em um terminal de usuário para lançar um serviço em uma primeira rede de origem tratado através da arquitetura de controle de política. O terminal de usuário efetua pelo menos, dos seguintes passos:

- Receber uma identidade de um Provedor de Identidade independente antes de se conectar a uma primeira rede de origem;

- Conectar-se a uma primeira rede de origem e receber um endereço de IP;

- Subscrever-se a um serviço disponível na rede de origem;

- Lançar o serviço subscrito em uma rede de origem pelo menos, uma vez.

Quando o terminal de usuário lança o mencionado serviço em uma segunda rede, o terminal de usuário pode efetuar pelo menos, os passos adicionais de:

- Realocar para uma segunda rede visitada;

- Efetuar deslocamento em uma rede visitada fornecendo sua identidade;

- Receber uma lista de serviços disponíveis através do controlador de política de Negócio;

- Lançar o mencionado serviço subscrito, se ele está disponível na rede visitada.

Um Provedor de Identidade independente dentro de Arquitetura de controle de política efetua pelo menos, os seguintes passos:

- Emitir uma identidade para um terminal de usuário e gerar uma correspondente entrada de terminal de usuário do IDP;

- Efetuar AAA no terminal de usuário quando ele se conecta a uma primeira rede de origem;

- Armazenar o endereço do Controlador de Política de Usuário da primeira rede de origem na entrada de terminal de usuário do IDP;

- Fornecer o endereço do UPC de origem para o controlador de política de Rede quando o terminal de usuário lança um serviço subscrito;

- Efetuar AAA no terminal de usuário quando ele se realoca para uma segunda rede;

- Fornecer o endereço do UPC de origem para o Controlador de Política de Usuário da segunda rede.

Um Controlador de Política de Usuário dentro de Arquitetura de controle de política efetua pelo menos, os seguintes passos quando um terminal de usuário se conecta a uma primeira rede de origem:

- Gerar uma entrada de terminal de usuário de UPC e armazenar o ID de um serviço subscrito;

- Acessar o Provedor de Identidade independente e registrar seu endereço de UPC na correspondente entrada de terminal de usuário do IDP;

- Armazenar o endereço do controlador de política de Serviço associada com o serviço subscrito na entrada de terminal de usuário de UPC;

- Armazenar o endereço do controlador de política de Rede da rede de origem na entrada de terminal de usuário do UPC;

Um Controlador de Política de Usuário pode efetuar pelo menos, os seguintes passos quando o mencionado terminal de usuário se realoca para uma segunda rede visitada:

- Um Controlador de Política de Usuário da segunda, rede visitada adquirindo o endereço do Controlador de Política de Usuário da primeira, rede de origem através da entrada de terminal de usuário do IDP;

- O Controlador de Política de Usuário da rede de origem enviando os IDs dos serviços subscritos dos terminais de usuário, para o Controlador de Política de Usuário na rede visitada;

- O Controlador de Política de Usuário da rede de origem enviando o endereço do controlador de política de Serviço associado com

cada serviço subscrito, para o correspondente controlador de política de Serviço da rede visitada;

Um Controlador de Política de Negócio dentro da mencionada arquitetura de controle de política aplica políticas relacionadas ao negócio nos serviços subscritos de um terminal de usuário de deslocamento, e as mencionadas políticas relacionadas ao negócio podem incluir acordos de deslocamento.

Um controlador de política de Serviço dentro do mencionado controle de política aplica políticas relacionadas à serviço em um serviço subscrito.

Um controlador de política de Rede dentro da mencionada arquitetura de controle de política mapeia políticas de serviço em políticas dependentes de rede, e pode criar políticas relacionadas de rede com base no estado da rede.

DESCRIÇÃO BREVE DOS DESENHOS

A presente invenção será agora descrita em mais detalhe e com referência aos desenhos anexos, nos quais:

- Figura 1 é um diagrama em bloco, de forma esquemática, ilustrando uma primeira modalidade de Arquitetura de controle de política de acordo com esta invenção;

- Figura 2 é um fluxograma ilustrando os passos efetuados quando um terminal de usuário se realoca para uma segunda, rede visitada;

- Figura 3 é um fluxograma ilustrando uma modalidade exemplar de um método em um terminal de usuário em Arquitetura de controle de política de acordo com a invenção;

- Figura 4 é um fluxograma ilustrando uma modalidade exemplar de um método em um Provedor de Identidade independente dentro de Arquitetura de controle de política de acordo com a invenção, e

- Figura 5 é um fluxograma ilustrando uma modalidade

exemplar de um método em um Controlador de Política de Usuário dentro Arquitetura de controle de política de acordo com a invenção.

DESCRIÇÃO DETALHADA

Na seguinte descrição, detalhes específicos são estabelecidos, tal como uma particular arquitetura e seqüência de passos de modo a fornecer um entendimento aprofundado da presente invenção. Contudo, é aparente para uma pessoa qualificado na arte que a presente invenção pode ser praticada em outras modalidades que pode divergir desses detalhes específicos.

Mais ainda, é aparente que as funções descritas podem ser implementadas usando software funcionando em conjunto com um microprocessador programado ou um computador de propósito geral, e/ou usando um circuito integrado específico de aplicação. Onde a invenção é descrita na forma de um método, a invenção pode também ser incorporado em um produto de programa de computador, assim como em um sistema compreendendo um processador de computador e uma memória, onde a memória é codificada com um ou mais programas que pode efetuar as funções descritas.

Esta invenção fornece Arquitetura de controle de política, compreendendo uma função de controle de política dividida em unidades funcionais de controle de política separadas, e. g. quatro unidades, que pode ser denotado Controlador de Política de Usuário , controlador de política de Rede, controlador de política de Serviço e controlador de política de Negócio. Ainda, a arquitetura compreende um Provedor de Identidade independente, que não é associada com qualquer operador de rede, tendo uma funcionalidade adicional habilitando-a a funcionar com a ancora e ponto de entrada para a descoberta de controlador de política. Quando a um terminal de usuário foi dado uma identidade em uma rede de origem, uma entrada será criada no Provedor de Identidade independente para este terminal de usuário,

e o terminal de usuário é de modo único, identificado através de sua identidade. Quando o terminal de usuário primeiro lança um serviço em sua rede de origem, ele vai primeiro localizar seus controladores de política, compreendendo as e. g. quatro mencionadas unidades funcionais, i. e. o Controlador de Política de Usuário , o Controlador de Política de Rede, o Controlador de Política de Serviço e o Controlador de Política de Negócio. Após todos os controladores de política serem encontrados, a informação vai também ser impulsionado a entrada do ' Provedor de Identidade ' associada ao terminal de usuário específico. Quando o terminal de usuário se move para uma nova localização dentro de uma outra rede, ele vai fornecer sua identidade para a rede visitada, que vai usar a identidade para recuperar o provedor de identidade. O Provedor de Identidade vai fornecer a informação considerando os controladores de política para a rede visitada, possibilitando a rede visitada para pegar subscrições de serviço e para determinar se qualquer acordo de negócio existe entre a rede visitada e a rede de origem, eventualmente permitindo o terminal de usuário de deslocamento para alcançar o mencionado serviço.

De acordo com a invenção, o Controlador de Política de Usuário UPC e o Controlador de Política de Negócio BPC são fornecidos com novas funcionalidades considerando suporte de deslocamento. Quando um terminal de usuário se subscreve a um serviço, a informação de subscrição será adicionada como uma entrada de terminal de usuário em uma tabela de informação de Usuário UPC no UPC de origem, junto com a identidade associada com este serviço. Quando o terminal de usuário se move para uma outra rede, o Local de Borda de Acesso (AES) na rede visitada será capaz de recuperar a localização do Provedor de Identidade independente IDP, e o Provedor de Identidade vai fornecer o endereço do UPC de origem do terminal de usuário a partir da correspondente entrada de sua Tabela de Informação de Usuário do IDP. Daí em diante, todas as subscrições de serviço

relacionadas do terminal de usuário podem ser pego do UPC de origem,com base na identidade do terminal de usuário. Esta informação será enviada ao BPC dedicado servindo a rede visitada, que vai aplicar as políticas de acordo de deslocamento. E por meio disso, a rede visitada vai informar que serviços que estão disponíveis para o terminal de usuário.

Uma primeira modalidade de Arquitetura de controlador de política de acordo com esta invenção é ilustrada no diagrama em bloco da figura 1, fornecido com entidades funcionais separadas relacionadas a tomada e imposição de decisão de política, tal como e. g. deslocamento, e todas políticas relacionadas a acordo de deslocamento são controlada através de uma unidade funcional denotada controlador de política de Negócio BPC.

A figura ilustra um terminal de usuário UE se realocando de uma rede de acesso 1 to uma segunda rede de acesso 2, assim como Arquitetura de controle de política possibilitando deslocamento do terminal de usuário na segunda rede de acesso. A realocação do terminal de usuário é indicada pela seta tracejada entre dois blocos de UE. A figura ainda ilustra a rede de IP 3, duas redes de serviço 4a, 4b e um gerenciador de publicação de Serviço 5.

IDP se refere a um Provedor de Identidade independente, que é associado com uma organização de terceira parte confiável e não com qualquer operador de rede, emitindo identidades para terminais de usuário e por meio disso , dissociando a identidade de usuário do operador de rede, possibilitando um igualdade de acesso. De acordo com esta invenção, o Provedor de Identidade independente IDP é fornecido com uma funcionalidade adicionada para agir como ponto de ancora de descoberta de controlador de política e autoridade de verificação de identidade.

Como ilustrado na figura 1, a função de controle de política de acordo com esta modalidade da invenção é dividida de forma lógica em quatro unidades funcionais, um controlador de política de Negócio, um

controlador de política de Usuário , um controlador de política de Rede e um controlador de política de Serviço. O controlador de política de Negócio e o controlador de política de Usuário são fornecidos com funcionalidades adicionais para permitir descoberta e localização entre tipos diferentes de redes, e para permitir deslocamento.

O BPC na figura se refere a um controlador de política de Negócio dedicado, que é responsável por gerar políticas relacionadas ao negócio, tal como acordos de deslocamento entre redes e SLA: s (Acordos de Nível de Serviço) , que é um acordo entre um provedor de serviço e um receptor de serviço, e para impulsioná-los para o ponto de aplicação de política, PEP, e. g. um Local de Borda de Acesso, AES.

UPC na figura se refere a um controlador de política de Usuário , que controla todas as políticas relacionadas ao usuário final, entre elas a identificação do usuário, AAA (autenticação, autorização, contabilidade) , registros de faturamento, e todos os serviços subscritos dos terminais de usuário, e é normalmente associada com um operador de rede.

SPC na figura se refere a um controlador de política de Serviço, que cria e impulsiona políticas relacionadas com serviço para e impulsiona as políticas relacionadas do serviço para ponto de imposição de política, PEP correto. Políticas de serviço descrevem a lógica global de negócio que é aplicada para solicitação de servidores de aplicação e pares de controlador de política de Serviços. O controlador de política de Serviço pode ser uma parte da rede de origem, mas também pode ser uma parte da rede de um provedor de serviço independente.

NPC na figura se refere a um controlador de política de Rede, que tem duas funções. Primeiramente, ele recebe políticas de serviço dos controladores de política de serviço e as mapeia em políticas dependentes da rede. Em segundo lugar, ele cria políticas relacionadas com a rede com base no estado da rede existente.

RM na figura se refere a um Gerenciador de Recursos, que gerencia os recursos da rede.

SM na figura se refere a um Gerenciador de Serviço, que é responsável por gerenciar e divulgar serviços para a rede do provedor de serviço.

AES na figura se refere a um Local de Borda de Acesso, que atua como ponto de imposição de política, i. e. " impõe " as políticas.

AN na figura se refere a um nó de acesso da rede de acesso.

UE na figura se refere a um terminal de usuário, que pode ser e. g. um telefone de comunicação móvel/celular ou um computador pessoal.

Daqui em diante é descrito como a descoberta de controlador de política é efetuada e como acordos de deslocamento são encontrados e aplicados de acordo com esta invenção, cobrindo os passos de antes de um terminal de usuário se conectar a uma rede de origem até ele receber serviços de deslocamento de acordo com a maneira pré-definida em uma rede visitada. Alguns dos passos individuais correspondem àqueles na arte anterior, mas as seqüências de passos são novas, já que o Provedor de Identidade IDP, o controlador de política de Negócio BPC e os controladores de política de Usuário UPCs que são envolvidos nos passos têm funcionalidades adicionais de acordo com esta invenção.

Antes de se conectar a uma rede, o terminal de usuário UE precisa receber uma identidade de um de Provedor de Identidade independente IDP, e. g. na forma de um cartão de IMSI (Assinante Móvel Internacional), ou como um para usuário/senha, que é capaz, modo único, identificar este terminal de usuário UE. Após se subscrever ao serviço, o terminal de usuário UE tem de lançá-lo pelo menos, uma vez na antes de deslocamento para uma rede visitada.

* Antes de um terminal de usuário UE se conectar a uma rede de origem:

a. O AES (Local de Borda de Acesso) dá informação de rede, tal como, nome do operador de rede, para um gerenciador de publicação de serviço 5. Esta informação pode e. g. ser adicionada ao nome do AES, tal como AES.telia.se.

b. Com base nesta informação, o gerenciador de publicação de serviço 5 contata um controlador de política de Negócio BPC, que é pré-definido para este gerenciador de publicação de serviço, e pega políticas considerando os provedores de serviço/serviços tendo acordo com um operador de rede.

c. O gerenciador de publicação de serviço pesquisa seu próprio diretório de serviço e envia todos os serviços disponíveis para o AES.

d. O AES gera um portal da rede listando todos os serviços disponíveis.

e. O terminal de usuário UE recebe uma identidade de um Provedor de Identidade independente IDP.

** O terminal de usuário UE se conecta a uma rede de origem:

a. O terminal de usuário UE envia solicitações de DHCP que são recebidas pelo AES, e o AES envia de volta um endereço de IP padrão para o terminal de usuário DE.

b. O terminal de usuário UE é re-direcionado para o portal da rede onde todos os serviços disponíveis estão listados.

*** O terminal de usuário UE se subscreve ao serviço:

a. O terminal de usuário UE fornece sua ID (identidade) para o AES.

b. A ID é autorizada e autenticada pelo IDP por meio de um AAA.

c. Após o AAA, o AES vai enviar a seguinte informação para o controlador de política de Usuário UPC na rede de origem: ID de UE ID, ID de serviço Subscrito, endereço ou nome do IDP.

d. Com base na informação acima, o UPC vai gerar uma tabela de informação de usuário do UPC com a entrada de UE para a identidade do terminal de usuário. Na entrada de UE, as identidades dos serviços subscritos são registradas, junto com os endereços do controlador de política de Serviço SPC associado com cada serviço subscrito, assim como o endereço do controlador de política de Rede NPC da rede de origem. Antes que o terminal de usuário UE lance um serviço pela primeira vez, a tabela de informação de Usuário do UPC (tabela 1) pode ter o seguinte conteúdo:

| UE | NPC | SERVIÇO | SPC |
|---|---|---|---|
| | vazio | ID 1 de Serviço | vazio |
| | | ID 2 de Serviço | vazio |
| | | " | " |
| | | ID n de Serviço | vazio |

d. O Controlador de Política de Usuário UPC então acessa a entrada de UE na tabela de informação de Usuário do IDP, informação tabela no Provedor de Identidade independente IDP, e registra a sinal próprio na mesma entrada, criando um par ID de UE - UPC. No Provedor de Identidade independente IDP, a mencionada tabela de informação de Usuário do IDP é mantida para todos os usuários/dispositivos que recebem Ids deste Provedor de Identidade independente IDP, junto com seu endereço de UPC de origem, e um exemplo do conteúdo nesta tabela é indicado abaixo, denotado tabela 2:

| UE | UPC |
|---|---|
| ID 1 | Endereço |
| ID 2 | Endereço |
| " | " |
| ID n | Endereço |

e. O terminal de usuário UE recebe um endereço de IP real:

**** O terminal de usuário UE lança um serviço:

a. O terminal de usuário UE e um servidor de aplicação (não mostrado na figura 1) acham o mesmo controlador de política de Serviço SPC usando um algoritmo pré-definido, e. g. através de uma negociação de

sinalização adequada, que é bem conhecido para a pessoa qualificada.

b. O controlador de política de Serviço SPC usa o ID do UE para ter acesso ao IDP, e para pegar o correspondente endereço de UPC da tabela de informação de Usuário do IDP.

c. O controlador de política de Serviço SPC registra seu endereço de SPC na tabela de informação de Usuário do UPC na entrada de UE e ID de Serviço específico.

d. O AES fornece O ID do UE para seu controlador de política de Rede NPC, que pode ser pré-definido para o AES ou encontrado através de indagação de DNS.

d. O controlador de política de Rede NPC pega o endereço de UPC endereço da tabela de informação de Usuário do IDP.

e. O controlador de política de Rede NPC registra seu endereço de NPC na tabela de informação de Usuário do UPC.

Após esses passos, a negociação e sinalização de serviço convencional vai continuar, com base no tipo de serviço. Após o terminal de usuário UE ter lançado vários serviços, a entrada do UE na tabela de informação de Usuário UPC no controlador de política de Usuário UPC pode corresponder a seguinte tabela 3:

| UE | NPC | SERVIÇO | SPC |
|---|---|---|---|
| ID | Endereço | ID 1 de Serviço | Endereço – 1 |
| | | ID 2 de Serviço | Endereço – 2 |
| | | ... | ... |
| | | ID n de Serviço | Endereço – n |

O processo de sinalização processo está completo, o terminal de usuário UE pode iniciar a usar o serviço.

***** O terminal de usuário UE se realoca para uma segunda (visitada) rede:

a. O terminal de usuário UE se conecta à rede visitada, e fornece sua ID.

b. O AES visitado recupera o endereço do Provedor de

Identidade independente IDP baseado na informação de ID do UE , e. g. por meio de uma indagação de DNS.

c. O Provedor de Identidade IDP independente efetua AAA sobre o ID dos terminais de usuário. Daí em diante, o endereço de UPC de origem do terminal de usuário é pego da entrada de UE da tabela de informação de usuário do ID e enviado de volta para o AES visitado, possibilitando ao controlador de Política de Usuário UPC da rede visitada adquirir o endereço do controlador de Política de Usuário UPC de origem.

d. O UPC de origem retorna os IDs de serviço dos serviços subscritos do terminal de usuário UE para o controlador de política de Usuário UPC e o AES na segunda e visitada rede, o ID de serviço de um serviço subscrito compreendendo informação considerando o provedor de serviço.

e. O AES visitado se comunica com o controlador de política de Negócio BPC dedicado através do gerenciador de publicação de serviço 5.

f. O controlador de política de Negócio BPC verifica para cada provedor de serviço se há um acordo de negócio entre o provedor de serviço e a rede visitada. Se um acordo de negócio existe, o serviço pode ser usado pelo terminal de usuário UE de deslocamento, caso contrário ao terminal de usuário UE será negado o serviço.

g. O AES visitado retorna uma lista de serviços disponíveis para o terminal de usuário UE de deslocamento.

****** O terminal de usuário UE lança um serviço da rede visitada:

Os passos a, b, c são os mesmos como na seqüência de passos anterior, pelo qual a rede visitada encontra o UPC de origem. A única diferença é que o AES visitado retorna não somente o ID do UE, mas também o ID de serviço relacionando o serviço que o terminal de usuário UE de deslocamento quer lançar.

d. O UPC de origem localiza as entradas de terminais de

usuário a partir de sua tabela de informação de Usuário do UPC, e acha o endereço do controlador de política de Serviço SPC associado com o serviço específico que o terminal de usuário UE de deslocamento quer lançar.

e. Por meio disso, o SPC e AES visitado descobrem o endereço do SPC associado com o serviço do terminal de usuário UE de deslocamento. O AES visitado pode buscar políticas considerando este serviço, ou o controlador de política de Serviço SPC visitado pode contatar o controlador de política de Serviço SPC associado com o serviço para políticas.

Após esses passos, o serviço prossegue na maneira convencional.

De modo a ainda explica e esclarecer a presente invenção, os passos efetuado quando um terminal de usuário se realoca para uma nova rede são ilustrados na figura 2.

No passo 21, o UE se conecta à nova e segunda rede, e fornece seu ID. No passo 22, o AES em uma rede visitada recupera o IDP com base na identidade do UE, através de e. g. indagação de DNS.

No passo 23, o IDP efetua AAA sobre o ID do UE, e o endereço do UPC na rede de origem é pego das entradas de UE do IDP na tabela de informação de Usuário do IDP no passo 24, e envia de volta para o AES visitado. Por meio disso, o UPC da rede visitada adquire o endereço do UPC de origem.

O UPC de origem envia, no passo 25, o ID do serviço subscrito do UE de volta ao UPC e AES na rede visitada, O ID do serviço compreendendo informação considerando o provedor de serviço.

No passo 26, o AES visitado se comunica com o BPC através do gerenciador de publicação de serviço 5, e o BPC determina, no passo 27, para cada provedor de serviço se há um acordo de negócio entre o provedor de serviço e a rede visitada. Se o acordo de negócio existe, o serviço pode ser

usado pelo UE de deslocamento, caso contrário ao UE será negado o serviço, no passo 28. O AES visitado retorna uma lista de serviços disponíveis para o UE de deslocamento no passo 29.

Figura 3 é um fluxograma ilustrando uma modalidade exemplar de um método de um terminal de usuário em Arquitetura de controle de política de acordo com esta invenção, o fluxograma compreendendo pelo menos, alguns dos passos efetuados através de um terminal de usuário de antes de se conectar a uma primeira rede, até que ele lance um serviço subscrito em uma segunda rede.

No passo 31, um terminal de usuário se registra com um Provedor de Identidade independente, IDP, e recebe uma identidade, tal como e. g. um cartão de IMSI ou uma senha. Daí em diante, no passo 32, o terminal de usuário se conecta a uma primeira rede 1, i. e. a rede de origem, e fornece sua identidade de modo a subscrever um serviço disponível, no passo 33. O terminal de usuário lança o serviço subscrito no passo 34, e daí em diante se realoca para uma segunda rede 2, i. e. a rede visitada, fornecendo seu ID. No passo 36 o terminal de usuário recebe uma lista de serviços disponíveis na rede visitada do AES da rede visitada. O AES obteve esta informação de um controlador de política de Negócio dedicado, através do gerenciador de publicação de serviço 5. Se é determinado no passo 37 que o serviço subscrito do terminal de usuário está disponível na rede visitada, o terminal de usuário lança o serviço, no passo 39, caso contrário ao terminal de usuário é negado lançar o serviço, no passo 38.

Figura 4 é um fluxograma ilustrando uma modalidade exemplar do método de um Provedor de Identidade independente dentro de Arquitetura de controle de política de acordo com esta invenção. O fluxograma compreende pelo menos, alguns dos passos efetuados através de um Provedor de Identidade independente IDP de antes da UE se conectar a uma prioridade rede, até que o UE se realoca para uma segunda (visitada)

rede.

No passo 41, o Provedor de Identidade independente emite uma identidade para um terminal de usuário UE, e quando este terminal de usuário se conecta a uma primeira rede 1, i. e. a rede de origem, o IDP efetua AAA no terminal de usuário, no passo 42. No passo 43, o IDP armazena o endereço do UPC da rede de origem do UE em sua tabela de informação de usuário do IDP. Este passo é efetuado pelo mencionado UPC de origem acessando a entrada de UE na tabela de informação de Usuário do IDP e registrando a si próprio. Quando o terminal de usuário lança um serviço subscrito na rede de origem, o IDP fornece o endereço do UPC de origem para o controlador de política de Rede NPC de origem, no passo 44, que é efetuado pelo NPC pegando o endereço de UPC de origem a partir do IDP.

Quando o terminal de usuário se realoca para uma segunda rede 2, i. e. a rede visitada, o IDP efetua AAA no terminal de usuário, no passo 45, e ainda fornece o endereço da UPC de origem para o UPC visitado através do AES visitado, no passo 46.

Figura 5 é um fluxograma ilustrando uma modalidade exemplar de um método de um controlador de política de Usuário UPC dentro de Arquitetura de controle de política de acordo com esta invenção. O fluxograma compreende pelo menos, algum dos passos efetuados através de um controlador de política de Usuário do UPC de quando um UE é conectado para uma primeira rede 1, até o UE pode lançar o serviço subscrito em uma segunda (visitada) rede.

No passo 51, o controlador de política de Usuário gera uma tabela de informação de Usuário UPC com uma entrada para entidade do UE. Na entrada de UE, as identidades dos serviços subscritos podem ser registrados, junto com os endereços do controlador de política de Serviço SPC associado com cada serviço subscrito, assim como o endereço do controlador de política de Rede NPC da rede de origem. Já que o UPC recebe a identidade

UE, o serviço subscrito ID e o endereço ou nome do IDP quando o UE se subscreve a um serviço, o ID do serviço subscrito é adicionado na entrada do UE na tabela de informação de Usuário UPC (tabela 1) .

No passo 52, o UPC acessa a tabela de informação de Usuário do IDP (tabela 2) e registra seu endereço na entrada de UE, criando um par de ID de UE - UPC par. No passo 53, o UPC armazena o endereço do controlador de política de Serviço SPC associado com o serviço subscrito do UE em sua tabela de informação de Usuário do UPC, e no passo 54 a UPC armazena o endereço do controlador de política de Rede NPC da rede de origem, e por meio disso , completando a entrada de UE na tabela de informação de Usuário do UPC.

Quando o terminal de usuário se realoca para uma segunda (visitada) rede 2, o UPC na rede visitada recebe o endereço do UPC de origem através do AES visitado e da tabela de informação de usuário do IDP, no passo 55. E por meio disso, o UPC de origem é capaz de recuperar a informação de terminal de usuário de sua tabela de informação de Usuário do UPC e enviar os IDs do serviço subscrito para o terminal de usuário de deslocamento para o UPC visitado, no passo 56, o ID do serviço subscrito compreendendo informação relacionada ao provedor de serviço.

Ainda, o UPC de origem recupera o endereço do controlador de política de Serviço SPC associado com os serviços subscritos do terminal de usuário a partir de sua tabela de informação de Usuário do UPC, e enviá-lo para o correspondente controlador de política de Serviço SPC da rede visitada, no passo 57, eventualmente possibilitando ao terminal de usuário lançar o serviço subscrito na rede visitada.

Assim sendo, a presente invenção usa um Provedor de Identidade independente, um controlador de política de Negócio e um controlador de política de Usuário fornecido com funcionalidades adicionais para possibilitar controladores de política em diferentes tipos de redes

localizar cada um ao outro, e suportar deslocamento de um terminal de usuário se movendo entre tipos diferentes de redes, tal com realocando e. g. a partir de umas redes de acesso fixas para umas redes de acesso rádio.

Por esse meio, a invenção fornece uma localização de controle de política melhorada e suporte ao deslocamento quando um terminal de usuário se realoca para uma rede de acesso de um tipo diferente. Dando a um Provedor de Identidade independente, as novas funcionalidades de acordo com esta invenção, a importância do Provedor de Identidade independente como uma terceira parte verdadeira independente é fortalecida. Isto é aquela dos passos principais em direção a arquitetura de rede mais livremente acoplada que é capaz de fornecer serviços aos usuários com base no princípio de igualdade de acesso.

Enquanto a invenção foi descrita com referência às modalidades exemplares específicas, a descrição é em geral somente pretendida para ilustrar o conceito inventivo e não deve ser tomada como limitando o escopo da invenção.

# REIVINDICAÇÕES

1. Arquitetura de controle de política arranjada para tratar políticas em redes de comunicação (1, 2), caracterizada pelo fato de que a arquitetura de controle de política compreende um provedor de identidade independente (IDP) arranjada para gerar entradas de terminal de usuário de IDP para informação de controle de política, caracterizada pelo fato de compreender controladores de política dividida de forma lógica em unidades de controle de política, as mencionadas unidades de controle de política incluindo um controlador de política de Usuário (UPC) arranjada para gerar entradas de terminal de usuários de UPC para subscrições de serviços.

2. Arquitetura de controle de política de acordo com a reivindicação 1, caracterizada pelo fato de que a informação de controle de política em uma entrada de terminal de usuário do IDP do Provedor de Identidade (IDP) compreende o endereço do Controlador de Política de Usuário (UPC) em uma rede de origem (1) do terminal de usuário (UE).

3. Arquitetura de controle de política de acordo com a reivindicação 1 ou 2, caracterizada pelo fato de que as mencionadas unidades de controle de política divididas de forma lógica ainda inclui um controlador de política de Negócio (BPC) arranjado para aplicar políticas relacionadas ao negócio nas subscrições de serviço.

4. Arquitetura de controle de política de acordo com a reivindicação 3, caracterizada pelo fato de que as mencionadas políticas relacionadas ao negócio do controlador de política de Negócio compreende acordos de deslocamento.

5. Arquitetura de controle de política de acordo com qualquer das reivindicações anteriores, caracterizada pelo fato de que as mencionadas unidades de controle de política divididas de forma lógica ainda incluem um controlador de política de Serviço (SPC) arranjado para aplicar políticas relacionadas a serviços aos serviços subscritos .

6. Arquitetura de controle de política de acordo com qualquer das reivindicações anteriores, caracterizada pelo fato de que as mencionadas unidades de controle de política divididas de forma lógica ainda incluem um controlador de política de Rede (NPC) arranjado para mapear políticas de serviço em políticas dependentes de rede.

7. Arquitetura de controle de política de acordo com a reivindicação 6, caracterizada pelo fato de que o controlador de política de Rede é arranjado adicionalmente para criar políticas relacionadas com a rede com base no estado da rede.

8. Controlador de Política independente (IDP) para arquitetura de controle de política de acordo com qualquer das reivindicações anteriores, caracterizado pelo fato de que, o Controlador de Política independente é arranjado para gerar entradas de terminal de usuário do IDP para informação de controle de política, as entradas de terminal de usuário do IDP compreendendo o endereço do Controlador de Política de Usuário (UPC) em uma rede de origem (1) de um terminal de usuário (UE) .

9. Controlador de política de Usuário (UPC) para arquitetura de controle de política de acordo com qualquer das reivindicações 1 a 7, caracterizado pelo fato de que o controlador de política de Usuário é arranjado para gerar entrada de terminal de usuário do UPC compreendendo o ID dos serviços subscritos de um terminal de usuário (UE) .

10. Controlador de política de Usuário (UPC) de acordo com reivindicação 9, caracterizado pelo fato de que o Controlador de Política de Usuário é arranjado adicionalmente para armazenar o endereço do controlador de política de Serviço (SPC) associado com cada serviço subscrito, e o endereço do controlador de política de Rede (NPC) da rede de origem, na mencionada entrada de terminal de usuário do UPC.

11. Controlador de política de Negócio (BPC) para arquitetura de controle de política de acordo com qualquer das reivindicações 2 a 7,

caracterizado pelo fato de que o controlador de política de Negócio é arranjado para aplicar políticas relacionadas ao negócio nos serviços subscritos de um terminal de usuário de deslocamento.

12. Controlador de política de Negócio de acordo com a reivindicação 11, caracterizado pelo fato de que as mencionadas políticas relacionadas ao negócio incluem acordos de deslocamento.

13. Método em um terminal de usuário (UE) de lançar o serviço em uma primeira rede de origem (1) tratada pela arquitetura de controle de política como definida em qualquer das reivindicações 1 a 7, caracterizado pelo fato do terminal de usuário efetua pelo menos, os seguintes passos:

- Receber (31) uma identificador de um Provedor de Identidade independente (IDP) antes de se conectar a uma primeira rede de origem;

- Se conectar (32) a uma primeira rede de origem e receber um endereço de IP;

- Se subscrever (33) a um serviço disponível na rede de origem;

- Lançar (34) o serviço subscrito em uma rede de origem pelo menos, uma vez.

14. Método em um terminal de usuário (UE) de acordo com a reivindicação 13, de lançar o mencionado serviço em uma segunda rede (2), caracterizado pelo fato do terminal de usuário efetua pelo menos, os passos adicionais de:

- Realocar (35) para uma segunda rede visitada;

- Efetuar deslocamento (35) em uma rede visitada fornecendo sua identidade;

- Receber (36) uma lista de serviços disponíveis através de um controlador de política de Negócios (BPC) dedicados;

- Lançar os serviços subscritos, se eles estão disponíveis em

uma rede visitada (37, 38, 39) .

15. Método em um Provedor de Identidade independente (IDP) dentro de uma arquitetura de controle de política de acordo com qualquer das reivindicações 1 a 7, caracterizado pelo fato de que o Provedor de Identidade independente efetua pelo menos, os passos seguintes:

- Emitir (41) uma identidade para um terminal de usuário (UE) e gerar uma correspondente entrada de terminal de usuário do IDP;

- Efetuar AAA (42) no terminal de usuário (UE) quando ele se conecta a uma primeira rede de origem (1) ;

- Armazenar (43) o endereço do controlador de política de Usuário (UPC) da primeira rede de origem (1) na mencionada entrada de terminal de usuário do IDP;

- Fornecer (44) o endereço do UPC de origem para o controlador de política de Rede (NPC) quando o terminal de usuário lança um serviço subscrito;

- Efetuar AAA (45) no terminal de usuário (UE) quando ele se realoca para uma segunda rede;

- Fornecer (46) o endereço do UPC de origem para o controlador de política de Usuário (UPC) da segunda rede (2) .

16. Método em um controlador de política de Usuário (UPC) dentro de uma arquitetura de controle de política como definida em qualquer das reivindicações 1 a 7, caracterizado pelo fato de que o controlador de política de Usuário efetua pelo menos, os seguintes passos quando um terminal de usuário (UE) se conecta a uma primeira rede de origem (1) :

- Gerar (51) uma entrada de terminal de usuário do UPC e armazenar o ID de um serviço subscrito;

- Acessar o Provedor de Identidade independente (IDP) e registrar (52) seu endereço de UPC no correspondente entrada de terminal de usuário do IDP;

- Armazenar (53) o endereço do controlador de política de Serviço (SPC) associada com o serviço subscrito na entrada de terminal de usuário do UPC;

- Armazenar (54) o endereço do controlador de política de Rede (NPC) de uma rede de origem na entrada de terminal de usuário do UPC.

17. Método em um controlador de política de Usuário (UPC) de acordo com a reivindicação 16, caracterizado pelo fato de que o controlador de política de Usuário efetua pelo menos, os seguintes passos quando o mencionado terminal de usuário se realoca para uma segunda rede (2) visitada:

- Um controlador de política de Usuário (UPC) da segunda, rede visitada adquirindo (55) o endereço do controlador de política de Usuário (UPC) da primeira, rede de origem através da entrada de terminal de usuário de IDP;

- O controlador de Política de Usuário (UPC) da rede de origem enviando (56) os IDs dos serviços subscritos aos terminais de usuário para o controlador de política de Usuário na rede visitada;

- O controlador de política de Usuário (UPC) da rede de origem enviando (57) o endereço do controlador de política de Serviço (SPC) associado com cada um dos mencionados serviços subscritos para o correspondente controlador de política de Serviço da rede visitada;

18. Método em um controlador de política de Negócio (BPC) dentro de uma arquitetura de controle de política de acordo com qualquer das reivindicações 2 a 7, caracterizado pelo fato de que o controlador de política de Negócio aplicando políticas relacionadas ao negócio nos serviços subscritos de um terminal de usuário de deslocamento.

19. Método em um controlador de política de Negócio de acordo com reivindicação 18, caracterizado pelo fato de que as mencionadas

políticas relacionadas ao negócio incluem acordos de deslocamento.

20. Método em um controlador de política de Serviço (SPC) dentro de uma arquitetura de controle de política de acordo com qualquer das reivindicações 5 a 7, caracterizado pelo fato de que o controlador de política de Serviço aplica as políticas relacionadas a serviço em um serviço subscrito.

21. Método em um controlador de política de Rede (NPC) dentro de uma arquitetura de controle de política de acordo com qualquer das reivindicações 6 a 7, caracterizado pelo fato de que o controlador de política de Rede mapeia políticas de serviço em políticas dependentes da rede.

22. Método em um controlador de política de Rede (NPC) de acordo com reivindicação 21, caracterizado pelo fato de que o controlador de política de Rede cria políticas relacionadas com a rede com base no estado da rede.

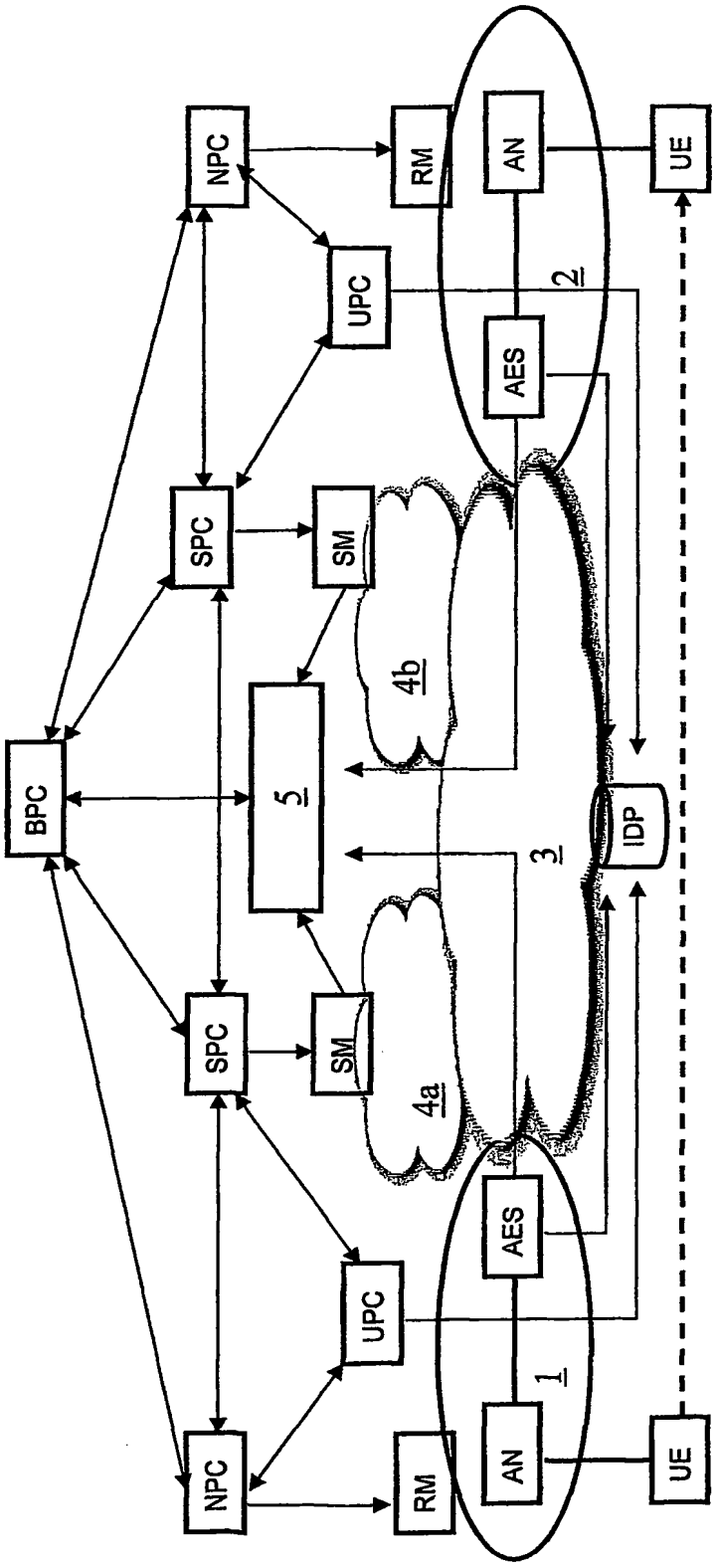

NPC
RM
AN
UE
UPC
2
AES
SPC
SM
4b
BPC
5
3
IDP
SPC
SM
4a
UPC
AES
1
NPC
RM
AN
UE

FIGURA 1

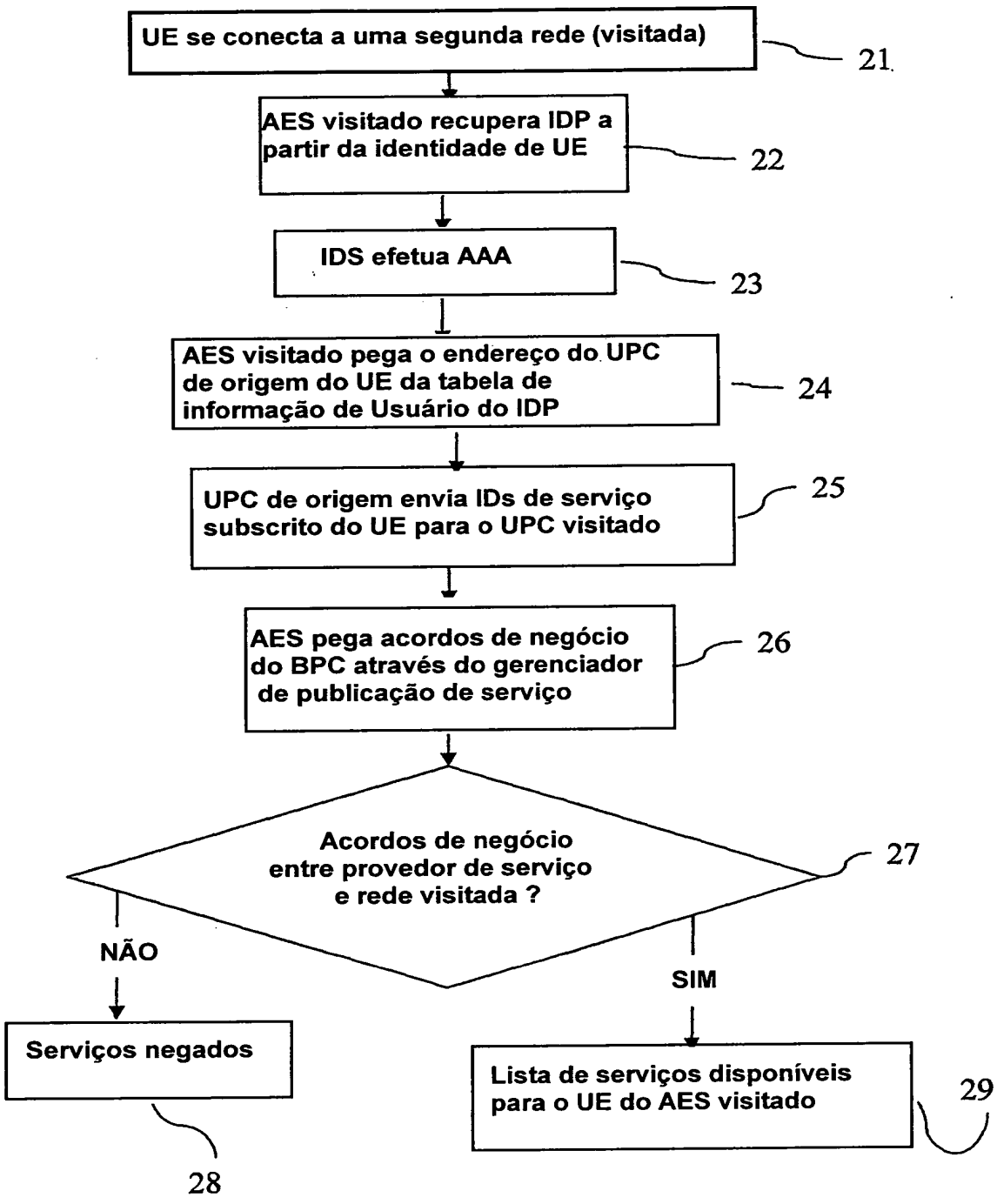

UE se conecta a uma segunda rede (visitada)
21
AES visitado recupera IDP a partir da identidade de UE
22
IDS efetua AAA
23
AES visitado pega o endereço do UPC de origem do UE da tabela de informação de Usuário do IDP
24
UPC de origem envia IDs de serviço subscrito do UE para o UPC visitado
25
AES pega acordos de negócio do BPC através do gerenciador de publicação de serviço
26
Acordos de negócio entre provedor de serviço e rede visitada ?
27
NÃO
SIM
Serviços negados
28
Lista de serviços disponíveis para o UE do AES visitado
29

FIGURA 2

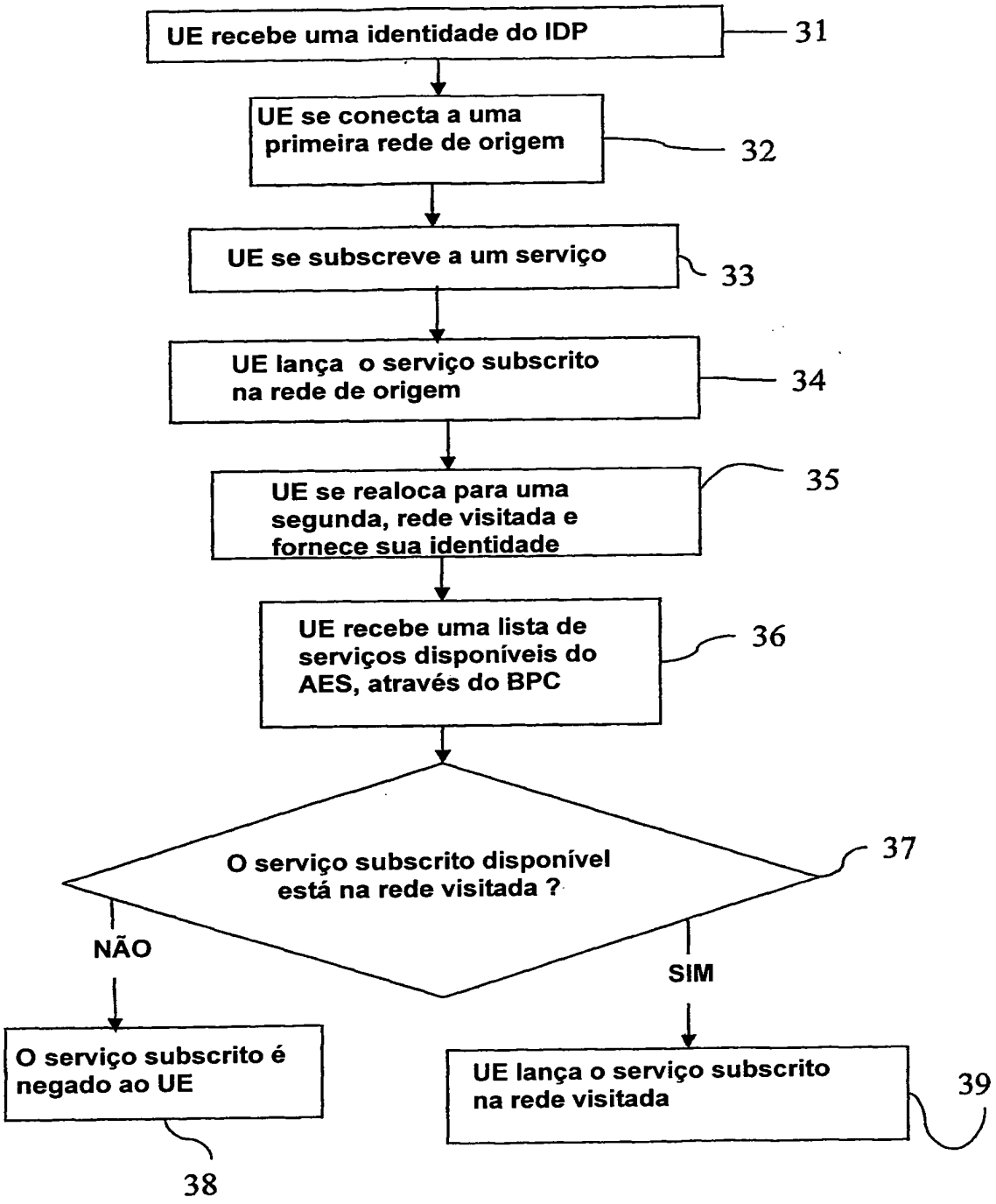

UE recebe uma identidade do IDP
31
UE se conecta a uma primeira rede de origem
32
UE se subscreve a um serviço
33
UE lança o serviço subscrito na rede de origem
34
UE se realoca para uma segunda, rede visitada e fornece sua identidade
35
UE recebe uma lista de serviços disponíveis do AES, através do BPC
36
O serviço subscrito disponível está na rede visitada ?
37
NÃO
SIM
O serviço subscrito é negado ao UE
38
UE lança o serviço subscrito na rede visitada
39

FIGURA 3

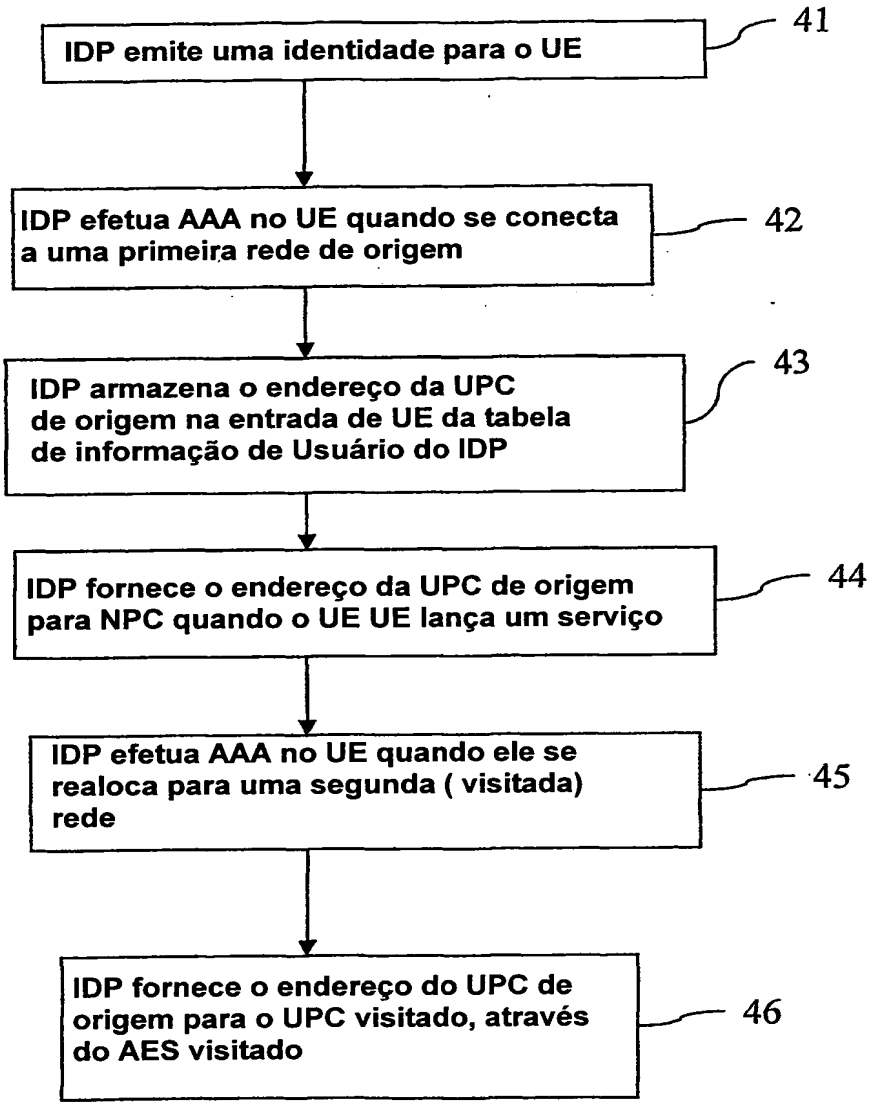

IDP emite uma identidade para o UE
41
IDP efetua AAA no UE quando se conecta a uma primeira rede de origem
42
IDP armazena o endereço da UPC de origem na entrada de UE da tabela de informação de Usuário do IDP
43
IDP fornece o endereço da UPC de origem para NPC quando o UE UE lança um serviço
44
IDP efetua AAA no UE quando ele se realoca para uma segunda ( visitada) rede
45
IDP fornece o endereço do UPC de origem para o UPC visitado, através do AES visitado
46

**FIGURA 4**

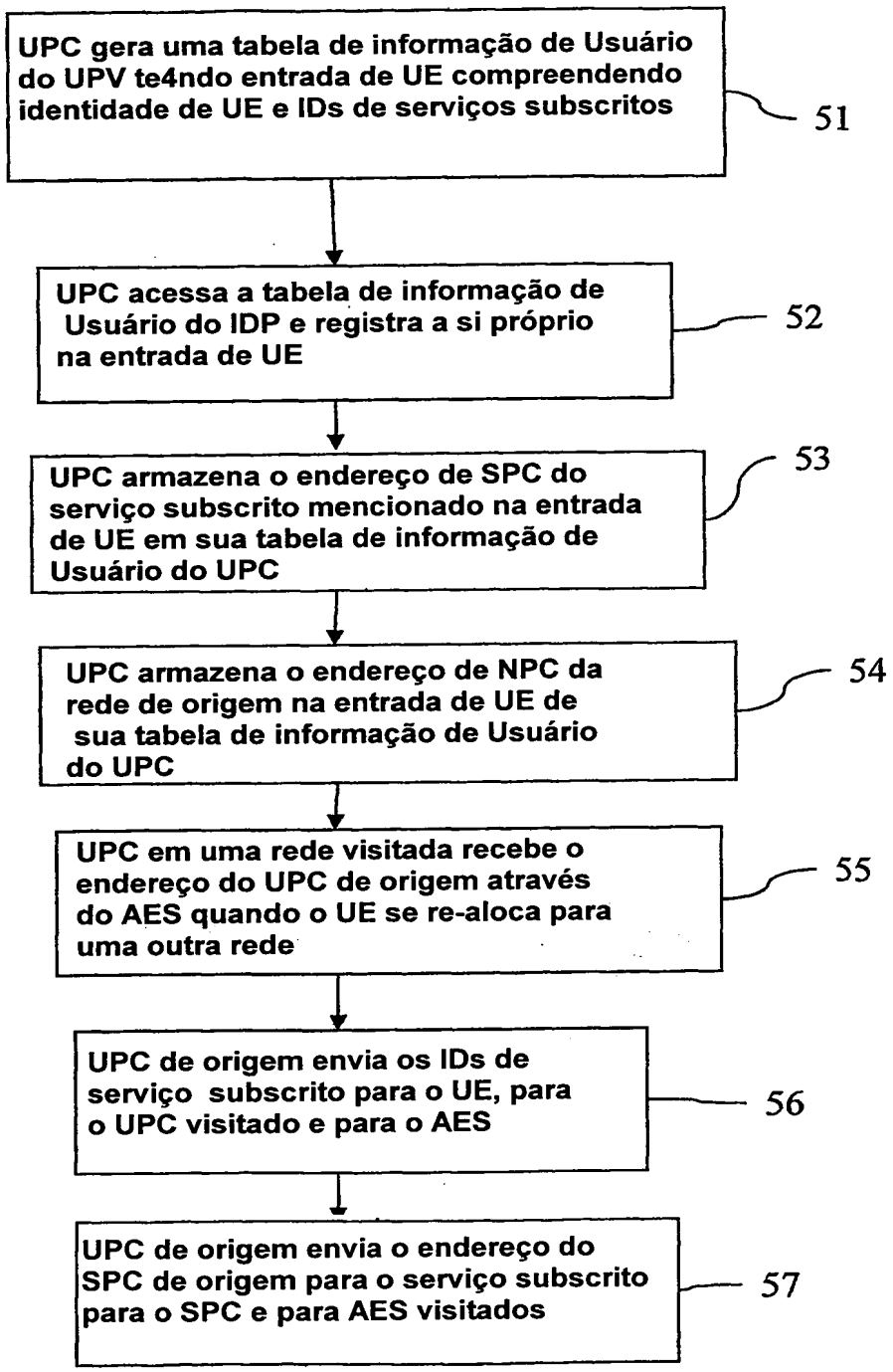

UPC gera uma tabela de informação de Usuário do UPV te4ndo entrada de UE compreendendo identidade de UE e IDs de serviços subscritos
51
UPC acessa a tabela de informação de Usuário do IDP e registra a si próprio na entrada de UE
52
UPC armazena o endereço de SPC do serviço subscrito mencionado na entrada de UE em sua tabela de informação de Usuário do UPC
53
UPC armazena o endereço de NPC da rede de origem na entrada de UE de sua tabela de informação de Usuário do UPC
54
UPC em uma rede visitada recebe o endereço do UPC de origem através do AES quando o UE se re-aloca para uma outra rede
55
UPC de origem envia os IDs de serviço subscrito para o UE, para o UPC visitado e para o AES
56
UPC de origem envia o endereço do SPC de origem para o serviço subscrito para o SPC e para AES visitados
57

**FIGURA 5**

PI 0622025-8

## RESUMO

"ARQUITETURA DE CONTROLE DE POLÍTICA, CONTROLADORES DE POLÍTICA INDEPENDENTE, DE POLÍTICA DE USUÁRIO, E DE POLÍTICA DE NEGÓCIO, MÉTODOS EM UM TERMINAL DE USUÁRIO DE LANÇAR O SERVIÇO EM UMA PRIMEIRA REDE DE ORIGEM E DE LANÇAR O MENCIONADO SERVIÇO EM UMA SEGUNDA REDE, E, MÉTODOS EM UM PROVEDOR DE IDENTIDADE INDEPENDENTE, EM UM CONTROLADOR DE POLÍTICA DE USUÁRIO, EM UM CONTROLADOR DE POLÍTICA DE NEGÓCIO, EM UM CONTROLADOR DE POLÍTICA DE SERVIÇO E EM UM CONTROLADOR DE POLÍTICA DE REDE"

Arquitetura de controle de política arranjada para tratar políticas em redes de comunicação, a arquitetura compreendendo um Provedor de Identidade independente (IDP) arranjado para gerar entradas de terminal de usuário do IDP para informação de controle de política. Ela ainda compreende ainda compreende controladores de política de modo lógico dividido em unidades de controle de política separadas incluindo um Controlador de Política de Usuário (UPC) arranjado para gerar entradas de terminal de usuário do UPC para subscrição de serviços e um controlador de política de Negócios (BPC) arranjado para aplicar políticas relacionadas ao negócios nos mencionados serviços.